Cyberspace, Surveillance, Law and Privacy

Watt, E.

CYBERSPACE, SURVEILLANCE, LAW AND PRIVACY

ELIZA WATT

A thesis submitted in partial fulfilment of the
requirements of the University of Westminster
for the degree of Doctor of Philosophy

September 2017

Table of Contents

Chapter 2: 'Cyberspace and Cybergeopolitics'

Introduction

1. Cyberspace and the 'Cybergeopolitics' of Global Internet Governance
   (a) Cybersecurity Dimensions
      (i) Cyber Security Approaches of the 'West'
      (ii) The 'Eastern' Approaches to Cybersecurity
         - The Russian Federation
         - The People's Republic of China

   (b) Internet Governance
      - The First Phase: Cyber Libertarianism versus Cyber Realism
      - The Second Phase: Global Governance-The 'Battle for the Sole of the Internet'
         - The Mulistakeholder Model and ICANN
         - The Sovereignst Model and the Intergovernmental Policy
      - The Role of the International Telecommunications Union
      - Policy Shaping Through Regional Organizations
      - Domestic Cyber Sovereignty

2. Sovereignty Under International Law and Its Application to Cyberspace
(a) Sovereignty
   (i) Territorial Sovereignty
   (ii) Other Legal Regimes

(b) Jurisdiction in Cyberspace
   (i) State Jurisdiction in Cyberspace

Conclusion

Chapter 3: 'The Role of International Law in Cyberspace Regulation'

Introduction

1. The Application of the Principles of International Maritime Law to the Problem of Cyberspace Governance Through the Use of Analogy
   (a) General: Use of Analogy in International Law

   (b) The Law of the Sea and Its Analogous Application to Cyberspace
      (i) The Development of the International Law of the Sea and Cyberspace Governance-Some Parallels

2. Cyberspace as a Global Common
   (a) The High Seas
   (b) The Outer Space
   (c) Antarctica
   (d) Cyberspace as a Global Common?

3. Cyberspace and the Common Heritage of Mankind
   (a) Common Heritage of Mankind in International Law

   (b) Common Heritage of Mankind and Cyberspace Governance

4. The Regimes Governing the Exclusive Economic Zone/Continental Shelf and Their Applicability to Cyberspace
   (a) Sovereign Rights of Coastal States

   (b) Jurisdiction of Coastal States
      (i) 'Creeping Jurisdiction'

   (c) The Applicability of the EEZ/CS Regimes to Cyberspace Governance

Conclusion

Chapter 4: 'The Right to Privacy in the Digital Age'

Introduction

Part I: General

1. Cyber Surveillance and Transborder Searches
   (a) Transborder Searches as Breach of Territorial Sovereignty
      (i) Transborder Searches of Open Source Data
      (ii) Transborder Searches of Protected Data
         - Transborder Searches of Protected Data with Consent
         - Transborder Searches of Protected Data Without Consent

Part II: The Right to Privacy of Communications

1. The Right to Privacy

   A. International Law ad the Right to Privacy of Communications
   B. Regional Human Rights Systems and the Right to Privacy of Communications
      (a) The European Convention on Human Rights
      (b) The Inter-American Human Rights System
   C. Domestic Legal Basis Permitting Interception of Communications
      (a) Domestic Legal Frameworks Authorising Foreign Surveillance and the Principle of Non-Discrimination

Part III. Do Human Rights Treaties Apply to Extraterritorial Cyber Surveillance and Transborder Access to Data?

1. Extraterritorial Application of Human Rights Treaties

   (a) A Narrow View
   (b) The Expansive View
   (c) Applicability of Human Rights Treaties to Extraterritorial Cyber Surveillance

2. Transborder Access to Data as a Violation to the Right to Privacy

Part IV: Cyber Surveillance as an Interference with the Right to Privacy of Communications

1. UN General Assembly Resolution 68/167

2. The Report of the UN High Commissioner for Human Rights
   (a) Mass Surveillance Necessarily Interferes with Privacy
   (b) The Interception or Collection of Metadata Interferes with the Right to Privacy
   (c) Retention of Data Amounts to Interference

3. UN Special Rapporteur

4. The Council of Europe

5. The IAHR Special Rapporteur

6. The Court of Justice of the European Union

7. The Legal Contours of the Interference with the Right to Privacy of Digital Communications

Part V: Justifications

1. Limitations: Articles 17 ICCPR, 8 ECHR and 11 ACHR
   (a) 'In Accordance with the Law'
      (i) Legal Basis
      (ii) Accessibility
      (iii) Foreseeability

   (b) Legitimate Aim-National Security
      (i) The Effectiveness of Cyber Surveillance Programmes in Fighting Terrorism

   (c) Necessity
      (i) Proportionality
      (ii) Existing Legal Safeguards

Conclusion

Chapter 5: 'International Legal Solutions to State Mass Cyber Surveillance'

Introduction

Part I: Regulation of States' Activities in Cyberspace Through a Hard Law Instrument

A. International Level
   (a) Solution 1- An International Legally Binding Treaty for Cyberspace Based on

Abstract

The thesis titled, *Cyberspace, Surveillance, Law and Privacy* analyses the implications of state sponsored cyber surveillance on the exercise of the human right to privacy of communications and data privacy of individuals, subject to untargeted interception of digital communications. The principle aim of the thesis is to assess the legality of mass cyber surveillance of the Five Eyes alliance, with an emphasis on the United States and the United Kingdom. The study also considers the growing trend among the law enforcement agencies to access data without consent located in foreign jurisdictions without recourse to the Mutual Legal Assistance arrangements. The objective of the thesis is to demonstrate that these activities breach states' human rights obligations under the international human rights frameworks and to show the unprecedented impact that surveillance technologies continue to have on this right. The research also highlights the inadequate protection of privacy in the internet. This leads to the evaluation of a number of possible legal solutions on the international level to the problem of mass surveillance, since the internet is a global environment designed for unrestricted data flows among jurisdictions and therefore facilitates continued violation of privacy of communications and data privacy. The thesis finds that bearing in mind (a) the highly politicised nature of the internet governance discourse, (b) the reluctance of states to subject peacetime espionage to international law regulation through a legally binding treaty, (c) the fact that international human rights law relating to privacy of communications is in need of modernization, (d) the reluctance of states to commit to a legally binding cyber treaty, (e) the slow pace with which customary cyber international law rules emerge and (f) the tendencies of states on the domestic level towards the introduction of draconian surveillance legislation at the expense of privacy, any progress in this regard at this stage will be piecemeal and likely to be achieved through a combination of the updating of the existing international and regional human rights and data protection instruments and soft law agreements.

Acknowledgments

I wish to thank my supervisors, Professor Hélène Lambert, Professor Marco Roscini and Professor Andreas Philippopoulos-Mihalopoulos. I am particularly grateful to Professor Lambert and Professor Roscini for their hard work, support and rigour, with which they guided me throughout the duration of this research. I should also like to thank Ms Ruth MacKenzie for her comments at the various stages of the research.

A special thanks to Dr Steve Greenfield for giving me an opportunity to gain a valuable teaching experience and Mr Stephen Bunbury for his kindness, support and for being a great role model.

Author's Declaration

I declare that all the material contained in this thesis is my own work.

Chapter 1: 'Introduction to the Thesis'

INTRODUCTION

On 6th June 2013 a British newspaper, *the Guardian* reported that the United States (US) National Security Agency (NSA) collects domestic telecommunications metadata from Verizon Business Network Services.[1] The following day, the same newspaper revealed details about PRISM, a suite of NSA programmes that targeted internet communications and stored data of 'non-US persons' outside the US and those communicating with them, together with the extent to which the US companies cooperate with the government.[2] More revelations followed, including details of the interception of communications by both the NSA and its British counterpart, Government Communications Headquarters (GCHQ) on political leaders attending 2009 London G20 summit and GCHQ conducting massive intercepts of domestic communications.[3] This information came to the fore, as a result of document disclosures by a former Booz Allen Hamilton employee, Edward Snowden. Snowden made it publically known that the scope of intelligence gathering activities, by the NSA and other similar organizations, is now unprecedented. Once a narrow, targeted focus of intelligence agencies on gathering information domestically has escalated to allegedly targeting communications of everyone by default.[4] Snowden confirmed that the NSA 'specifically targets the communications of everyone. It ingests them by default. It collects them in its system and it filters [...] analyses [...] measures […] and […] stores them for periods of time simply because that's the easiest, most efficient, and most valuable way to achieve these ends',[5] that is getting intelligence by whatever means.

---

[1] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' (6 June 2013) *The Guardian*, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

[2] Susan Landou, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11 IEEE Computer and Reliability Societies, p. 66.

[3] ibid.

[4] ibid.

[5] Laura Poitras and Glenn Greenwald, 'NSA Whistleblower Edward Snowden: I Don't Want to Live in a Society That Does These Sort of Things' (9 June 2013) *The Guardian* <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>.

These revelations have thrust into the limelight the fact that many states have a great capacity to conduct simultaneous, invasive, targeted and broad-scale surveillance then ever before.[6] With the declining costs of technology and data storage, the financial disincentives of states to conduct digital surveillance have diminished.[7] Equally, the technological platforms upon which global political, economic and social life are increasingly reliant, are not only vulnerable to mass surveillance, but they actually facilitate it.[8] These and similar observations from international organizations, human rights bodies, a number of states and countless civil society groups underpinned subsequent discussions regarding the legality of intelligence gathering activities of the NSA and its partner agencies, especially relating to the right to privacy and freedom of expression. In addition, a related but relatively unexplored problem that has emerged in recent years, which is also facilitated by the borderless internet, relates to the tansborder data access without consent by the Law Enforcement Agencies (LEAs) pursuant to criminal/terrorism investigations.

Most of the attention that followed the allegations of the NSA and GCHQ activities has centred around the assessment and reform proposals of the exiting domestic legal frameworks. Thus, the United Nations General Assembly adopted a series of resolutions on the right to privacy in the digital age as a result of the Snowden leaks.[9] These non-legally binding documents called upon all states to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasising the need for states to ensure the full and effective implementation of their obligations under international human rights law.[10] However, relatively little consideration has been given to the human rights obligations of the states involved in cyber surveillance under international human rights law and international legal redress and solutions regarding mass surveillance. This thesis therefore not only addresses the question of the legality of these activities in the context of states' international human rights obligations, but also identifies a need for greater global and coordinated protection of privacy of communications and data protection. Furthermore, recognizing the complex nature of the issues involved, this study looks further afield to

[6] UN HRC, 'The Right to Privacy in the Digital Age. Report of the Office of the High Commissioner for Human Rights' UN Doc A/HRC/27/137 (30 June 2014), para 2.
[7] ibid.
[8] ibid.
[9] UN GA Resolution, *The Right to Privacy in the Digital Age*, UN Doc 68/167 (14 December 2013); UN GA Resolution, *The Right to Privacy in the Digital Age*, UN Doc 66/169 (14 December 2014); UN GA Resolution, *The Right to Privacy in the Digital Age*, UN Doc A.3/71/L.39/Rev.1 (16 November 2016).
[10] ibid.

international espionage law. In so doing, it positions cyber surveillance within the context of other signals intelligence gathering operations. It identifies a legal gap that inadvertently facilitates the practices of some of the world's largest intelligence agencies, namely the lack of international treaty and the absence of customary international law rules regulating peacetime espionage. The thesis puts forward a number of options to bring mass untargeted cyber surveillance activities in line with states' international human rights obligations. Consequently, it positions the calls from some states, international human rights organizations and civil society for a hard law solution within the broader cyber security and internet governance discourse. To that end, it conceptualises a cyber treaty modelled on United Nations Convention of the Law of the Sea 1982 (UNCLOS).[11] The study finds that due to the polarised attitudes of states to the issues of cyberspace management an internationally binding treaty addressing state behaviour in this domain is unlikely to be achieved at this stage and in any case, will take a considerable amount of time to come to fruition. Furthermore, it is still unknown how privacy of communications and data privacy would be safeguarded through such an instrument. Bearing this in mind, the thesis concludes that any progress in this regard will most likely be incremental and to occur as a combination of various measures on an international and regional levels, such as the processes of modernizing the already existing privacy frameworks (in particular Article 17 of the International Covenant of Civil and Political Rights 1966 and Article 8 of the European Convention on Human Rights 1950), 'globalizing' the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 and the gradual development of customary law rules regulating untargeted mass surveillance, cyber espionage and transborder data access without consent through soft law.

This chapter delineates the aims, objectives and scope of the work. It defines the terms used throughout the thesis, such as cyberspace, cyber surveillance and transborder access to data. It posits cyber surveillance within the broader category of peacetime espionage and shows that mass surveillance programmes such as PRISM and Tempora can be attributed to the states concerned thus triggering their responsibility for internationally wrongful acts. However, generic attribution regarding other forms of cyber espionage must not be assumed, as

[11] United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 397, entered into force 1 November 1994.

attribution will be triggered on the basis of the effective control test and each case must be considered individually.

The chapter continues to set out the international human rights framework, which will form the legal bases in Chapter 4 for the evaluation of the legality of cyber surveillance and transborder data access without consent. It also discusses the methodology used for conducting the research.

DEFINITIONS

This part will define the terms cyberspace and peacetime espionage, including (a) cyber espionage and cyber surveillance; (b) the actors involved; (c) the targets of mass surveillance; (d) the means and methods used and (e) the types of intercepted data. It will discuss the status of peacetime espionage and cyber espionage, including cyber surveillance under international law. It will also address the issue of state responsibility and attribution in the context of cyber espionage and cyber surveillance. Finally, the term transborder data searches/access to data will be defined.

1. Cyberspace

'Cyber' is a prefix that denotes 'computer and electromagnetic spectrum-related activities'.[12] The term cyberspace features in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0),*[13] a second document of this type compiled by an International Group of Experts at the invitation of North Atlantic Treaty Organization (NATO) Cyber Defence Centre of Excellence with an aim of promoting and informing the debate among states regarding the applicability of international law in the cyber domain. The Manual defines cyberspace as 'the environment formed by physical and non-physical components to store, modify and exchange data using computer networks'.[14]

It is a man-made domain, which encompasses the global digital communications environment

[12] Joseph S. Nye, 'Nuclear Lessons from Cyber Security?', (2011) Strategic Studies Quarterly, 18.

[13] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

[14] ibid, Glossary p. 564.

that is embedded in political, economic and social activity.[15] The definition adopted for the purposes of this thesis is borrowed from Benkler, who describes cyberspace as an environment consisting of three layers: the physical, the logical and the content.[16] The first includes the wires, cable and radio frequency spectrum.[17] The second consists of software, whilst the third is the information created by the users.[18] As a term, cyberspace was popularized in the fantasy work of a science fiction novelist William Gibson, who in his 1984 novel *Neuromancer*[19] described this environment as a 'consensual hallucination experienced daily by billions of legitimate operators […] A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity'.[20]

2. Peacetime Espionage

(a) Espionage, Cyber Espionage and Cyber Surveillance

Espionage involves the gathering of information relating to closely protected secrets, often considered as a matter of national security, or of military importance. It is defined, as 'a consciously deceitful collection of information, ordered by a government or organization hostile to, or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the collecting.'[21] Espionage is one of the oldest political and military activity known in history, whose roots can be traced to ancient Egypt, Greece, Rome and China.[22] Accounts of spying appear in some of the world's earliest documents, including

[15] Ronald J. Deibert & Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls', (2012) 18 Global Governance, 339.
[16] Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulating Toward Sustainable Commons and User Access', (2000) 52 Federal Communications Law Journal 561, p. 562.
[17] ibid.
[18] ibid.
[19] William Gibson, *Neuromancer,* (New York: Ace Books 1984).
[20] ibid.
[21] Geoffrey B. Demarest, 'Espionage in International Law', (1996) Denver Journal of International Law and Policy 24, p. 326.
[22] Allen Dulles, *The Craft of Espionage* (New York, David West Group Co., 1963).

those dating from the times of Pharaoh Ramses (ca. 1274 BC.).[23] Today it is also widely 'regarded by states as a necessary tool for pursuing their foreign policy and security interests and for maintaining the balance of power at the inter-state level'.[24] As a method of intelligence gathering, espionage can be subdivided into five categories: (a) imagery intelligence (image reproduction by electronic or optical means, including photography, radar, infrared, and remote sensing from sky or space); (b) signals intelligence (or SIGINT) (information derived from the interception of signal transmission); (c) measurement and signature intelligence (applying various scientific methods, such as electro-optical, acoustic, radio frequency etc. for data extraction); (d) open source intelligence (collecting publically available information) and (e) human intelligence (or HUMINT) (overtly and covertly deriving information from human sources).[25] The next part of this chapter will define cyber espionage, outline its various types and give reasons as to why cyber espionage cannot be said to form part of international customary law.

(b) Cyber Espionage

Whilst it could be said that espionage has existed since the dawn of human history, peacetime cyber espionage is a relatively new, but rapidly expanding phenomenon. Some commentators even argue that cyber espionage currently enjoys a 'golden age'.[26] There are numerous reasons for this, including that it 'reduces risks to intelligence agencies, allows large scale out sourcing of intelligence collecting activities and offers possibilities hitherto unheard of in terms of the ease, swiftness and inexpensiveness of intelligence gathering and with regard to the amount of collected information'.[27] *Tallinn Manual 2.0* defines cyber espionage as 'the use of cyber capabilities to surveil, monitor, capture or exfiltrate electronically transmitted or

[23] Gale Encyclopedia of Espionage and Intelligence, 'Espionage and Intelligence, Early Historical Foundations', <http://www.faqs.org/espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html>.
[24] Max Planck Encyclopedia of Public International Law, 'Spies' (September 2015) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e295?result=1>.
[25] ibid.
[26] see for example Katharina Ziolkowski, 'Peacetime Cyber Espionage-New Tendencies in Public International Law' in *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publications, Tallinn 2013), p. 425.
[27] ibid.

stored communications, data, or other information'.[28] Among the most publicised operations of this kind are GhostNet,[29] Shady Rat,[30] Flame[31] and the Red October.[32] In recent years cyber espionage has become almost common-place. The prevalence, with which these operations take place could by exemplified by the release in 2013 of the Mandiant Report[33] exposing one of the People's Republic of China (China) most persistent cyber economic espionage units, referred to as Advanced Persistent Threat 1 (APT1), believed to be the People's Liberation Army's Unit 61398. Allegedly, the Unit 'has systematically stolen hundreds of terabytes of data from at least 141 organizations across a broad range of industries in English speaking countries and has demonstrated the capability and intent to steal from dozens of organizations simultaneously'.[34] APT1 maintains an extensive infrastructure of computer systems around the

---

[28] *Tallinn Manual 2.0*, supra note 13, Rule 32, p. 168.

[29] *Information Warfare Monitor*, 'Tracking GhostNet: Investigating a Cyber Espionage Network' < http://www.nartv.org/mirror/ghostnet.pdf>.
GhostNet, discovered in 2009 and attributed to China, has successfully infiltrated computer systems of embassies, foreign ministries and other government offices in 103 countries, including the Dalai Lama's Tibetan exile centres in India, London and New York City.

[30] Dimitri Alperovitch, 'Revealed: Operation Shady Rat. An Investigation of Targeted Intrusions into More Than 70 Global Companies, Governments and Non-Profit Organizations During the Last Five Years' (2011) <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.
Dimitri Alperovitch, the vice president of an internet security company McAfee, reported that since 2005 this Remote Access Tool (RAT) targeted at least 72 organizations, including defence contractors, numerous global businesses, the United Nations and the International Olympic Committee. McAfee Report characterised these intrusions as 'a five year targeted operation by one specific actor', allegedly China.

[31] *The Daily Telegraph*, 'Flame: World's Most Complex Computer Virus Exposed', (28 May 2012) <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html.> Flame, active between 2010 and 2012, targeted individuals, government and educational institutions mainly of Iran, but also Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia and Egypt. According to *The Daily Telegraph* 'it could gather files, remotely change settings on computers, turn a computer microphone on to record conversations, take screen shots and copy instant messaging chats'.

[32] Kaspersky, 'Red October. Diplomatic Cyber Attacks Investigation. Report' (14 January 2013) <https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/>. In 2012 Kaspersky Lab revealed a still on-going and large scale cyber espionage network, which targets diplomatic, communications, nuclear and energy (including oil and gas) government sectors in Easter Europe, former USSR countries and Central Asia. The report produced by that organization stated that 'the main objectives of the attackers were to gather intelligence from the compromised organizations, which included computer systems, personal mobile devices and network equipment'.

[33] 'Mandiant: APT1 Exposing One of China's Cyber Espionage Units. Report' (2013) < http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

[34] ibid p. 3.

world, with potentially hundreds of human operators.[35] Other reports of cyber espionage also abound. In 2014 CrowStrike Global Threat Report, for example, noted an alarming increase in such attacks with more nations involved than ever before for economic competitive, political and nationalistic reasons.[36] The unprecedented scale of these activities was also revealed by Edward Snowden, who in 2013 released a number of documents to *The Guardian,* relating to the US National Security Agency (NSA) global surveillance programme.

Based on the current state practice, at least three broad forms of cyber espionage can be distinguished: (i) economically and politically motivated cyber espionage, which includes industrial espionage (ii) military cyber espionage; and (iii) mass cyber surveillance (also termed as bulk interception of communications). The next part will discuss economically and politically motivated espionage and suggest as a separate sub-category of cyber espionage-cyber surveillance.

(i) Economically and Politically Motivated Cyber Espionage

These types of espionage may be conducted by state agencies (such as the NSA and GCHQ) or on behalf of states, by individual hackers, or groups acting for states (for example Chinese Comment Crew or APT1),[37] or on their own behest.

Economic or industrial cyber espionage involves the theft of intellectual property and industrial secrets. These covert cyber intrusions are usually targeted and focus on, *inter alia*, industry and the research and technology sector, thus potentially undermining a country's economy and global competitiveness.[38] The scale and propensity of these practices against some nations, including the US, is such, that it is now recognized as posing serious threat to that country's national security. Some commentators note that the haemorrhage of US intellectual property allegedly due to cyber espionage activities perpetrated by China has currently reached the level of national crisis.[39] It has been observed that nearly every US business sector, such as advanced materials, electronics, pharmaceuticals, biotechnology,

---

[35] ibid.
[36] Kelly Jackson Higgins, 'Nation State Cyber Espionage. Targeted Attacks Becoming Global Norm' < http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/13190>.
[37] *Wired*, 'Chinese Military Group Linked to Hacks of More Than 100 Companies' (19 February 2013) < https://www.wired.com/2013/02/chinese-army-linked-to-hacks/>.
[38] Christina Skinner, 'An International Law Response to Economic Cyber Espionage' (2014) 46 Connecticut Law Review p. 1167.
[39] ibid, p. 1168.

chemicals, aerospace, heavy equipment, autos, home products, software and defence systems, has experienced massive theft and illegal reproduction.[40] China relies on, *inter alia*, hackers at state funded universities and privately owned Chinese technology companies. It is said to be more prolific at conducting cyber espionage than all other countries put together.[41] The scale of the problem is such, that the US White House officially accused China of cyber espionage. On 19 May 2014 the US Department of Justice indicted five members of the People's Liberation Army for the alleged economic cyber espionage activities of Unit 61398.[42]

The United States has also been blamed for economically motivated cyber espionage. The leaked Edward Snowden documents in 2013 revealed that the NSA endeavoured to exploit the technology of Huawei, the Chinese telecommunications giant, through creating 'back-doors' directly into the company's networks- the so called operation 'Shotgiant'.[43] President Obama's administration was adamant that the NSA breaks into the company's networks were motivated by legitimate national security purposes.[44] However, according to the leaked documents the purpose also included gaining access to Chinese's customers in such countries as Iran, Afghanistan, Pakistan, Kenya and Cuba, secured as a result of Huawei investing in new technologies by lying undersea cables to connect its $40 billion a year networking empire.[45] The US and China has been involved in a struggle to create norms relating to industrial cyber espionage since 2009,[46] including the signing of an agreement not to support or conduct cyber enabled theft of intellectual property in 2015,[47] as will be discussed in more detail in Chapter 5 of this thesis.

---

[40] ibid.

[41] David E. Sanger and Nicole Perlroth, 'NSA Breached Chinese Servers Seen as Security Threat' (22 March 2014) *The New York Times* < https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0>.

[42] The US Department of Justice, Office of Public Affairs, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labour Organization for Commercial Advantages' (19 May 2014) <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

[43] Higgins, supra note 36.

[44] ibid.

[45] ibid.

[46] Martin Libicki, 'The Coming of Cyber Espionage Norms' in H. Roigas et al. (eds.) *9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE Publications 2017) 7-19, p. 9.

[47] *Wired*, 'US and China Reach Historic Agreement on Cyber Espionage' (25 September 2015) < https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/ >.

Among the many instances of politically motivated cyber espionage are the NSA monitoring of an American law firm representing a foreign government in trade disputes with the US, the targeted surveillance of the United Nations, the European Union and other international organizations through such operations as 'Blackfoot',[48] 'Perdido' and 'Powell'.[49] These operations, according to the NSA internal document had a key influence on 'American negotiating tactics at the UN' in connection with the Iraq war, as the NSA was able to inform the US State Department and the US Ambassador to the UN that the required majority had been secured before the vote was held on the UN resolution.[50] The recent example of targeted politically motivated cyber espionage is the Russian Federation's (Russia) intrusion into the US Democratic National Committee (the 'DNS hack').[51] The incident, first exposed by the private security firm CrowdStrike,[52] was allegedly conducted by two groups linked to the Kremlin, identified as Cozy Bear and Fancy Bear and exposed in 2016.[53] In the run up to the 2016 US elections, the Kremlin was allegedly able to gain access to the email cache, which were released by WikiLeaks, damaging presidential candidate Hilary Clinton's election prospects.[54] Whilst the DSN hack was not vote-tempering and President Obama emphasised that President Trump's campaign merely exploited the hack to their advantage, Russia's alleged involvement in the election is currently under investigation. Furthermore, questions have been raised regarding that country's influence in several other key European elections in 2017.[55]

[48] Council of Europe Parliamentary Assembly, *Mass Surveillance*, (18 March 2015) Doc. 13734 p.10. 'Blackfoot' was the NSA operation to gather data from French diplomats' offices at the New York UN headquarters.
[49] ibid. Operation 'Perdidot' targeted the European Union's offices in New York and Washington, whilst 'Powell' was NSA's operation involving eavesdropping on the Greek UN offices in New York.
[50] ibid, p. 11.
[51] Dmitri Alperovitch, 'Bears in the Midst: Intrusion into the Democratic National Committee' (15 June 2015) CrowdStrike Blog <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
[52] ibid.
[53] *The Guardian*, 'Top Democrat's Emails Hacked by Russia After Aid Made Typo, Investigation Finds' (14 December 2016) < https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds>
[54] ibid.
[55] Libicki, supra note 46, p. 12.

(ii) Cyber Surveillance

Surveillance is the 'close observation or listening of a person or place in the hope of gathering evidence'[56] and forms part of the SIGINT collection. The origins of collecting signals intelligence can be traced to the advent of the telegraph. Telegraphic transmissions became recognized as public property once radiated signal entered the public domain and therefore are perceived as being open and available for anyone to detect and collect.[57]

This thesis focuses on mass, untargeted cyber surveillance conducted by state intelligence agencies against individuals world-wide for national security purposes, as against targeted instances of cyber espionage (economic/industrial, political and military). The definition of cyber surveillance used throughout the thesis originates from the 2013 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the United Nation's Human Rights Council, which defines communications surveillance as:

> 'the monitoring, interception, collection, preservation and retention of information that has been communicated, relying or generated over communications networks.'[58]

The next part of this chapter will define cyber surveillance activities in more detail by describing (a) the actors involved; (b) the targets of mass surveillance (c) the means and methods employed and (d) the types of intercepted data.

- The Actors Involved in Mass Cyber Surveillance

This thesis will focus on the legality of cyber surveillance activities of the intelligence agencies of the Five Eyes coalition of states, in particular the United State and the United Kingdom. The Five Eyes comprise the five English speaking intelligence agencies, namely: the US National

[56] Bryan A. Garner (ed.), *Black's Law Dictionary* (West Group 1999) 1459.
[57] Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2006) 28 Michigan Journal of International Law p. 631.
[58] UN HRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to the Freedom of Opinion and Expression, Frank La Rue' UN Doc A/HRC/23/40 (17 April 2013), p.3.

Security Agency,[59] the British Government Communications Headquarters (GCHQ)[60] and partner agencies from Canada, Australia and New Zealand.[61] The study will predominantly focus on the activities of the NSA and GCHQ for the following reasons. First, human rights law is concerned with the protection of individuals against violations conducted by states and public authorities, imposing on states the duty to ensure and secure the rights to individuals.[62] It will be shown below that mass cyber surveillance can be directly attributed to the US and UK, which raises the questions of the legality of these practices, explored in Chapter 4 of the thesis. Secondly, the US dominance over the internet is beyond doubt, with much of the traffic being routed through that country. Equally, the pre-eminence in the global market of the American private internet companies (such as Google, Apple, Amazon or Facebook) gives the US broad access to all internet traffic travelling through its territory. In addition, the UK's GCHQ reportedly has the biggest access to the internet traffic of all the Five Eyes countries.[63] Finally, mass surveillance seems to be conducted pursuant to national laws of those states and justified on the bases of access to material relating to terrorism and organized crime, which is important for the purposes of legal scrutiny with regards to the compliance of these domestic laws with the human rights obligations of these states. Although the consideration of human rights obligations of the private sector involved in surveillance and transborder data access without consent (the so-called tech giants such as Google, Facebook, Apple, Microsoft etc.) is part of the issue regarding the protection of online privacy, it is beyond the scope of this work.

The Five Eyes operates under an arrangement said to have been entered into in 1947, called the United Kingdom-United States Security Agreement (the UKUSA Agreement). Very little is known outside the state services what exactly that agreement comprises. It is not however

---

[59] National Security Agency, 'Mission and Strategy' (3 May 2016) < https://www.nsa.gov/about/mission-strategy/>.

[60] The UK GCHQ, in existence in various forms since 1919, is mainly responsible for SIGINT collection.

[61] Canada's intelligence agency is called Communications Security Establishment Canada (CSEC); Australian's- Australian Signals Directorate (ASD) and New Zealand's- Government Communications Security Bureau (GCSB).

[62] International Covenant on Civil and Political Rights, New York, (16 December 1966), 999 UNTS 195 (ICCPR) art 2(1); Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (5 May 1949) ETS No. 005, 213 UNTS 222, art 1; African Charter on Human and People's Rights (27 June 1981) OAU Doc. CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), art. 1; UN HRC General Comment No. 31 'Nature of the General Legal Obligations Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13, para 8.

[63] *Wired*, 'A Simple Guide to GCHQ's Internet Surveillance Programme Tempora' (24 June 2013) < http://www.wired.co.uk/article/gchq-tempora-101>

an international treaty, as it has not been registered with the UN Secretariat in accordance with Article 102 Charter of the United Nations.[64] Therefore being secret, it cannot be 'invok[ed] before any organ of the United Nations'.[65] UKUSA has not only established the Five Eyes for the purpose of sharing primarily signals intelligence,[66] but gave the partners a much wider scope of operations enabling the agencies to intercept, collect, analyse and decrypt intelligence information.[67] Purportedly, UKUSA assigns the responsibility for surveillance to various partners by allocating them the interception 'rights' of different parts of the globe.[68] The agreement also provides for the establishment of jointly run operations centres, 'where operatives from multiple intelligence agencies of the Five Eyes work alongside one another.'[69] The level of cooperation under the agreement is so complete that the national (intelligence) product is often indistinguishable.[70] For that reason the operational methods of the UK and US will be treated as representing the policy stance of all the Five Eyes conducting mass surveillance pursuant to the UKUSA.

- The Targets of the Mass Surveillance

The subject of the interceptions are not only a vast number of the ordinary people world wide, but also some organizations, including, United Nations Children's Fund (UNICEF), Doctors of the World,[71] numerous heads of state, including the German Chancellor Angela Merkel and other state leaders from some 122 countries, including, Columbia, Belarus, Guatemala, Peru

[64] Charter of the United Nations (24 October 1945), 1 UNTS XVI, art 102(1).
[65] ibid, art 102(2).
[66] Privacy International, 'Eyes Wide Open. Special Report' (26 November 2013) <https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf>, p. 4.
[67] ibid, p. 6.
[68] ibid. For example, UK zone includes Africa and Europe, together with the east of the Ural Mountains; Canada's covers north latitudes and the Polar regions; Australia's- Oceania and New Zealand's- the south Pacific.
[69] Privacy International, 'Two Years After Snowden', (June 2015) <https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN.pdf>.
[70] Privacy International, 'The Five Eyes', <https://www.privacyinternational.org/node/51>
[71] Privacy International, 'Two Years After Snowden', supra note 69.

and Somalia.[72] According to the 2015 report of the Parliamentary Assembly of the Council of Europe, *Mass Surveillance*, the US Foreign Intelligence Surveillance Court (FISC) allowed the NSA to intercept information concerning all but four states of the entire world (namely the other four states of the Five Eyes coalition, except the sovereign territories such as the British Virgin Islands) as well as international organizations, including the World Bank, the International Monetary Fund and the International Atomic Energy.[73]

This research will predominantly address the state violations of the right to privacy of private individuals regarding their digital communications. The thesis does not consider in great detail the legality of interception of information that falls within the sovereign authority of states, i.e. 'data which belongs to a state but which is being stored on or transmitted through cyber infrastructure located on the territory of another state',[74] including pertaining to that of the heads of states. The interception of that type of data is beyond the scope of this study, but is highly likely to breach not only the right to privacy under international law, but also as discussed by Buchan, in certain circumstances the principle of territorial sovereignty and non-intervention 'when it has more than insignificant impact on the authority structures of a state'.[75]

- Means and Methods

No fewer than thirteen methods of mass surveillance have been identified[76] thus far, some of which fall outside the scope of this thesis, but they are all worth outlining to illustrate the vast scale of currently conducted operations. Most of these methods are based on the allegations, which emerged from the Snowden documents, subsequently endorsed and validated by many international and regional human rights organizations, including the Parliamentary Assembly of the Council of Europe in the 2015 report *Mass Surveillance.*[77]

---

[72] *The Guardian*, 'NSA Listed Merkel Among Leaders Subject to Surveillance-Report', (29 March 2014) < http://www.theguardian.com/world/2014/mar/29/nsa-merkel-leaders-surveillance-documents-snowden>.
[73] Council of Europe, 'Mass Surveillance', supra note 48, p. 7.
[74] Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' in Anna-Maria Osula and Henry Roigas (eds,) *International Cyber Norms: Legal, Policy and Industry Perspective* (NATO CCD COE Publications 2016) p. 76; Russell Buchan, 'Cyber Espionage in International Law', in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015), pp. 168-190.
[75] ibid.
[76] Privacy International, 'Eyes Wide Open', supra note 66, p. 5.
[77] supra note 48.

The means and methods of mass surveillance of communications include:

(a) direct interception of transatlantic undersea internet cables by the NSA and GCHQ using respectively the Tempora and the Upstream programmes:

(i) Tempora started in late 20111 and is allegedly run by GCHQ under secret agreements with commercial companies ('intercept partners') and involves attaching of intercept probes to transatlantic fibre optic cables located on the UK soil, which carry data to western Europe from telephone exchanges and internet servers in north America. This provides analysts the access to 'huge amounts of data' including all web, email and social chats.[78] The obtained information is held in a 'repository'- content for three days and metadata for up to 30 days 'to allow retrospective analysis and forwarding to other systems'.[79]

(ii) Upsteam data collection programmes, such as BLARNEY, OAKSTAR, FAIRVIEW and STROMBREW, allegedly involve the collection by the NSA of communications from the infrastructure, which carries internet traffic, rather than from servers of internet companies and involves 'the collection of communications from fibre optic cables and infrastructure as data flows by'.[80]

(b) Collection by the NSA of private electronic data from servers of nine US internet companies, under the PRISM programme, the so-called PRISM providers, namely: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. The programme was first authorised by the then President Bush, following the attacks of 11 September 2011 and has been expanded under the Foreign Intelligence Services Act of 2006 and 2007. The types of data collected include emails, chats, videos, photos, stored data, video conferencing and online social networking details.[81]

(c) Interception of internal fibre optic cables used by Google and Yahoo through a joined NSA-GCHQ project called MUSCULAR to transmit unencrypted data

[78] David Anderson, 'A Question of Trust. Report of the Investigatory Powers Review', (June 2015) < https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>, p. 330.
[79] ibid.
[80] ibid.
[81] ibid.

between their data servers.[82] Allegedly in 2012-2013 in thirty days 181 million records were sent from a British collection point to the USA via that programme.[83]

(d) collection of text messages by the NSA from around the world through a tool called DISHFIRE. According to Edward Snowden, almost 200 million text messages per day in 2011 were collected this way, through SMS analysis, which often contain metadata and metacontent (content derived metadata). The metacontent includes notifications relating to credit card transactions and flight plans, which can enhance analytics.[84]

(e) interception of webcam images using a programme called OPTIC NERVE. Allegedly, GCHQ had intercepted and collected webcam images from Yahoo from 1.8 million Yahoo accounts globally.[85] OPTIC NERVE saved one image every five seconds and users were 'unselected', i.e. the collection was in bulk, rather than targeted.[86]

(f) tracking the location of mobile phones. According to Privacy International, 'the NSA collects nearly 5 billion records a day pertaining to the location of mobile phones around the world under the set of programmes known collectively as CP-TRAVELLER'.[87] This is done to such an extent that 'the capabilities are outpacing [the NSA's] ability to ingest, process and store the data';[88]

(g) intercepting telephone calls of entire countries, under the programmes code- named MYSTIC and SOMALGET. Although worth mentioning as part of a 'package' of surveillance methods, these activities are outside the scope of this thesis;

(h) lobbying for surveillance laws abroad: according to Privacy International, a special NSA team, named Foreign Affairs Division, has been tasked with pressurising other countries to change their laws to enable mass surveillance and co-operate with the NSA. As with the interception of telephone call conversations mentioned above, these practices are outside the ambit of this chapter,

(i) providing other partner intelligence agencies, such as Germany and Denmark, with equipment and expertise in order to tap undersea cables in their territories in order

[82] ibid.
[83] ibid. p. 331.
[84] ibid.
[85] ibid.
[86] ibid.
[87] bid.
[88] ibid.

to acquire more information from them. According to Privacy International, 'the technology enables partners to 'ingest' massive amounts of data in a manner that facilitates processing and provides a copy of the intercepted communications to the Five Eyes';[89]

(j) undermining encryption standards; Bullrun and Edgehill are decryption programmes that the NSA and GCHQ have allegedly been using to sabotage encryption standards and undermine the ability to securely communicate;[90]

(k) infecting individuals' devices with intrusive malware in order to be able to have unrestricted access to any smartphone or any other computer at any time, not just in exceptional circumstances;

(l) controlling core communications infrastructure. According to Privacy International, the NSA and GCHQ working in partnership with telecommunications companies, are 'aggressively involved in shaping traffic to artificially change the route of internet communications, redirecting them to flow past Five Eyes interception points' in addition to 'tapping' the communications that cross their borders;[91]

(m) stealing the encryption keys: allegedly, GCHQ and NSA 'hacked into the internal computer network of Gemalto, the largest manufacturer of SIM cards in the world, stealing billions of encryption keys used to protect the privacy of mobile phone communications around the word.'[92]

- Types of Intercepted Data

The revelation of Edward Snowden in 2013 disclosed that the NSA operates two types of programmes pursuant to two different regulatory frameworks, each authorising collection of either the metadata, or contents of communications.

[89] ibid.
[90] ibid.
[91] ibid.
[92] ibid.

- Metadata

Metadata is also know as communications data, which is 'all other information about a communication other than the content- the where, when, who, how long and how'.[93] In terms of electronic communications, such as emails, communications data refers to the 'to' and 'from' lines in the email and its technical details, but not the subject line of the content.[94] In the context of the UK law, a definition of communications data is contained in Article 21(4)(b) of the Regulation of Investigatory Powers Act 2000 (RIPA), which states that:

> communications data are made up of 'traffic data' and 'any information which includes none of the contents of communications (apart from any information falling within paragraph (a)) and is about the use made by any person […] in connection with the provision to or use by any person of any telecommunications services.[95]

This type of data has a significant value to security and law enforcement agencies, as it can help build a detailed picture of an individual's personality, habits and contacts. Unlike content data, it is also not misleading. RIPA recognized the importance of gathering information derived from communications data and in Section 22 lists eight broadly defined purposes, for which metadata could be accessed, including in the interest of national security, crime prevention and public safety.[96]

---

[93] Big Brother Watch, 'Briefing Note: Why Communication Data (Matadata) Matter?' < http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf>

[94] ibid.

[95] Regulation of Investigatory Powers Act 2000, s. 21(4)(b).

[96] Regulation of Investigatory Powers Act 2000, s. 22 states:

(1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.

(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary—
  (a) in the interests of national security;
  (b) for the purpose of preventing or detecting crime or of preventing disorder;
  (c) in the interests of the economic well-being of the United Kingdom;
  (d) in the interests of public safety;
  (e) for the purpose of protecting public health;
  (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

- Content of Communications

The US Foreign Intelligence Services Act 2008 (FISA) on the basis of section 702 allows the government, through the use of the PRISM programme, to conduct surveillance targeting the contents of communications of non-US persons reasonably believed to be located abroad, when the surveillance will result in acquiring 'foreign intelligence information'.[97] The US may acquire 'foreign intelligence information' on a number of national security grounds, including information related to 'actual or potential risk', or 'other grave hostile acts of a foreign power or an agent of a foreign power',[98] possible sabotage,[99] 'clandestine foreign intelligence activities'[100] and 'information relating to the conduct of the foreign affairs of the United States.'[101]

The information is gathered in bulk and therefore does not necessarily fall within the rubric of these enumerated grounds. Edward Snowden disclosures revealed and President Obama's Review Group Report[102] confirmed, that *all* information accessible to NSA is bulk collected. Having collected all the material, the NSA officials would then query communications using specific 'identifiers', such as phone numbers and email addresses that they reasonably believe

---

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

[97] Foreign Surveillance Intelligence Act1978 (amendment 2008), Title VII s. 702 'Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons' (50 U.S.C. sec. 1881a):

'This authority allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad.'

[98] 50 U.S.C § 1801 (e)(1)(A) states that:

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

[99] 50 U.S.C § 1801 (e)(1)(B)

[100] 50 U.S.C § 1801 (e)(1)(C)

[101] 50 U.S.C § 1801 (e)(1)(B)

[102] Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 'Liberty and Security in a Changing World' (December 2013). <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

are used by non-US persons abroad to communicate foreign intelligence information.[103] The 2014 US Presidential Policy Directive 28 (PPD-28)[104] confirmed collection of signals intelligence in bulk,[105] where collection in bulk means 'the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)'.[106] The PPD-28 circumscribed the scope of previously broadly defined 'foreign intelligence' information by limiting it to 'information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists' and enumerated specific grounds for the US bulk collection of non-publicly available signals intelligence, including espionage, terrorism, threat from weapons of mass destruction and cyber security threats.[107]

(c) Espionage/Cyber Espionage and International Law

Being a common practice in international relations even at times of peace,[108] states have

[103] ibid. The Report states on p. 136 that:
Under section 702, the determination of which individuals to target pursuant to these FISC-approved certifications is made by NSA without any additional FISC approval. In implementing this authority, NSA identifies specific "identifiers" (for example, e-mail addresses or telephone numbers) that it reasonably believes are being used by non-United States persons located outside of the United States to communicate foreign intelligence information within the scope of the approved categories (e.g., international terrorism, nuclear proliferation, and hostile cyber activities). The NSA then acquires the content of telephone calls, e-mails, text messages, photographs, and other Internet traffic using those identifiers from service providers in the United States.'

[104] The White House Office of the Press Secretary, 'Presidential Policy Directive- Signals Intelligence Activities. Policy Directive/PPD-28' (17 January 2014)
< https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[105] ibid. Section 2 of the PPD-28 states that:
'Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value', p. 4.

[106] ibid.

[107] ibid. p. 5.

[108] The law of armed conflicts, *jus in bello*, recognizes the existence of these practices, but does not regulate them directly. Instead, the relevant legal instruments relate to the treatment

been cautious to subject espionage to international regulation, which accounts for the lack of international norms directly designed to regulate these activities through an international treaty, or convention.[109] At least one of the reasons for this lack of engagement is that it is not in the interest of nation states, or the international system, to permit regulation of their intelligence gathering activities.[110] Simply put, most states partake in the conduct of espionage and expect that it may be conducted against them. In spite of the lack of a general rule in international law prohibiting peacetime espionage,[111] these activities are not conducted in a legal vacuum. International law norms, such as the general prohibition of intervention, the principle of territorial sovereignty, the law of the sea, air law, the law on diplomatic relations and human rights law do apply but in an indirect manner.[112] Therefore, their lawfulness must be assessed on a case-by-case basis. Some authors, such as Wright argued that the traditional forms of espionage violate the principle of territorial sovereignty, stating that:

> [i]n times of peace […] espionage and in fact any penetration of the territory of a state by agents of anther state in violation of the local law is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of another state.[113]

Other legal scholars have advocated however that espionage is not only common place but also critical to maintaining international peace and security since it actively contributes to the fight against international terrorism and the proliferation of weapons of mass destruction. [114] Equally, the widespread state practice evidenced by the existence of intelligence agencies proves that espionage services are a legitimate function of a state. [115] Their intelligence collection activities are therefore perfectly lawful, since they have often been put on a statutory

---

of spies; see for example: Regulations Concerning the Laws and Customs of War on Land, Annexed to Convention (IV) Respecting the Laws and Customs of War on Land, The Hague, 18 October 1907, Article 29; Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, 8 June 1977, Article 46 (1), (2), (3) and (4).

[109] ibid.

[110] Sulmasy and Yoo, supra note 57, p. 626.

[111] ibid. 'State's practice throughout history (…) supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited'.

[112] Max Plank Encyclopedia, supra note 24.

[113] Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in International Affairs' in Richard Falk (ed.,) *Essays on Espionage and International Law* (Ohio State University Press 1962), p. 12.

[114] Sulmasy and Yoo, supra note 57, p. 637.

[115] Jeffrey H. Smith, 'State Intelligence Gathering and International Law: Keynote Address' (2007) 28 Michigan Journal of International Law p. 544

footing in the domestic legal systems, as for instance is the case with the US National Security Act of 1947.[116] Consequently, this state practice led some commentators to assert that peacetime espionage is legal as a matter of customary international law[117] and by extension so must be cyber espionage.[118] However, before such a conclusion could be reached, the legality of peacetime espionage (including cyber espionage) must be assessed in the light of the principles dictating how customary law is formed. The first port of call is the UN Statutes of the International Court of Justice 1948.[119] Article 38(1)(b) of the Statutes lists, among other sources of law, 'international custom, as evidence of general practice accepted as law'.[120] International customary law consists of two elements,[121] namely (a) state practice, or *usus* and (b) the acceptance of such practice as law (*opinio juris*). This two element approach to the identification of a rule of customary law, which requires an assessment of both practice and the acceptance of that practice as law, is reiterated by the International Law Commission in its Second Report on the Identification of Customary International Law.[122]

(i) State Practice

In order to establish customary law, the International Court of Justice (ICJ) declared in the *Asylum Case* (Columbia v Peru)[123] that a customary rule must be 'in accordance with a constant and uniform usage practiced by the States in question'.[124] The requirement that some degree of uniformity amongst state practices was essential before a custom could be established was emphasised in the *Fisheries Case*.[125] This condition was also reiterated in *North Sea Continental Case,*[126] where the ICJ held that indispensable to the formation of a new rule of customary law is the requirement that state practice must be 'both extensive and virtually

[116] Sulmasy and Yoo, supra note 57, p. 628.
[117] see for example Christopher Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19 American University International Law Review; Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 Air Force Law Review; Demarest supra note 21.
[118] Buchan, supra note 74, p. 81
[119] United Nations, Statutes of the International Court of Justice, 18 April 1946.
[120] ibid, art 38(1).
[121] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v United States of America), (Merits) (27 June 1986) ICJ Reports, para 207.
[122] UN GA International Law Commission, 'Second Report on the Identification of Customary International Law' (22 May 2014) UN Doc A/CN.4/672.
[123] *Asylum Case (Columbia v Peru),* (20 November 1950) ICJ Reports 226.
[124] ibid. p. 284.
[125] *The Fisheries Case* (United Kingdom v Norway) (18 December 1951) ICJ Reports 116, 131, 138.
[126] *North Sea Continental Shelf Case* (Federal Republic of Germany v Denmark; Federal Republic of Germany v the Netherlands) (20 February 1969) ICJ Reports 3, para 74.

uniform in the sense of the provision invoked'.[127] In the *Military and Paramilitary Activities in and against Nicaragua* (the *Nicaragua* case) the ICJ observed that there is no need for 'an absolutely rigorous conformity'[128] of a particular practice by states. Nor is there a requirement that all states must have participated in a certain practice.[129] Rather there must be a 'general', not universal practice and that of the most influential or powerful states would carry the general weight.[130] However, even absent universal acceptance, the requirement of 'extensive and virtually uniform' state practice is 'an extremely high threshold'[131] that states must meet before a legally binding custom can be created. Espionage and by extension cyber espionage, falls at this first hurdle. Despite there being an extensive state practice of espionage and widely held tacit acceptance of it being a common, inherent and established function of a state, this practice is usually accompanied by a 'policy of silence'.[132] Yet, the International Law Commission's Second Report on the Identification of Customary Law clearly states that 'it is difficult to see how practice can contribute to the formation or identification of general customary international law unless and until it has been disclosed publicly'.[133] Consequently, secret state practice does not 'contribute to the formation or identification of general customary international law'.[134] The signals intelligence sharing agreements amongst some states are inevitably secret. This is certainly the case regarding signals intelligence co-operation among the Five Eyes coalition pursuant to the 1947 UKUSA Agreement. The initial Agreement tied the two countries into a worldwide network of listening posts run by the NSA and GCHQ and was later extended to include intelligence sharing among Canada, Australia and New Zealand. It was published and officially acknowledged for the first time in 2010 after freedom of information requests from Britain and the US some sixty years after signing.[135] Under UKUSA the UK and the US agreed to exchange the knowledge from operations involving interception, decoding and transmitting foreign communications, including the acquisition of

[127] ibid, p. 72.
[128] supra note 115, para 186.
[129] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press 2004) p. 4.
[130] ibid.
[131] Buchan, supra note 74, p. 82.
[132] Ziolkowski, supra note 21, p. 441.
[133] International Law Commission Report on the Identification of Customary International Law, supra note 122, para 47; Buchan supra note 74, p. 82.
[134] ibid.
[135] The National Archives, 'Newly Released GCHQ Files: UKUSA Agreement' < https://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf>

communication documents and equipment.[136] UKUSA expressly provided that the activities of GCHQ were to be wrapped in official secrecy, stating that 'it will be contrary to the agreement to reveal its existence to any third party whatsoever'.[137] It was so secretive, that reportedly even the Prime Minister of Australia did not know of its existence until 1973.[138] In addition, the official state denials of conducting cyber surveillance negate this practice qualifying as being conducted publically and openly, since statements made on behalf of governments are classed as a source of state practice for the purposes of ascertaining the existence of customary law rule.[139] For example, in 2013 the then GCHQ director Ian Lobban, called to testify before the UK parliamentary committee in the aftermath of the Snowden disclosures, insisted that the agency was not conducting espionage *en masse* on the British public.[140] In 2014 the New Zealand spy agency Government Communications Security Bureau worked to implement a mass metadata surveillance system as the top government officials publically insisted that no such programme was planned and would not be legally permitted.[141] States sometimes are forced to publicly acknowledge to secret intelligence collection activities, as was the case with the 2014 Obama Speech on the NSA Reform, admitting NSA mass surveillance.[142] Nevertheless, these activities remain covert and as noted by Buchan 'to accept such conduct as evidence of state practice is at odds with the basic tenant of customary international law that state practice is material and detectable'.[143] Therefore, although undoubtedly there is a widespread state engagement in peacetime espionage activities, it is doubtful that it can be established as forming part of *usus* for the purposes of international customary law.

---

[136] *The Guardian,* 'Not So Secret: Deal at the Heart of the UK-US Intelligence' (25 June 2010) < https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released>.
[137] ibid.
[138] Tim Leslie and Marc Concoran, 'Explained: Australia's Involvement with the NSA, the US Spy Agency at Heart of Global Scandal' (19 November 2013) < http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786>.
[139] Malcolm Show, *International Law* (Cambridge University Press, 2008) pp. 81-84.
[140] *Japantimes*, 'Britain's GCHQ 'the Brains', America's NSA 'the Money' Behind Spy Alliance (18 November 2013) <http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.WUKHR8fpV-W>.
[141] Glen Greenwald and Ryan Gallagher, 'New Zealand Launched Mass Surveillance Project Whilst Publically Denying It' (15 September 2014) < https://theintercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/>.
[142] *The Washington Post*, 'Transcript of President Obama's Jan. 17 Speech on NSA Reforms' (17 January 2014) < https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html?utm_term=.d61efb68b674>.
[143] Buchan, supra note 74, p. 83.

(ii) *Opinio Juris*

It is also unlikely that peacetime espionage/cyber espionage satisfies the second element, that is *opinio juris*. *Opinio juris* is a belief that a state activity is legally obligatory. It is a factor, which turns the usage into a custom and renders it part of the rules of international law.[144] The ICJ explained the concept of *opinio juris* in the *Nicaragua* case in the following terms:

> […] for a new customary rule to be formed, not only must the acts concerned 'amount to settled practice' but they must be accompanied by *opinio juris sieve neccessitatis.* Either the [s]tates taking such action or other [s[tates in a position to react to it, must have behaved so that their conduct is evidence of a belief that the practice is rendered obligatory by the existence of a rule of law requiring it. The need for such belief […], the subjective element, is implicit in the very notion of *opinio juris*.[145]

The states concerned must therefore feel that they are conforming to what amounts to a legal obligation.[146] Cyber espionage and in particular mass cyber surveillance is difficult to reconcile with this element to establish a customary rule. As will be shown in Chapter 4 of this thesis, mass cyber surveillance is unlawful under the International Covenant of Civil and Political Rights, the European Convention on Human Rights and the American Convention on Human Rights. To that end, the UN High Commissioner's for Human Rights Report, *The Right to Privacy in the Digital Age*[147] prepared at the request of the UN General Assembly, emphasised that 'overt and covert digital surveillance in jurisdictions around the world have proliferated with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure.' [148] The views expressed in that report, together with UN General Assembly Resolutions 68/167,[149] 69/166[150] and A/C.3/71/L.39/Rev.1[151] on *The Right to Privacy in the Digital Age,* evidence deep concern among most nations regarding mass surveillance. They also reflect the attitudes of the international community. All these points to the lack of 'evidence of a belief that [mass untargeted cyber surveillance] is rendered obligatory by the existence of a rule of law requiring it'.[152] Furthermore, customary law is established by virtue

[144] Show, supra note 139, p. 84
[145] *Nicaragua* case, supra note 121, pp. 108-109.
[146] *North Sea Continental Shelf* case, supra note 126, para 77.
[147] Report of the Office of the United Nations High Commissioner for Human Rights, supra note 6.
[148] ibid.
[149] UN GA Resolution 68/167, supra note 9.
[150] UN GA Resolution 69/166, supra note 9.
[151] UN GA Resolution A/C.3/71/L.31/Rev.1, supra note 9
[152] *Nicaragua* case, supra note 121.

of a pattern of a claim, absence of protest by states particularly interested in the matter at hand and acquiescence by other states.[153] The ICJ defined acquiescence in the *Gulf of Mine* case as 'equivalent to tacit recognition manifested by unilateral conduct which the other party may interpret as consent'.[154] Thus, where states are seen to acquiesce in the behaviour of other states without protesting against them the assumption is that such behaviour is accepted as legitimate.[155] This clearly is not the case with mass cyber surveillance, as a number of states following the 2013 Snowden disclosures vehemently protested against the NSA activities as being contrary to international law.[156] For example, the then President of the Federative Republic of Brazil Dilma Rousseff directly attacked the NSA at the UN General Assembly address accusing the agency of violating international law by its indiscriminate collection of personal information of Brazilian citizens and economic espionage targeted on the country's strategic industries. The President called these actions illegal not only because they breach the right to privacy, 'without which there can be no true freedom of expression and opinion and therefore no effective democracy', but also because they 'undermine the respect for sovereignty without which there can be no basis for the relationship among nations'.[157] Other states have also expressed their disapproval. For instance, the German Bundestag set up a Committee of inquiry on the NSA affair in 2014, which is the only parliament among the Council of Europe member states, which has taken such a step.[158] Therefore, based on the widely held condemnations from the international organizations (including the UN General Assembly, the UN Human Rights Council, the UN Office of the High Commissioner for Human Rights, the Council of Europe) and individual states (such as Brazil and Germany), it can not be said that nations acquiesce without protestation to cyber espionage, particularly mass cyber surveillance. On the contrary, there is clear evidence of protest based on breaches of international law, including international human rights, which negates agreement to these practice and thus, the formation of customary rule.

In summary, peacetime espionage, including mass cyber surveillance, cannot be said to have become part of customary law because it fails to meet the two requirements set out in

---

[153] Show, supra note 139, p. 89.
[154] *Case Concerning Delimitation of the Maritime Boundary in the Gulf of Maine Area* (12 October 1984), 71 ILR 74.
[155] Show, supra note 139, p. 89
[156] Buchan, supra note 74, p. 84.
[157] Address by Her Excellency Dilma Rousseff of the Federative Republic of Brazil at the General Assembly of the United Nations (New York 24 September-1 October 2013) <http://webtv.un.org/watch/brazil-general-debate-68th-session/2688077853001/>.
[158] Council of Europe, 'Mass Surveillance', supra note 48, para 77.

Article 38(1)(b) of the Statute of the International Court of Justice. First, these practices do not fulfil the requirement of constant and uniform state practice, being seldom acknowledged publically, conducted pursuant to secret agreements and often officially denied. Secondly, they cannot be said to form part of *opinio juris* because many states clearly do not believe that they are lawful under international law. In fact, as noted above, some states publicly assert the lack for respect for human rights and point out that these practices breach international law principle of territorial sovereignty. The fact that cyber surveillance is not regulated by an international treaty and is not part of international customary law is therefore crucial in the discussion as to how to bring these activities within the rule of law globally. The ways that this can be achieved and their prospects of success will be discussed in Chapter 5 of the thesis.

(d) Cyber Espionage, Cyber Surveillance and State Responsibility

Another issue that must be addressed at this stage is that relating to state responsibility, a fundamental principle of international law, which provides that whenever one state commits an internationally unlawful act against another state, international responsibility is established between them.[159]

The episodes of cyber espionage and hostile cyber operations (some examples of the former were outlined above, whilst some examples of the latter will be considered in Chapter 2 of this thesis), show the challenges that these activities pose to international law also in relation to establishing responsibility. As *lex generalis*, the principle of state responsibility applies in cyberspace. To that end, the UN Group of Government Experts recognized that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law.[160] In addition, the International Group of Experts drafting the *Tallinn Manual 2.0* agreed in Rule 14 that 'a [s]tate bears international responsibility for a cyber-related act that is attributable to the [s]tate and that constitutes a breach of an international legal obligation'.[161]Generally, responsibility for hostile cyber operations will depend on whether a particular act can be attributed to the state as it is the state that is

[159] Show, supra note 139, p. 778.
[160] UN GA, 'Report of Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/68/98 (24 June 2013), para 23; UN GA, 'Report of Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015), para 28(f).
[161] *Tallinn Manual 2.0*, supra note, 13 Rule 14, p. 84.

responsible for the internationally wrongful acts of the *de jure* and *de facto* state organs.[162] Therefore, attribution in cyberspace is critical when determining the rights and responsibilities of states, for without it 'states are limited in their options to defend against unlawful cyber operations, both within jus ad bellum and jus in bello'.[163] This is an equally important issue in the context of states' human rights obligations, as it is the state who bears 'a prime responsibility and duty to protect, promote and implement all human rights and fundamental freedoms.'[164]

(i) The Nature of State Responsibility

The concept of state responsibility and its customary law status has been confirmed by the International Court of Justice in such cases as the *Nicaragua,*[165] the *Tehern Hostages*[166] and *Gabčíkovo–Nagymaros*.[167] It was summarized by the Permanent Court of International Justice (PCIJ) in the *Factory at Chorzów* case[168] as '[…] principle of international law, and even a general conception of law, that any breach of an engagement involves an obligation to make reparation.'[169] This responsibility as a matter of international law will arise when two elements are met. First, an act or omission is attributable to the state.[170] Secondly, it constitutes a breach of an international obligation.[171]

This approach has been reiterated by the International Law Commission in the Articles on the Responsibility of State for Internationally Wrongful Acts (Articles on State

[162] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro) (*Bosnian Genocide Case*) [2007] ICJ Rep. 43.
[163] Peter Z. Stockburger, 'Control and Capabilities Test: Toward a New *Lex Specialis* Governing State Responsibility for Third Party Cyber Incidents' in H. Rõigas, et al, (eds.), *9th International Conference on Cyber Conflict: Defending the Core* (CCD COE NATO Publications 2017) 149-162, p. 150.
[164] UN GA, Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, Adopted by General Assembly Resolution 53/144 (9 December 1998), art 2.
[165] *Nicaragua* case, supra note 121, paras 283, 292.
[166] *Case Concerning United States Diplomatic and Consular Staff in Teheran* (USA v Iran) [1980] ICJ Rep. 3.
[167] *Gabčíkovo–Nagymaros Project* (Hungary/Slovakia) [1997] ICJ, para 47.
[168] *The Factory at Chorzów* (Claim for Indemnity) (Germany v Poland) [1928] PCIJ Ser. A No. 17.
[169] ibid, at 29.
[170] supra note 139.
[171] *Bosnian Genocide* case, supra note 162, at 115.

Responsibility), adopted in 2001.[172] Although the Articles are not a treaty, they have been extensively cited by international courts and tribunals, are evidenced in state practice and therefore considered as an authoritative statement of the customary law on state responsibility.[173] Thus, Article 1 of the Article reiterates the general rule and states that 'every internationally wrongful act of a [s]tate entails the international responsibility of that [s]tate'.[174] Article 2 provides that there is an internationally wrongful act when conduct consisting of an action or omission (a) is attributable to the state under international law and (b) constitutes a breach of an international obligation of the state.[175] The Commentary to Article 2 explains that term "'attribution' is used to denote the operation of attaching a given action or omission to a [s]tate".[176] The Commentary also makes it clear that 'for particular conduct to be characterized as internationally wrongful act, it must first be attributable of the [s]tate', which it goes on to explain is 'a real organized entity, a legal person with full authority to act under international law'.[177] Furthermore, the Commentary explicitly recognizes that a state does not act of itself, but " 'an act of the [s]tate' must involve some action or omission by a human being or group' [for] 'states can act only by and through their agents and representatives'".[178] It follows that to establish responsibility there must be a link between the state and the person or persons actually committing the unlawful act or omissions.[179] To that end, the Articles identify the following categories of individuals, whose acts may be imputable to the state:

(a) state organs (exercising legislative, executive, judicial or any other function), notwithstanding of their position within the state hierarchy.[180] This category covers all the individual and collective entities, which make up the organization of the state and act on its behalf.[181] This provision reflects customary international law and as stated by

[172] The International Law Commission Articles on State Responsibility [2001] Yearbook of the International Law Commission, Vol. 2, Part 2.
[173] UN GA Responsibility of States for Internationally Wrongful Acts-Compilation of Decisions of International Courts, Tribunals and other Bodies (Report to the Secretary General) UN Doc A/65/76 (2010); UN GA Responsibility of States for Internationally Wrongful Acts-Comments and Information Received form Governments (Report of the Secretary General) UN Doc A/65/96, in Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace* (Edgar Elgar Publishing 2015), p.58.
[174] Articles on State Responsibility, supra note 172, art 1.
[175] ibid, art. 2.
[176] ibid, para 12, p. 36.
[177] ibid, para 5, p. 35.
[178] ibid.
[179] Show, supra note 139, p. 786.
[180] Articles on State Responsibility, supra note 172, art 4.
[181] ibid, the Commentary, para 1, p. 40.

the ICJ in the *Bosnian Genocide* case (Bosnia v Serbia), it is 'one of the cornerstones of state responsibility that the conduct of any state organ is to be considered an act of the state under international law and therefore gives rise to responsibility of the state if it continues a breach of an obligation of the state';[182]

(b) persons or entities exercising elements of government authority, which are not an organ of the state under Article 4, but are empowered by the law of that state to exercise elements of the governmental authority and are 'acting in that capacity in the particular instance'.[183] The Commentary to Article 5 explains that this provision is 'intended to take account of the increasing common phenomenon of parastatal entities, which exercise elements of governmental authority in place of [s]tate organs, as well as situations where former [s]tate corporations have been privatized but retain certain public or regulatory functions'.[184] An example of such a parastatal entity is a private security firms authorised to act as prison guards;[185]

(c) an organ placed at the disposal of a state by another state, if that organ was acting in the exercise of elements to the governmental authority of the former state.[186] The instances of such situations may include a section of the health service placed under the orders of another country to assist in overcoming an epidemic, or judges appointed in particular cases to act as judicial organs of another state;[187]

(d) state organs, persons or entities empowered to exercise elements of the governmental authority even if when so acting they they exceed their authority or contravene instructions.[188] This provision addresses unauthorised or *ultra vires* acts of state organs. It makes it clear that the conduct of such an organ or entity empowered to exercise elements of the governmental authority acting in its official capacity is attributable to the state even if the organ acted in excess of the authority or contrary to instructions;[189]

(e) person or groups acting on the instructions of, or under the direction or control of the state.[190] The Commentary explains that as a general principle the conduct of private

[182] *Bosnian Genocide* case, supra note 162, para 385.
[183] Articles on State Responsibility, supra note 172, art 5.
[184] ibid, art 5 Commentary, para 1, p. 42.
[185] Show, supra note 139, p. 787.
[186] Articles on State Responsibility, supra note 172, art 6.
[187] ibid, art 6 Commentary, para 3, p. 44.
[188] ibid, art 7.
[189] ibid, art 7 Commentary, para 1, p. 45.
[190] ibid, art 8.

persons or entities is not attributable to the state under international law.[191] However, there may be circumstances 'where such conduct is nevertheless attributable to the state because there exits a specific factual relationship between the person or entity engaging in the conduct and the [s]tate'.[192] This could occur either where (i) a private person acts on the instructions of the state in carrying out the wrongful conduct or (ii) where a private person acts under the states' direction or control.[193] In cases involving private persons acting on the instructions of the state (category (i)), the attribution to that state is widely accepted in international jurisprudence.[194] Instances where responsibility will be attributed in this context include state organs supplementing their own action by recruiting private persons as auxiliaries, who are not part of state police or armed forces but who are sent abroad to carry out a particular mission.[195] However, in the case of private persons acting under the state's direction or control (category (ii)), the issue whether conduct was carried out 'under direction or control' is more complex. Such conduct, according the the Commentary to Article 8 'will be attributable to the [s]tate only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation'.[196] The ICJ interpreted the degree of control that a state must exert in order to give rise to responsibility as 'effective control'. In the *Nicaragua* case[197] the Court had to determine whether the conduct of the *contras* was attributable to the United States in order to hold that country responsible for breaches of international humanitarian and human rights law committed by the *contras.* The ICJ found that the US assistance and the general control over the *contras* were not sufficient in the absence of further evidence to attribute their acts to the US government. The Court stated that '[f]or this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that [s]tate had effective control of the military and paramilitary operations in the course of which the alleged violations were committed'.[198] Therefore, general overall control would have been insufficient for responsibility to arise. However, the International Criminal Tribunal for the Former

[191] ibid, art 8 Commentary, para 1, p. 47.
[192] ibid.
[193] ibid.
[194] ibid, para 2, p. 47.
[195] ibid.
[196] ibid, para 3, p. 47.
[197] *Nicaragua*, supra note 121.
[198] ibid, para 64-65.

Yugoslavia in the *Tadić* case[199] adopted a more flexible approach to determine attribution, holding that the degree of control might vary according to the circumstances and a high threshold might not always be required.[200] To that end, the Tribunal applied the 'overall control' test to ascertain whether acts of hierarchically structured groups, such as military groups, armed bands, irregulars or rebels could be attributed to the state. In rejecting the higher standard of 'effective control' in favour of the 'overall control', the Tribunal held that such groups are less likely to receive express direction and control from that state due to their 'structure, a chain of command and a set of rules as well as the outward symbols of authority'.[201] It is therefore more likely that a state would exercise 'overall control' over such groups, that is only have control over the group generally and not specifically directing them with regards to each specific act.[202] This lower standard of attribution has however been criticised by the ICJ in the subsequent *Bosnian Genocide* case.[203] The Court declined to uphold the 'overall control' test and reaffirmed the customary status of the 'effective control' standard, holding that the actions of Serbia and certain paramilitary groups were not attributable to the Federal Republic of Yugoslavia because there was insufficient evidence to show that the state instruction and direction was given in case of each operation where the alleged violations occurred. In so doing, the ICJ reaffirmed the approach adopted in the *Nicaragua* case, stating that '[i]t must […] be shown that [the] 'effective control' was exercised, or that the [s]tate's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations'.[204]

(f) person or a group of persons if the person or group was in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority;[205]

(g) insurrectional or other movement in the event that the insurrection is successful and the movement become the government of the state;[206] and finally

---

[199] *Prosecutor v Tadić* [1999] ICTY Appeals Chamber Judgment, IT-94-1-A.
[200] ibid.
[201] ibid, para 120.
[202] Articles on State Responsibility, supra note 172, art 8 Commentary.
[203] *Bosnian Genocide* case, supra note 162.
[204] ibid, para 211-15.
[205] Articles on State Responsibility, supra note 172, art 9.
[206] ibid, art 10.

(h) approval and adoption by a state of acts of private persons or entities.[207]

In addition to the requirement that an action or omission must be attributable to a state to trigger its responsibility under international law, Article 12 of the Articles of State Responsibility requires that there must be a breach of an international obligation.[208] The Commentary to Article 12 explains that the breach of international obligation means that the act in question is not in conformity with that which is required by that obligation regardless of its origin.[209] This applies to all international obligations of states, whatever their origin may be and include customary rules of international law, obligations arising under a treaty and general principles applicable within the international legal order.[210]

(ii) Attribution in the Context of Cyber Espionage

Rule 15 of the *Tallinn Manual 2.0* makes it clear that 'cyber operations conducted by organs of a [s]tate, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the [s]tate'.[211] This provision reflects Article 4(1) of the Articles on State Responsibility as it reiterates that a sate would be held liable for wrongful acts of its organs, such as the military or intelligence agencies.[212] The interpretation of 'state organ' in Rule 15 of the *Tallinn Manual 2.0* likewise reflects the broad definition adopted by the International Law Commission[213] and includes 'all persons or entities that have that status under the [s]tate's domestic laws […] regardless of their function or place in the governmental hierarchy'.[214] It follows that 'any cyber activity undertaken by the intelligence, military, internal security, customs, or other [s]tate agencies engages [s]tate responsibility if it violates an international legal obligation binding on that [s]tate'.[215] Such organs must perform governmental function and the responsibility will be triggered even if the conduct in question is *ultra virus*, that is it exceeds the authority granted by the states or contravenes its

[207] ibid, art 11.
[208] ibid, art 12.
[209] ibid, art 12 Commentary, para 3, p. 55.
[210] ibid.
[211] *Tallinn Manual 2.0,* supra note 13, Rule 15, p. 87.
[212] ibid, Rule 15 Commentary, para 1, p. 87.
[213] Articles on State Responsibility, supra note 172.
[214] *Tallinn Manual 2.0,* supra note 13, para 2, p. 87.
[215] ibid.

instructions.[216] What qualifies as elements of governmental authority are those that represent quintessential governmental function, that is activities over which governments typically exercise competence, such as the conduct of foreign affairs, the operation of police force etc.[217] In order to attribute a particular conduct to the state in the context of cyber espionage, two situations must be distinguished: (a) cyber surveillance and (b) other forms of espionage (industrial, political and military).

- Attribution and Mass Cyber Surveillance Programmes

Mass cyber surveillance conducted through such surveillance programmes as PRISM, Tempora and Upstream are highly likely to be attributable to the United States and the United Kingdom for at least two reasons. First, they are operated by state intelligence agencies (the NSA and GCHQ), which under Article 4 of the Articles of State Responsibility (reflected in Rule 15 of the *Tallinn Manual 2.0*) are the organs of those states, as they conduct state functions. Thus, the National Security Agency is the official US cryptologic organization, constituted under the National Security Council Intelligence Directive (NSCID No. 9) issued by President Truman and the National Security Council in 1952.[218] Founded in 1952, the NSA is the biggest signals intelligence agency in the United States, mainly focused on the oversees, rather than domestic surveillance. Among its functions are internet and phone interceptions and code breaking. Following the controversy of the Watergate scandal, the NSA was placed under the investigation of the US Senate Church Committee in 1975.[219] As a result of the Committee's findings, the US Congress enacted the Foreign Intelligence Surveillance Act 1978 (now amended by the 2008 Amendment Act), which set guidelines with regards to what and how the NSA was to conduct its collection activities.[220] In particular, the organization was placed under the supervision of the Foreign Intelligence Surveillance Court (FISC), so that any interception of communications of the American citizens had to be conducted pursuant to a warrant issued by the FISC.[221] The Foreign Intelligence Surveillance Act (as amended) is also

[216] ibid, paras 5-6; Articles on State Responsibility, supra note 172, art 4, para 13.
[217] *Tallinn Manual 2.0*, supra note 13, para 9, p. 89.
[218] *The Saturday Evening Post*, 'A Brief History of the NSA: From 1917 to 2014' (17 April 2014) < http://www.saturdayeveningpost.com/2014/04/17/culture/politics/a-brief-history-of-the-nsa.html >. The NSA begun as a secret organization referred to as 'No Such Agency'.
[219] ibid.
[220] ibid.
[221] ibid.

one of the legal basis upon which the NSA conducts its signals intelligence gathering abroad. Similarly, GCHQ performs state functions set out under the UK Intelligence Services Act 1994.[222] Being a primarily foreign-focused intelligence agency, its signals intelligence role can only be exercised in the interest of national security, economic well-being of the UK and in support of the prevention or detection of serious crime.[223] GCHQ provides advice and assistance to certain UK bodies and public sector for the protection of communications in the UK.[224] The overall responsibility within the UK government for intelligence and security matters lies with the Prime Minister, whilst the day-to-day ministerial responsibility for GCHQ, with the Foreign Secretary. The activities of GCHQ are subject to scrutiny by the Intelligence and Security Committee of Parliament, whilst its interception of communications operations are authorised under the Regulation of Investigatory Powers Act 2000.[225] Complaints regarding GCHQ can be brought before the Investigatory Powers Tribunal.[226]

Secondly, the government of the US was forced to publically admit the existence of its mass cyber surveillance apparatus, particularly the PRISM programme,[227] following the Snowden disclosures and consequently face the uproar from other heads of state, including Brazil and Germany. Whilst the UK confirmed that it has been the recipient of data from PRISM via its intelligence sharing relationship with the US, the government adopted a 'neither confirm nor deny policy' towards Tempora.[228]

On these bases it could therefore be concluded that intelligence collection authorised by the US FISA 2008 and UK RIPA 2000 through *inter alia* the PRISM and Tempora programmes operated by the NSA and GCHQ engage these countries responsibility under international law since they can be attributable to these states and as shown in Chapter 4 of this thesis, violate their international human rights obligations, thus constituting an internationally wrongful act.

---

[222] UK HMG, 'GCHQ Oversight' (17 April 2016) <https://www.gchq.gov.uk/features/gchq-oversight >.
[223] ibid.
[224] ibid.
[225] ibid.
[226] ibid.
[227] Policy Directive PPD-28, supra note 104.
[228] Liberty, 'Liberty's Evidence to the Intelligence and Security Committee's Inquiry into Privacy and Security' (14 February 2014)
< https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20evidence%20to%20the%20ISC%20inquiry%20into%20privacy%20and%20security%20%28Feb%202014%29.pdf>

- Attribution and Other Forms of Cyber Espionage

Attributing other forms of cyber espionage to any given state is more problematic as these types of operations may involve state, or non-state actors. Each instance of cyber espionage must therefore be assessed separately.

As already noted above, a state is generally responsible for internationally wrongful acts by both the state organs[229] and non-state actors who are neither *de jure* or *de facto* state organs, but who operate under the direction or control of the state.[230] In the context of cyber espionage, a state's responsibility will therefore be triggered if (a) a particular cyber operation can be attributed to that state organ or (b) be imputed to that state if conducted by non-state actor (that is neither *de jure* or de *facto state* organ) if that entity is if fact acting on the instructions of, or under the direction or control of the state carrying out the conduct.[231] As noted above, the direction and control requirement has been interpreted and confirmed by the International Court of Justice in the *Nicaragua*[232] and the *Bosnian Genocide*[233] judgments as the 'effective control' test. This test has been endorsed by the International Group of Experts in the *Tallinn Manual 2.0* as applicable in cyberspace and reflecting customary international law.[234] Thus, Rule 17 of the *Tallinn Manual 2.0* confirms that 'cyber operations conducted by a non-[s]tate actor are attributable to a [s]tate when: (a) engaged in pursuant to its instructions or under its direction or control, or (b) the [s]tate acknowledges and adopts the operations as its own'.[235] Cyber operations of such state agencies as the NSA and GCHQ seem to be excluded from the ambit of Rule 17 as the commentary to this rule explains that 'acting pursuant to instructions of a [s]tate is generally equated with conduct that is authorised by that [s]tate, but does not fall within the scope of Rule 15 [Attribution of cyber operations by State organs], which addresses entities that have been legally empowered to exercise particular elements of government authority.'[236] Rule 17 therefore covers non-state actors that function as a state's auxiliary.[237] State responsibility in this context will be established on the basis of the effective

[229] Articles on State Responsibility, supra note 172, art 4(1).
[230] ibid, art 8.
[231] ibid.
[232] *Nicaragua* case, supra note 121.
[233] *Bosnian Genocide* case, supra note 162.
[234] *Tallinn Manual 2.0* supra note 13, Rule 17, Commentary para 5.
[235] ibid, Rule 17 p. 94.
[236] ibid, para 4 p. 95.
[237] ibid.

control of a particular cyber operation, whenever it is the state that determines the execution and course of the specific operation and the cyber activity engaged in by the the non-state actor is the 'integral part of the operation'.[238] Moreover, 'effective control includes both the ability to cause constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway'.[239]

The identification of a particular individual or entity for the purposes of attribution is evidentially very difficult as any cyber operation can be conducted with a degree of anonymity and/or denied. An internationally wrongful act in cyberspace may be ascribed to a particular computer (by way of its IP address that pin points its geographical location). However, the identity of its users is uncertain and may only be known by way of presumption, or through an exposure of a whistle blower.[240] It follows, that if a computer can be identified as a government computer due to its location, for example in a government department or on diplomatic premises, than a cyber espionage operation may in principle be attributed to the state.[241] This could be so on the basis of the identity of the operator, who may be presumed to be a government agent, or the location of the computer, as it falls under the exclusive and complete control of the state. An illustration of attribution on this basis is the German government diplomatic protest against the UK and US government's espionage against German governmental departments, including the office of the Chancellor from the UK and US embassies in Berlin.[242]

The difficulty regarding attribution, unless it is formally acknowledged, is further compounded where cyber espionage appears to be conducted by a non-state actor. A case in point is the cyber breaches of the US Democratic National Committee's computer system (the DNS hack) discussed previously, by two entities identified as Cozy Bear and Fancy Bear. These two groups were linked by the US authorities to the Russian state. This was justified by the US government on the grounds of their "advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft" and because both groups 'engage in extensive political and economic espionage for the benefit of

[238] ibid, para 6; Articles on State Responsibility, supra note 172, art 8, Commentary para 3.
[239] *Tallinn Manual 2.0*, ibid.
[240] Constantine Antonopoulos, 'State Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace* (Edgar Elgar Publishing 2015) 55-72, pp. 62-65.
[241] Articles on State Responsibility, supra note 172, art 4, *Tallinn Manual 2.0* supra note 13, Rule 15.
[242] Nigel Morris et. al., "Germany Calls in Britain's Ambassador to Demand Explanation Over 'Secret Berlin Listening Post'" (6 November 2013) in Antonopoulos, supra note 240.

the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services'.[243] In January 2017 the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) issued a Joint Analysis Report, titled 'GRIZZLY STEPPE-Russian Malicious Cyber Activity',[244] which publically attributed the DNC cyber intrusion to the Russian state. The report 'provid[ed] technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services (RIS) to compromise and exploit networks and endpoints associated with [*inter alia*] the US elections'.[245] Public attribution to the Russian state, the document stated, is supported by the technical indicators from the US intelligence community, the DHS, FBI, private sector and other entities.[246] The report expanded on the previous Joint Statement issued in October 2016 from the DHS and the Director of National Intelligence on Election Security.[247] It concluded that the technical indictors prove that threat actors are 'likely associated' with the Russian state.[248] However, the focus on the report for attribution purposes was not on the 'effective control' test but instead on capabilities, methods, motivations and technical indicators.[249]

This and other examples of recent state practice regarding publicly attributing hostile cyber operations to other states[250] point to the growing tendency that "imputed state responsibility for the unlawful cyber operations of non-[s]tate actors who are neither *de jure* nor *de* facto [s]tate organs is being assigned without rigid adherence to the 'effective control' test [but on the basis of] control and capabilities test, examining motivations, geographic location, technical indicators and relationship between the non-[s]tate actor and the [s]tate".[251]

---

[243] Dmitri Alperavich, 'Bears in the Midst: Intrusion into the Democratic National Committee' in Stockburger, supra note 163, pp. 159-161.
[244] US Department of Homeland Security and Federal Bureau of Investigation, 'GRIZZLY STEPPE-Russian Malicious Cyber Activity. Joint Analysis Report' (29 December 2016) <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf >
[245] ibid.
[246] ibid.
[247] ibid.
[248] ibid.
[249] Stockburger, supra note 163, p. 161.
[250] ibid. This includes the US publicly attributing the 2014 attack on Sony to North Korea, the 2016 public attribution by that country of certain cyber attacks to Iran in 2016 and publicly linking the 2014 Yahoo intrusion to the Russian state.
[251] ibid.

3. Transborder Data Searches

In addition to the globe-spanning networks created by the intelligence agencies, the law enforcement agencies (LEAs) seem also to exercise an almost unrestricted transborder access to data stored in 'a cloud' and/or on servers located in other jurisdictions by private companies as part of their criminal investigations. In most countries these authorities comprise the police, but they may also include prosecutors' offices, designated military/defence authorities, financial and tax agencies, border/customs officials and special directorates.[252]

The ability of the LEAs to directly access computer data has been an on-going practice even before the Snowden revelations,[253] but his exposures highlighted that enormous amounts of data generated daily can be accessed by the authorities of third countries, often without any authorisation, in order to secure electronic evidence for the purposes of criminal prosecution, circumventing the formal cooperation channels, such as the Mutual Legal Assistance (MLA) procedures. The scale and the seriousness of the problem have been recognized *inter alia*[254] by

[252] For example, the European Union Framework Decision 2006/960/JHA, 18 December 2006, art 2 defines a competent law enforcement authority as 'a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities', expressly excluding from this definition the intelligence services.
The US definition is quite broad and states that law enforcement agencies are 'any number of agencies (outside the Department of Defence) chartered and employed to enforce US laws in the United States, a state or territory (or political subdivision) of the United States, a federally recognized Native American Tribe or Alaskan Native Village, or within the borders of a host nation.' US Department of Defence Directory of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 February 2016), <http://fas.org/irp/doddir/dod/jp1_02.pdf>, p. 139.

[253] The first widely publicised example in this regard became known as the 'SWIFT affair' and was disclosed by the media in 2006. According to their reports, for several years US LEAs had been accessing massive amounts of personal data related to European financial transactions by obtaining that information directly from a private company, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) based in Belgium. The affair revealed that a European company can transfer data to the US without complying with the applicable EU legal procedures for years, with seemingly acquiescent silence of certain European institutions and without any sanctions. For more on the SWIFT affair see Gloria Gonzalez Fuster, Paul De Hert and Serge Gutwirth, 'SWIFT and the Vulnerability of Transatlantic Transfers', (2008) International Review of Law, Computers and Technology, 191-2002.

[254] Additionally, Council of Europe Article 29 Data Protection Working Party, 'Article 29 Working Party's Comments on the Issue of Direct Access by Third Countries' Law Enforcement Authorities to Data Stored in Other Jurisdiction, as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime' (5 December 2013) (Ares.2013) 3645289-05/12/2013, <http://ec.europa.eu/justice/data-protection/article-

the Cyber Crime Committee (T-CY), [255] a body that represents the state parties to the Cybercrime Convention (the Budapest Convention).[256] Based on Article 46 of the Budapest Convention, the consultations of the Committee aim at facilitating the effective use and implementation of that Convention, the exchange of information and the consideration of any future amendments.[257] In the 2014 report titled 'Transborder Access to Data and Jurisdiction: Options for Further Action' by the T-CY, the T-CY observed that the increasing number of countries unilaterally access data stored abroad for criminal justice purposes. The T-CY recognized the problems these practices create but noted that relying on states to adopt their own solutions would lead potentially to a 'jungle situation', whilst taking no action would result in more crime and violation of human rights. [258] The Report warned that the Budapest Convention must not be used for national security or mass surveillance purposes, as it does not permit blanket/transborder access, collection and transfers of data.[259] Similar concerns were raised by the Council of Europe Article 29 Data Protection Working Party (Article 29 Working Party), a body composed of representatives from the data protection authorities of each EU Member State, the European Data Protection Supervisor and the European Commission. According to the view expressed by the Article 29 Working Party 'transborder data transfers in the field of law enforcement must exclude blanket/mass transborder access, collection or transfer to/of data, which is incompatible with the [European Union] Charter of Fundamental Rights and the European Convention of Human Rights'.[260] In addition the Council of Europe

29/documentation/otherdocument/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf>.; Council of Europe Commissioner for Human Rights, Nils Muižnieks 'The Rule of Law on the Internet and in the Wider Digital World' (2014) <http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf>, p. 18; and the Centre for European Policy Studies, 'Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights' <*https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf*>.

[255] Council of Europe, 'Cybercrime Convention Committee' < https://www.coe.int/en/web/cybercrime/tcy>.

[256] Council of Europe, Convention on Cybercrime, (23 November 2001), ETS No. 185.

[257] ibid.

[258] Cybercrime Convention Committee (T-CY), 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' Report Prepared by the Ad-hoc Subgroup on Tranborder Access and Jurisdiction Adopted by the 12th Plenary of the T-CY (2-3 December 2014), para 2.2.5, p.7 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf>.

[259] ibid, paragraph 2.2.1 p. 5.

[260] Article 29 Data Protection Working Party, supra note 254.

Commissioner for Human Rights, Nils Muižnieks, in his 2014 report observed that Article 32 of the Budapest Convention 'appears to support the tendency of law-enforcement agencies to resort to "informal" means of information gathering, even across borders, without laying down clear safeguards (for instance that such informal measures should not be used for intrusive information-gathering activities that normally, in a state under the rule of law, require a judicial warrant).'[261] He also noted that Article 32, 'seems to support the tendency of such authorities to increasingly "pull data" directly from servers in other countries, or to demand that companies within their jurisdiction-particularly the main internet giants-do this for them, without recourse to formal, inter-state mutual legal assistance arrangements, arguably in violation of the sovereignty of the state where the data are found'.[262]

This situation creates challenges for international law, as it is highly likely to breach human rights obligations of the states concerned, as will be explored in Chapter 4 of this thesis.

METHODOLOGY

Cyberspace is a relatively new environment for scholarly enquiry. It has been widely accepted that many of the international human rights that individuals enjoy offline are also protected online.[263] This thesis therefore goes beyond the enquiry as to whether international human rights law applies to this environment. Instead, it seeks the answer to the following questions:

1. What are the obligations of states with regards to the protection of online privacy when conducting mass untargeted cyber surveillance/transborder data searches?

2. Do states violate the right to privacy when engaging in these practices?

[261] Council of Europe Commissioner for Human Rights, supra note 254, p. 18.
[262] ibid.
[263] UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' UN Doc A/HRC/32/L.20 (27 June 2016) para. 1; UN GA Res., *The Right to Privacy in the Digital Age* UN Doc A/RES/68/167 (18 December 2013), supra note 9, para 3; UN GA, 'Report of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015), supra note 159, paras. 13(e), 26; Agreement Between the Governments of the Member States of Shanghai Cooperation Organization on Cooperation in the Field of International Security (19 June 2009), art. 4(1).

3. How do the existing international human rights treaties apply in the context of cyber surveillance/transborder data searches? For example, are states bound by human rights obligations when conducting extraterritorial surveillance and if so, what legal test applies?

4. Are individuals' rights safeguarded sufficiently under the existing international law, or is there a need for a new international treaty setting out privacy norms?

5. If, so what are the prospects that such an instrument be adopted? What other options are there if this is not feasible?

The research methods adopted for the purposes of this thesis is doctrinal, sometimes also described as theoretical legal research. Doctrinal research asks what the law is on a particular issue. [264] Generally, this type of research is concerned with analysis of the legal doctrine and how it has developed and applied. It is conducted through the collection and analysis of primary sources, such as relevant legislation and case law, together with secondary materials such as journal articles and other written commentaries on the case law and legislation. [265] The researcher's principle or even sole aim is to describe a body of law and how it applies.[266]

This thesis researches a particular aspect of states' behaviour in cyberspace in the context of international human rights law. In order to establish the content and scope of these norms the research enquires into the sources of international law, as specified in Article 38(1) of the Statutes of the International Court of Justice. Article 38(1) provides that:

> [t]he Court, whose function is to decide in accordance with international law such disputes as are submitted to it shall apply:
> (a) International conventions, whether general or particular, establishing rules recognized by the contesting states;
> (b) International custom, as evidence of a general practice accepted as law;
> (c) The general principles of law recognized by civilized nations;

[264] Mike McConville and Wing Hong Chui (eds.) *Research Methods for Law* (Edinburgh University Press 2007), pp.16-19.
[265] ibid.
[266] ibid.

(d) Subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of the rules of law.

The sources used for the purposes of conducting this research can be grouped in the following categories: (a) international treaties; (b) evidence of emerging customary law; (c) judicial decisions; (d) teaching of publicists; (e) acts of international organizations and (f) soft law. Each source will be briefly described in turn.

(a) International Treaties

Article 38(1) refers to international treaties as sources establishing rules and as such they represent legally binding obligations undertaken by state parties. A definition of a treaty is found in Article 2 of the Vienna Convention of the Law of the Treaties, which states that a treaty is 'an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation'.[267]

The right of privacy of communications is guaranteed in a number of international and regional treaties. This research centres on the International Covenant on Civil and Political Rights 1966 (ICCPR),[268] the European Convention on Human Rights 1950 (ECHR)[269] and the American Convention of Human Rights 1969 (ACHR).[270] The reason for selecting these legal instruments are two fold. First, they set out the benchmark of privacy protection internationally and regionally. Secondly, they are also applicable to the United States and the United Kingdom-the states with the most advanced cyber surveillance capabilities and in case of the US, prolific transboder data searches.[271]

From October 2012 the number of states parties to the ICCPR stands at

[267] Vienna Convention on the Law of the Treaties, concluded at Vienna 23 May 1969, 1155 UNTS 331, 8 ILM 679, entered into force 27 January 1980, art 2(1)(a).
[268] supra note 62.
[269] ibid.
[270] Organization of American States, American Convention on Human Rights (Pact of San Jose) adopted at San Jose, Costa Rica, 22 November 1969.
[271] United Nations Treaty Collection, International Covenant on Civil and Political Rights, Status at 13 April 2016, <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&lang=en#EndDec>;

167, including the Five Eyes members. Australia ratified the ICCPR in 1978, Canada in 1976, New Zealand in 1978, the United Kingdom in 1976. The US signed the ICCPR on 5 October 1977 and ratified it on 8 June 1992. According to the US Declaration (1) '[…] the provisions of articles 1 through 27 of the Covenant are not self-executing', which means that the Covenant does not have effect in domestic law as the US has not passed legislation to give it such effect. Therefore, individuals may not rely directly on its provisions in the US courts.[272]

The European Convention on Human Rights binds only those state parties of the Council of Europe, which ratified the Convention and includes 47 members. The only signatory from the Five Eyes is the United Kingdom, which incorporated it as part of its domestic law with the entry into force of the Human Rights Act 1999 on 2 October 2000. The ECHR does not have any legal effect on the United States or the other Five Eyes members at either domestic, or international level.

The US has signed the Pact of San Jose on 6 January 1977 but has not ratified it, therefore it cannot be bound by the Convention.[273] The remaining four members of the Five Eyes neither signed nor ratified it. Nevertheless, it will be taken into consideration for the purposes of Chapter 4, 'Right to Privacy' as the practices of the Five Eyes clearly impact on the right to privacy in the Pan-American system.

The research does not however consider in any great detail the African Charter on Human and People's Rights (AFCHPR),[274] as it lacks specific recognition of the right to privacy. Brief mention is nevertheless made in Chapter 5. Nor does it address the legality of mass surveillance/transborder data searches in relation to the obligations contained under the African Union Convention on Cyber Security and Personal Data 2014.[275] For the Convention to enter into force, Article 36 specifies the number of ratification at fifteen.[276] Thus far, only Senegal has ratified the treaty.[277]

---

[272] ibid.
[273] Inter-American Commission on Human Rights, B-32 American Convention on Human Rights, 'Pact of San Jose'.
< http://www.cidh.org/basicos/english/Basic4.Amer.Conv.Ratif.htm>
[274] African (Banjul) Charter on Human and People's Rights, adopted June 27 1981, OUA Doc CAB/LEG/67/3 rev 5, 21 ILM 58 (1982), entered into force 21 October 1982.
[275] African Union, African Union Convention on Cyber Security and Personal Data, adopted 27 June 2014.
[276] ibid, art. 36.
[277] List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data, (15 June 2017)
< https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_.pdf >

(b) Custom

International law treats states as the principle law makers of the international system. In that sense, 'states are simultaneously the main subjects of international law and the entities, whose choices and conduct generate positive international law. The choices and conduct of states are their 'practice' and the general practice of states is an essential element in the emergence, evolution, decline and disappearance of norms of customary international law'.[278]

Since 1947 the task of the 'promotion of the progressive development of international law and its codification' has been vested in the International Law Commission (ILC) by the UN General Assembly.[279] The ILC's report on the Identification of Customary Law[280] adopts as its basic approach to the determination of the existence and content of a rule of customary international law general practice that is accepted as law (*opinio juris*).[281] Each element must be separately ascertained and requires an assessment of evidence.[282] The Law Commission confirmed that requirement of practice entails predominantly states' conduct in the exercise of their executive, legislative, judicial or other function.[283] The forms of state practice includes, *inter alia* 'diplomatic acts and correspondence, conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference, conduct in connection with treaties, executive conduct, including operational conduct 'on the ground', legislative and administrative acts and decisions of national courts'.[284] The requirement of *opinio juris* was explained by the ILC to mean that 'the practice in question must be undertaken with a sense of legal right or obligation'.[285] The forms of evidence of acceptance as law (*opinio juris*) include among others, 'public statements made on behalf of [s]tates, official publications government legal opinions, diplomatic correspondence, decisions of national courts, treaty provisions, and

[278] Stephen Hall, 'Researching International Law', in McConville, supra note 264.
[279] UN GA, Resolution 174(II), UN Doc A/Res/147(II) (21 November 1947).
[280] UN GA, International Law Commission, 'Identification of Customary International Law. Text of the Draft Conclusions Provisionally Adopted by the Drafting Committee', UN Doc A/CN.4/L.872 (30 May 2016). The text contains draft conclusions adopted by the Drafting Committee during the sixty-sixth (2014), sixty-seventy (2015) and sixty-eight (2016) sessions of the Commission.
[281] ibid, draft conclusion 2.
[282] ibid, draft conclusion 3.
[283] ibid, draft conclusions 4-5.
[284] ibid, draft conclusion 6.
[285] ibid, draft conclusion 9.

conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference'.[286]

The methodology in this thesis regarding how states approach the subject of governance of cyberspace, how international law applies to that domain, how to protect certain rights and resolve internet's future stewardship reflect the aforementioned forms of state practice and *opinion juris* articulated by the International Law Commission. To that end, a wide array of material was consulted in the process of the research of this study to ascertain the current trends in state practice. The sources used therein represent the official position of states individually, or collectively acting through a variety of international organizations. Examples of documents that were consulted included:

- speeches of heads of state or state officials;
- transcripts of governmental proceedings;
- domestic legislation;
- decisions of domestic courts and tribunals;
- press releases and communiques;
- policy statements;
- official manuals issued to state officials and armed forces.

Where official documents are not available, unofficial sources such as online newspaper reports and academic works have been used.

(c) Judicial Decisions

Article 38(1)(d) of the Statutes of the International Court of Justice provides that judicial decisions are amongst the 'subsidiary means for the determination of the rules of law'. Although judicial decisions are not themselves sources of law, they may be used to ascertain the existence and scope of rules sourced in treaties, custom and the general principles of law.[287] This study considered the jurisprudence of the most prominent tribunals, including the International Court of Justice, the European Court of Human Rights (ECHR), the Inter-American Court of Human Rights and the Human Rights Committee of the United Nations (HRC). The focus of the enquiry in this regard related in particular to the interpretation of the

[286] ibid, draft conclusion 10.
[287] ibid.

meaning and scope of the right to privacy and its application in the context of cyber surveillance practise of the Five Eyes states. Furthermore, the decisions of some courts, such as the ECHR may be influential on the way certain rights are interpreted by other human rights bodies, such a the HRC. They have also decisive impact on state practice, as being legally binding states must accept the court's view of international law and alter their behaviour accordingly. This is reflected in the *Asylum* case, where the ICJ remarked that:

> [i]t should be remembered […] that the decision in a particular case has deep repercussions, particularly in international law, because views which have been confirmed by that decision acquire quasi-legislative value, in spite of the legal principle to the effect that the decision has no binding force except between parties and in respect of that particular case.[288]

Consequently, the recent decisions of the ECHR and to some extent of the Court of Justice of the European Union discussed in Chapter 4 'The Right to Privacy', in relation to mass surveillance and data retention serve as a valuable guide in relation to the direction of the legal developments in this area.

(d) Teachings of Publicists

Article 38(1) of the Statutes of the International Court of Justice specifies that the teachings of the most highly qualified publicists of the various nations are also amongst the subsidiary means for the determination of the rules of law. These publications are not themselves sources of law, but may be used to ascertain the existence and scope of rules sourced in treaties, custom and the general principles of law. In the context of cyberspace one such source that this thesis makes a frequent reference to is the *Tallinn Manual 2.0*, referred to earlier in this chapter. The *Manual* is not an official document, but a product of two separate endeavours undertaken by Groups of Independent Experts acting in their personal capacity.[289] As such, it does not represent the view of its sponsoring nations, or NATO. However, it is an authoritative guide as to how international law applies to cyber operations, aimed at an objective re-statement of *lex lata*.[290]

[288] *Asylum case*, supra note 123.
[289] *The Tallinn Manual 2.0*, supra note 13, p. 2.
[290] ibid, p. 3.

(e) Acts of International Organizations

International organizations, such as the UN General Assembly or the Council of Europe provide forums within which international relations may be conducted. The International Law Commission Report on Identification of Customary Law states that 'a resolution adopted by an international organization or an an intergovernmental conference cannot, of itself create a rule of customary international law'.[291] It may however 'provide evidence for establishing the existence and content of a rule of customary international law, or contribute to its development'.[292] It may also 'reflect a rule of customary international law if it is established that the provision corresponds to a general practice that is accepted as law (*opinio juris*).[293] Accordingly, UN General Assembly resolutions do not generate rules, which form part of general international law, but nevertheless may help to create such rules.[294] In that sense, they and the acts of the regional organizations, such as the Council of Europe, may provide evidence of *opinio juris*. They may therefore contribute to the emergence of rules of customary international law binding on all states.[295] This study takes account of series of UN General Assembly resolutions, including those that were adopted by the Assembly shortly after the Snowden disclosures, such as the resolutions on the *Right to Privacy in the Digital Age.*[296]

(f) Soft Law

Soft law is described as 'any material which is not intended to generate, or is not per se capable of generating, legal rules but which may, nonetheless produce certain legal effects.'[297] The thesis considers a number of such non-legally binding instruments, including presidential declarations, UN GA resolutions, various guidelines and bilateral agreements, referred to throughout the thesis and discussed in more detail in Chapter 5 'International Legal Solutions'.

[291] International Law Commission, supra note 280, draft conclusion 12.
[292] ibid.
[293] ibid.
[294] Hall, supra note 278.
[295] ibid.
[296] supra note 9.
[297] Hall, supra note 278, p. 203.

These materials provided an indication of the likely future course of international law's development in the context of mass surveillance.

The research was conducted between 2013-2017 and was almost entirely contemporaneous with the legal and political developments in the area of cyber surveillance disclosures of Edward Snowden in 2013. It relied on the primary and secondary sources described above. The selection process of these sources reflected the manner in which international law is created. Where possible authoritative sources were consulted, which influenced particular research findings. A number of historical sources were also used, as the means of the background to the research (in particular in Chapters 2 and 3 relating to the internet governance discourse and cyber security matters).

The research findings were also influenced to some degree by the researcher's participation in a number of international conferences and exchanges in the field of cyber security attended between 2013-2017.

SCOPE OF THE THESIS

The thesis consists of six chapters.

Chapter 1, 'Introduction', introduces the topic, defines the main terms, sets out the legal framework and describes the methodology used.

Chapter 2, 'Cyberspace and Cybergeopolitics', forms the background to the thesis with an aim to illustrate the long standing political and ideological differences with regards to the future stewardship of the internet evidenced through the protracted internet governance discourse. The Chapter discusses the divergent policies to cybersecurity approaches by selected nations forming seemingly opposing sides, broadly represented by China and Russia on the one hand and the United States and most European countries on the other.

Chapter 3, 'The Role of International Law in Cyberspace Regulation', builds on these findings and proceeds to analyse the international legal status of cyberspace. The Chapter's main conclusions are that this is an environment, in which states may not claim full sovereignty, but where nations can and do exercise sovereign rights. It is also not a global common under the existing international law regimes. The Chapter finds some similarities between this domain and international seas and applies by analogy the United Nation Law of the Sea Convention 1982 as a possible guide upon which to model a legally binding international

treaty. The rationale for doing so stems from the repeated calls from some states since the 1990s to codify the behaviour of states in cyberspace in a hard law instrument.

The calls from states, international organizations and civil society for the legal regulation of state behaviour, including ceasing mass cyber surveillance and better protection of online privacy intensified in the aftermath of Edward Snowden[298] disclosures of 2013. Chapter 4, 'Privacy in the Digital Age', focuses on the legality of state sponsored cyber surveillance and transborder access to non-publically available data with regards to the right to privacy of communications and data protection under the international and regional human rights treaties, namely the International Covenant on Civil and Political Rights 1966, Article 17 (ICCPR)[299]; the European Convention on Human Rights 1950, Article 8 (ECHR);[300] the Convention for the Protection of Individuals with Regard to Automatic Processing of Individual Data 1981, Article 5 (Convention 108)[301] and the American Convention on Human Rights 1969, Article 9 (the Pact of San Jose).[302] The subjects of enquiry are the intelligence and law enforcement agencies of the Five Eyes alliance. The Chapter finds that both these activities breach the right to privacy of communications of the individuals located within the territories of the intercepting states and foreigners outside state borders. This supports the need to clarify in what circumstances and how would states be liable for their violations of that right.

In light of the increased wave of terrorist attacks in the recent years, the practice of states shows growing tendencies for deploying more surveillance powers to conduct domestic and extraterritorial surveillance at the expense of civil liberties, particularly the right to privacy. However, achieving an international consensus for a cyber treaty setting out 'the rules of the road', which could also curtail cyber surveillance and protect online privacy, seems elusive. This is the subject of discussion in Chapter 5, 'International Legal Solutions to State Mass Surveillance'. The Chapter recognizes that hard law global solution at this stage is unlikely. Focusing on the right to privacy, this Chapter considers other options, including (a) regional multilateral treaty put forward by the Council of Europe (CoE); (b) the expanding of the reach

---

[298] BBC News, 'Edward Snowden: Leaks That Exposed US Spy Programme' (17 January 2014) < http://www.bbc.co.uk/news/world-us-canada-23123964>.

[299] International Covenant on Civil and Political Rights, supra note 62, art. 17.

[300] Convention for the Protection of Human Rights and Fundamental Freedoms, supra note 62, art. 8.

[301] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Individual Data, (28 January 1981) ETS 108, entered into force 1 October 1985, art. 5.

[302] American Convention on Human Rights, surpa note art. 9.

of the recently modernized Convention 108 beyond Europe (c) modernizing and supplementing the already existing legal framework contained in Article 17 ICCPR and Article 8 ECHR and (d) a number of soft law options.

The concluding Chapter 6 summarises the findings. Edward Snowden revelations of 2013 brought into the sharp focus the persistent and sustained state practice of conducting cyber surveillance *en masse*. Some of the means employed, such as the use of the PRISM and Upstream programs, received legislative approval. Others, such as Tempora have not been officially acknowledged by the authorities, but continue unabated. This thesis demonstrated that even those surveillance programmes that received legislative attention and control are unlawful, as they almost certainly breach the right to privacy under international human rights treaties. Governments of many states emphasise that bulk intelligence gathering, pursuant to more draconian legislative powers would facilitate greater success in pursuing their national security goals. However, doubts exist as to the operational utility of these programmes. Consequently, there can be no doubt that the right to privacy of communications online and data privacy require a concerted effort from the international community. This process will most likely be incremental and facilitated by informal agreements, diplomatic channels and bringing the existing international laws up to date. The chapter does not dismiss the need for an international legally binding instrument, in a form of either a cyber treaty modelled on the UNCLOS 1982, or a separate privacy treaty for the digital domain. However, it takes the realistic approach, concluding that such a solution will depend on a number of factors, not least of which is the political will of states as primary law makers.

Chapter 2: 'Cyberspace and Cybergeopolitics'

INTRODUCTION

With the significant rise in civilian and military functions conducted in cyberspace, the idea that this domain needs governance has increasingly gained consensus among the international community, especially in the light of the proliferation of deleterious activities, from cyber crime, attacks on cyber infrastructure, exploitation of cyber systems to unsolicited emails (spam). Equally, states recognized that this threat cannot be adequately dealt with by any single nation acting alone, as 'cyberspace extends far beyond the domain of internal affairs of any state'.[303] The need for a framework for effective international cooperation on matters relating to cyber security[304] is beyond doubt and the work undertaken by intergovernmental bodies, such as the United Nations (UN) reflects this reality.[305] Although international law is the obvious mechanism[306] to regulate states' cyber behaviour, thus far very few specific rules exist. The discussion regarding the management of cyberspace and in particular the internet began in the 1990s, at the time of the early technological developments of this facility. It focused on whether the internet is susceptible to any form of state regulation. With the growing state practice showing the trend to shape and constrain behaviour in cyberspace within their jurisdictions for strategic, security and political ends this debate no longer plays a significant role. Cyberspace can and is subject to state regulation and the major players now deliberate how exactly to achieve this. To that end, a UN Group of Government Experts (UN GGE) representing 15 United Nations member states, including the People's Republic of China

[303] Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law Makers', (2017) Leiden Journal of International Law.
[304] UN ITU-T X 1205, 'Overview of Cyber-security',< https://www.itu.int/rec/T-REC-X.1205-200804-I>. The ITU defines cyber security to mean 'the collection of tools, policies, security concepts security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets'.
[305] Michael N. Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms' in Anna Maria Osula and Henry Rõigas (eds.), *International Cyber Norms: Legal, Policy and Industry Perspectives* (NATO CCD COE Publications, Tallinn 2016), 23-47, p. 23.
[306] ibid.

(China), the Russian Federation (Russia) and the United States (US), reached an agreement that international law applies to that domain in non-legally binding reports submitted to the UN General Assembly in 2013 and 2015.[307] However, despite reaching this broad agreement, it remains uncertain how international law applies. One aspect of this uncertainty is the lack of consensus regarding an adoption of a hard law international treaty for cyberspace, despite a number of proposals from some states. This lack of agreement among states has been further exacerbated following the 2013 Edward Snowden disclosures regarding mass cyber surveillance, which reinforced political distrust and led to many states and international organizations condemning these practices and calling for greater protection of human rights in cyberspace. Consequently, the codification of the applicable rules in a binding treaty remains the subject of much contention, whilst the development of specific customary law rules seems elusive.

The purpose of this chapter is to provide a background to the thesis by outlining the historical and current geopolitical dynamics of cyberspace governance and approaches to cyber security in order to discuss in more detail the way forward relating to the stewardship of this domain in Chapter 5 of this study. This chapter consists of two parts. Part one outlines cyber security approaches of selected 'cyber powers', represented by the United States and some European countries on the one hand and Russia/China on the other hand. This part discusses the ideological and cultural divergence in their approaches to the management of this domain both on the domestic and international levels, encapsulated by the multistakeholder and sovereignist models. This to some extent, explains the the lack of agreement in the sphere of internet governance and cyber security. This in part accounts for the continued lack of consensus regarding the adoption of a multilateral treaty and the emergence of clear customary international law rules. This part of the chapter goes on to highlight the tendencies in state practice towards greater assertion of control over the activities in cyberspace. One recent example of this trend (discussed in more detail on Chapter 5 of this thesis) is the calls for a European-only communication network in the aftermath of the 2013 Edward Snowden disclosures with an aim of having a technical infrastructure for online communications on the

[307] UN GA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/68/98 (24 June 2013), para 19; UN GA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015).

European soil to ensure the legal protection of data against foreign abuse.[308] Such quests for separation lead in part two to engage with the fundamental question related to the legal status of this domain under international law. Thus, this part first asks whether states can claim full sovereignty over cyberspace *per se*, or any part therein. It concludes that asserting full sovereignty over the entire cyberspace by any given state is not possible,[309] but that states may and do exercise territorial and extraterritorial jurisdiction over cyberspace activities.[310] By examining the current trends in state practice in the context of prescriptive, enforcement and judicial jurisdiction, part two lays down the theoretical foundations for discussing in Chapter 3 how to achieve the balance between national interests and the assurance that the internet remains an open medium of communication in years to come.

1. CYBERSPACE AND THE 'CYBERGEOPOLITICS' OF GLOBAL INTERNET GOVERNANCE

(a) Cyber Security Dimensions

With increased recognition of the importance of globally interconnected electronic communications, the economic wealth it helps to create, political stakes involved, not to mention the threat derived from hostile cyber operations, the international community has become engrossed in the debate regarding the future of cyberspace and challenges posed to national security.[311] Threats of cyber attack[312] attributed to the ease and relatively low cost of inflicting harm on the functionality of computer-operated physical infrastructures by a variety of actors (such as, hackers, ideologically motivated individuals, states, criminal and terrorist

[308] Uta Kohl, 'Jurisdiction in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and Cyberspace,* (Edward Elgar Publishing 2015), 30-55, p. 53.
[309] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) Rule 1, p.13.
[310] ibid, Rule 8.
[311] The nature, brief history and the current trends in internet governance will be discussed below in this chapter.
[312] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014). Roscini defines cyber attack as the 'cyber operations, whether in offence or in defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system, or network', p. 17.

organizations) exposes the vulnerabilities of most nations, even those with superior military power.[313] Although extreme scenarios of deleterious cyber operations have not yet occurred,[314] several states were subjected to cyber attack, of which other states were suspected as the instigators.[315] One of the earliest examples was the June 1982 gas pipeline explosion in Siberia, as a result of an alleged logic bomb installed in the computer system by the US Central Intelligence Agency.[316] Other such high profile cyber operations include the 2007 denial of service attacks on Estonia, which lasted over a month, but did not result in loss of life, cause material damage, or injury.[317] The release of the Stuxnext worm in 2010 on Iran's industrial infrastructure with the alleged purpose of sabotaging the Natanz uranium facility[318] has been described as 'the first and so far only known use of malicious software designed to cause material damage by attacking the Supervisory Control and Data Acquisition (SCADA) system of a national critical infrastructure'.[319] In November 2014 a group calling itself 'Guardian of Peace', allegedly from North Korea, hacked Sony Pictures demanding the withdrawal from public release Sony's North Korean comedy, 'The Interview'. The incident was described by James Clapper, the US Director of National Intelligence, as 'the most serious cyber attack ever made against US interests'.[320] There are other documented cases, where the deployment of cyber operations were used in connection with and in aid of military campaigns or armed conflicts, for example against Georgia in 2008.[321] These instances show that the internet, designed to be borderless, is a means by which benevolent, or malevolent, actions taken in one

[313] ibid, p. 2
[314] Thomas Rid, *Cyberwar Will Not Take Place*, (C Hurt & Co. Publishers 2013).
[315] Roscini, supra note 10, p. 4
[316] ibid.
[317] ibid; This attack resulted in the shutting down government websites, newspapers, TV stations, banks and other targets and involved over a million computers based in more than 100 countries hijacked and lined through the use of bootnets.
[318] ibid.
[319] ibid, p. 6
[320] Oliver Langhland, 'FBI Director Stands by Claim that North Korea was Source of Sony Cyber Attack', *The Guardian* (7 January 2015) <http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey>. The attack involved thousands of documents published on line including personal email correspondence, employees' personal data, executive pay and unreleased films and scripts.
[321] Roscini, supra note 10. Cyber operations against Georgia were conducted before and during the armed conflict with the Russian Federation and included causing government websites to go off-line, defacement and replacing content with anti-Georgian propaganda, together with carrying out Denial of Service Attacks.

country will have an outcome in another without the user ever having left their own country.[322] There can therefore be no doubt that the need for international cooperation in handling cyber security is not only desirable, but increasingly necessary, as cyber threats are serious, growing and destabilizing.[323]

So widespread is the concern amongst the international community that since 1998 the UN General Assembly began adopting annual resolutions,[324] highlighting that information technologies 'can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security'.[325] In addition and also as a result of these concerns, a number of United Nations Groups of Governmental Experts (UN GGE) were established with the purpose of examining threats in cyberspace and how to cooperatively address them.[326] As a consequence, the GGE reached of a broad agreement that international law and in particular the Charter of the United Nations is applicable in cyberspace.[327] Other organizations have become increasingly engaged with cyber security issues too, including the Organization for the Security and Cooperation in Europe, which in 2010 Astana Commemorative Declaration recognized cyber threats, as one of the 'emerging trans-national threats'.[328] In 2008 North Atlantic Treaty Organization's (NATO) set up Cooperative Cyber Defence Centre of Excellence (CCD COE) accredited with full status of international military organization and in 2010 issued *New Strategic Concept,* which acknowledged the damage that can be inflicted as a result of cyber attack.[329]

---

[322] Tim Maurer, 'Cyber Norm Emergence at the United Nations- An Analysis of the Activities at the UN Regarding Cyber-Security', Belfer Center for Science and International Affairs, (September 2011) <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.

[323] Nazli Choucri and Daniel Goldsmith, 'Lost in Cyberspace: Harnessing the Internet, International Relations and Global Security', (2012) 68(2) Bulletin of the Atomic Scientists, <http://thebulletin.sagepub.com>.

[324] Roscini supra note 10, p. 2. Among them UN GA Resolution 55/28 (20 November 2000); 56/19 (29 November 2001); 59/61 (3 December 2005); 61/54 (6 December 2006); 62/17 (5 December 2007); 63/37 (2 December 2008); 64/24 (2 December 2009); 65/41 (8 December 2010); 66/24 (2 December 2011); 67/27 (3 December 2012).

[325] ibid.

[326] UN GGE Reports, supra note 5.

[327] ibid.

[328] Roscini, supra note 10.

[329] NATO, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by the Heads of State and Government at the NATO Summit in Lisbon (19-20 November 2010) <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf >.

To date there is no all encompassing international law treaty specifically dealing with threats to cybersecurity, or a uniform states' agreement of *opinio juris* capable of forming the basis of customary international law in this area. However, as already mentioned, there is a generally accepted states' view that international law applies to cyberspace operations.[330] There are also a number of regional treaties that provide a 'patchwork of regulations' for cyberspace activities.[331] Among them are the 1992 Constitution of the International Telecommunications Union,[332] Council of Europe 2001 Convention on Cybercrime (the Budapest Convention),[333] the 2009 Shanghai Cooperation Organization's Information Security Agreement (the Yekaterinburg Agreement)[334] and the African Union Convention on Cyber Security and Personal Data Protection.[335] These international agreements, albeit important in their own right, have their limitations.[336] For example, the Budapest Convention aims to meet challenges of fighting cyber crimes, such as online fraud, copyright infringement and child pornography by harmonizing national laws, improving investigative techniques and increasing cooperation among states. However, the Convention excludes from its scope of application 'conduct undertaken pursuant to lawful government authority'[337] and therefore does not apply to cyber operations conducted by states.[338] To date, forty-five states have ratified the Convention, including non-Council of Europe members, such as Australia, Japan and the United States.[339] Other legal instruments, such as the Yekaterinburg Agreement and the African Union Convention on Cyber Security have either very limited membership (the

[330] UN GGE Reports, supra note 5.
[331] Mačák, supra note 1.
[332] Constitution of the International Telecommunications Union, 1825 UNTS 143 (1992).
[333] Council of Europe, Convention on Cybercrime (March 2002) 41 ILM 282.
[334] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (16 June 2009) < http://cis-legislation.com/document.fwx?rgn=28340>.
[335] African Union Convention on Cyber Security and Personal Data Protection, (2014) EX.CL/846(XXV).
[336] Mačák, supra note 1.
[337] Cyber Crime Convention, Explanatory Report, para 38 <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>.
[338] Roscini, supra note 10, p. 19.
[339] Treaty Office, Council of Europe, Status Report on Convention on Cybercrime, Council of Europe, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

Yekaterinburg Agreement),[340] or have not yet come into force (the African Union Convention).[341]

The reluctance of states to codify the applicable rules in a comprehensive multilateral treaty is well documented.[342] A number of unsuccessful attempts have been made since 1996 with France putting forward an early proposal titled *Charter for International Cooperation on the Internet*.[343] Subsequent endeavours also failed with the Shanghai Cooperation Organization submitting to the UN General Assembly a *Code of Conduct for Information Security* in 2011 and 2015.[344] Thus far, none of these proposals have been embraced with enthusiasm by other states[345] and the unwillingness to commit to an international treaty been further fuelled by the distrust generated by the 2013 Snowden disclosures.[346]

Equally, states seem reluctant to contribute towards the development of cyber-specific customary international rules.[347] Many countries have issued cyber security defence documents, some of which contain references to international law and therefore are 'not only helpful as an assistance in treaty interpretation, but can also be evidence of state practice and could declare and seek to impose on those who are subject to its guidance, a certain *attitude* to the law, or an *interpretation* of the law, or an operational *intent* that relates to existing law either supportively or in some problematic way'.[348] However, judging from the official attitudes to cyber security outlined below by the 'cyber powers' represented by the US and its allies on the one hand (broadly termed the 'West') and China, Russian and other like minded states on the other hand (the 'East'), it soon becomes apparent why a clear *opinio juris* on matters relating to cyber security is not easily ascertainable and thus far failed to crystalize.

---

[340] Mačák, supra note 1.
[341] African Union Convention, supra note 33, art 34.
[342] See for example, Kristine Eichensehr, 'The Cyber-Law of Nations' (2015) 103 Georgetown Law Journal, 317; Mačák, supra note 1; Onna Hathaway, et al., 'The Law of Cyber Attack' (2012) 100 California Law Review 817.
[343] Mačák, supra note 1.
[344] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, UN Doc A/66/358, (14 September 2011); Letter dated 9 January 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, UN Doc 69/723 (13 January 2015).
[345] Mačák, supra note 1.
[346] The prospects of states engaging in this form of law making and what role may the human rights play will be discussed in more detail in Chapter 5 of this thesis.
[347] supra note 1.
[348] Roscini, supra note 10, p. 27

Generally, in order to determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is state practice that is accepted as law (*opinio juris*).[349] This includes taking into account the evidence of the contrary practice of states that does not support the purported rule.[350] The divergent approaches of states discussed in the next part of this chapter also to some extent explain the reasons for the inability to adopt an 'omnibus' treaty in the near future. To illustrate these conflicting attitudes to cyberspace public statements made on behalf of these states, official cyber security documents and other forms of evidence will be outlined below to show the rivalry among the major powers relating to the principles that should govern not only international cyber security law, but also the issues related to internet governance.

(i) Cyber Security Approaches of the 'West'

The US has been described as the 'only one' cyber superpower in the world[351] and since 1999 has been prolific in its production of official documents on cyber security matters.[352] The US attitude to cyberspace generally and to the internet in particular are broadly representative of the other states comprising the Five Eyes alliance. These could be encapsulated in one phrase, that is 'internet freedom', which was first introduced by the then Secretary of State,

[349] International Law Commission, Identification of Customary International Law, UN Doc A/CN.4/L/872 (30 May 2016).
[350] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion (1996) ICJ 311, p. 311-12.
[351] Kenneth Geers, 'Pandemonium: Nation States, National Security and the Internet', The Tallinn Papers, (2014) NATO CCD COE Publications on Strategic Cyber Security, Vo. 1 No. 1 < https://ccdcoe.org/publications/TP_Vol1No1_Geers.pdf>.
[352] These include: (1) US Department of Defence, 'An Assessment of International Legal Issues in Information Operations', (May 1999) <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>; (2) Chairman of the Joint Chiefs of Staff, 'The National Military Strategy for Cyberspace Operations', (December 2006) <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>; (3) Department of Defence, 'Strategy for Operating in Cyberspace', (July 2011)< http://www.defense.gov/news/d20110714cyber.pdf>; (4) US Department of the Air Force, 'Cornerstones of Information Warfare', (17 April 1997) <http://www.dtic.mil./cgi-bin/GetTRDoc?AD=ADA323807>; (5) 'Cyberspace Operations Air Force Doctrine Document 3-12' (15 July 2010), which on p. 49 sets out doctrine of cyberspace operations <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-060.pdf>; (6) White House, 'Information Operations, Joint Publication 3-13'(27 November 2012) <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>; (7) 'The National Strategy to Secure Cyberspace'(February 2003) <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>.

Hilary Clinton in her speech of that title in 2010.[353] Secretary Clinton called cyberspace a 'global network common' and remarked, *inter alia*, that 'the [US] stands for a single internet, where all humanity has equal access to knowledge and ideas'. [354] These views were subsequently echoed by the Obama Administration in the 2011 *International Strategy for Cyberspace: Prosperity Security and Openness in a Networked World* (International Strategy 2011).[355] The document sought to establish its normative perspective for cyberspace as a global political space and to that end, stated that the US government's main goal in cyberspace is to:

> work internationally to promote an open, interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security and fosters free expression and innovation. To achieve that goal, [the administration] will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships and support the rule of law in cyberspace.[356]

It could be said that the *International Strategy 2011* is representative of the US views regarding cyberspace as it unveiled that country's plans for the future of the domain. At the forefront of this vision was that cyberspace, viewed as a global political space is to be governed by the rule of law. At the core of the administration's international cyberspace policy was the commitment to fundamental freedoms (freedom of expression and association, to receive and impart information and ideas through any medium and regardless of frontiers)[357], privacy, the free flow of information,[358] respect for property, protecting from crime and the right of self-defense.[359] Preserving global network functionality and improving cyber security featured strongly, in addition to ensuring that in future cyberspace is globally interoperable, with stable

---

[353] Hilary Rodham Clinton, 'Remarks on Internet Freedom', US Department of State, (2010) < http://www.cfr.org/internet-policy/clintons-speech-internet-freedom-january-2010/p21253 >.
[354] ibid.
[355] US White House, *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked Wold* (May 2011) <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.
[356] ibid p. 8.
[357] ibid
[358] ibid p. 5
[359] ibid p. 10

networks and reliable access. The administration's vision regarding its future governance was unequivocally based on continuing with the multistakeholder model (described in more detail elsewhere in this chapter), which the document states, is not limited to governments, but includes appropriate stakeholders.[360] *International Strategy 2011* made several references to the need for the 'rule of law' in cyberspace domestically and internationally.[361] The 'rule of law' was defined in the report, as 'a civil order in which fidelity to laws safeguards people and interests; brings stability to global markets; and holds malevolent actors to account internationally'.[362] The stability that the *International Strategy* referred to should be achieved through norms of behaviour,[363] or as the document put it, 'an environment of expectations that ground foreign and defense policies and guide international partnerships'.[364] Furthermore, it expressly referred to the role that international law should play in this domain, stating that:

> [t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state [behavior], in times of peace and conflict, also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step is such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace. [365]

Thus, the ideological thrust of the *International Strategy* could be summarized as an attempt to marry protecting national security interests in cyberspace with upholding fundamental freedoms, through close international cooperation and consensus building through norms. It also illustrates the reluctance to contribute to the articulation of cyber-specific customary law rules, seemingly preferring to enhance the development of customary law through promoting the development of international cyber norms. Similar attitudes were also expressed in the 2011 US Department of Defense *Cyberspace Policy Report,* according to which:

[360] ibid p. 10
[361] ibid p. 3 and 5
[362] ibid p. 5
[363] ibid p. 9
[364] ibid.
[365] ibid.

> [t]he United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of US policy, long standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarification in certain areas.[366]

This trend is also discernable from the 2015 US *Law of War Manual* 2015 as supplemented by its 2016 version.[367] The Manual addressed, *inter alia*, how the law of war principles and rules apply to relatively novel cyber capabilities and the cyber domain.[368] It observed that:

> [a]s a matter of US policy, the United States has sought to work internationally to clarify how existing international law and norms, including the law of war principles apply to cyber operations.[369]

In the words of one commentator, the Manual is 'a representative example of another missed opportunity to steer the development of cyber custom' as it 'skirts virtually all of the unsettled issues, including standards of attribution, rules of targeting or the requirement to review cyber weapons.'[370] It is true to say that law and norms are very closely related concepts in international law and inter-state agreements on norms may incrementally influence the development of the law.[371] Nevertheless, a crucial difference is that a violation of a binding rule of international law gives rise to international legal responsibility,[372] whilst the same

---

[366] US Department of Defence, 'Department of Defence Cyberspace Policy Report: A Report to Congress Pursuant to the National Defence Authorisation Act for the Fiscal Year 2011' (November 2011), Section 934, p. 78.
[367] US Department of Defence, Office of the General Counsel, *Law of War Manual* (2016) <https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.
[368] ibid, chapter 16.
[369] ibid.
[370] Mačák, supra note 1.
[371] ibid.
[372] International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, 2001 YILC, Vol. 53 II (Part Two), art. 1.

cannot be said of non-legally binding norms regulating cyber conduct.[373]

The United Kingdom 2011 *Cyber Security Strategy. Protecting and Promoting the UK in a Digital World*[374] by and large reflects these themes. The UK vision for cyber security in 2015 is:

> […] for UK to drive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and strong society.[375]

The UK government, having recognized the 'limits of its competence in cyberspace'[376] and the fact that much of the infrastructure it needs to protect is owned and operated by the private sector, specifically stated that the expertise and innovation required to keep pace with the threat will be business-driven.[377] The document also acknowledged the need to seek partnership with other countries to improve defense in view of the fact that the internet is fundamentally transnational and dependent on the infrastructure not entirely based in the UK. References were made to the role and protection of human rights, in particular the right to privacy, in the context of pursuing cyber security policies that enhance individual and collective security. To achieve these set goals, the *Strategy* urged everyone, that is the private sector, individuals and government to work together.[378] Nevertheless, the subsequent UK *National Cyber Security Strategy 2016-2021*[379] (Cyber Strategy 2016) recognized that the approach taken in the 2011 National Cyber Security Strategy 'has not achieved the sale and pace of change required to stay ahead of the fast moving threat'.[380] The UK government's vision for 2021 is that 'the UK

---

[373] supra note 1.
[374] UK HM Government, *UK Cyber Security Strategy, Protecting and Promoting the UK in the Digital World* (November 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf >.
[375] ibid p. 8.
[376] ibid p. 22.
[377] ibid.
[378] ibid.
[379] UK HM Government, *National Cyber Security Strategy 2016-2021* (2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf >.
[380] ibid, para 1.3, p. 7.

is secure and resilient to cyber threats, prosperous and confident in the digital world'.[381] In order to realize this vision, the government will work to defend against cyber threats, deter all forms of aggression in cyberspace and develop an innovative cyber security industry.[382] Cyber Strategy 2016 reiterated the need for international action and 'investment in partnerships that shape the global evolution of cyberspace in a manner that advances [the UK's] wider economic and security interests'.[383] The document recognized that international cooperation on cyber issues has become an essential part of wider global economic and security debates, which lacks a single agreed vision.[384] Importantly, the Strategy stated that:

> [t]he UK and its allies have been successful in ensuring some elements of the rules-based international system are in place: there has been agreement that international law applies to cyberspace; that human rights apply online as they do offline; and a broad consensus that the multi-stakeholder approach is the best way to manage the complexities of governing the [i]nternet. However, with a growing divide over how to address the common challenges of reconciling national security with individual rights and freedoms, any global consensus remains fragile.[385]

Among the objectives set in the Cyber Strategy 2016 is the 'safeguard[ing] of the long term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning the UK's national security'.[386] This will be achieved through, *inter alia*, 'UK […] continu[ing] to champion the multi-stakeholder model of internet governance [and] oppos[ing] data localization.'[387] The UK approach to achieve these ends rests, among other things, on 'strenghten[ing] and embedd[ing] a common understanding of responsible state behavior in cyberspace, build[ing] on agreement that international law applies in cyberspace, continu[ing] to promote the agreement of *voluntary, non-binding, norms of responsible state behavior* and *suppor[ting] the development and implementation of confidence building measures* [emphasis added]'.[388]

---

[381] ibid, para 1.4, p. 7.
[382] Ibid, para 1.5, p. 7.
[383] ibid, para 1.6, p. 7.
[384] ibid, para 8.1, p. 61.
[385] ibid, para 8.2, p. 61.
[386] ibid, para 8.3, p. 61.
[387] ibid.
[388] ibid, para 8.4, p. 61.

In summary, the policy pronouncements regarding cyber security matters of the United States, also echoed by the other Five Eyes partners such as the UK, can be viewed as (a) the continued promotion of the internet as an open environment, where information can flow unimpeded among jurisdictions; (b) a policy stance, according to which international customary law rules apply to cyberspace operations and therefore there is no need to invent new rules and (c) the belief that any additional rules would be developed through voluntary, non-legally binding norms and confidence building measures.

(ii) The 'Eastern' Approaches to Cyber Security

- The Russian Federation

Non-Western states seem to be taking a rather different view, when it comes to defining cyberspace, cyber security policies and the overall approach to its future governance. Whilst the Western governments tend to use the term 'cyberspace', Russian and Chinese sources refer to it as 'information space'.[389] The term 'information space' is featured in such Russian documents as *Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020*[390] and the 2011 *Draft Convention on International Information on Security* (Draft Convention).[391] The phrase has also been used in the *Draft International Code of Conduct for Information Security 2011*,[392] a document submitted to the United Nations by China, Russia and other countries, which having been rejected by the US, was re-drafted and re-submitted in 2015.[393] The Russian 2011 *Draft Convention on International Information on Security*,[394] an official government document released at an international meeting of high-ranking officials responsible for security matters in

---

[390] The Government of the Russian Federation, 'Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020', <https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>.
[391] The Government of the Russian Federation, *Draft Convention on International Information Security* (28 October 2011) <http://rusemb.org.uk/policycontact/52/>.

[392] UN GA 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General', supra note 43.

[393] ibid.
[394] *Draft Convention on International Information Security*, supra note 89.

Yekaterinburg, defines 'information space', as 'the sphere of activity connected with the formation, creation, conversion, transfer, use and storage of information infrastructure and information itself'.[395] It considers 'information security', as the 'protection of [Russia's] national interests in the information sphere defined by the totality of balanced interests of the individual, society and the state'.[396] The 2011 *Draft Convention* contains 23 issues of concern to Russia in that environment, some of which run counter to the views on the use and governance of the internet championed by the Western states. The fundamental points of divergence are that Russia perceives free flow of information content as a threat. This can be gleaned from Article 4, which lists 'main threats to international peace and security in the information sphere'. Among them Art 4(8) considers the following, as one of such dangers:

> [t]he manipulation of the flow of information in the information space of other governments, disinformation, or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical and aesthetic value.[397]

Conversely, both the US and the UK are strong advocates of free information flow. The already referred to United States *International Strategy for Cyberspace* for instance, pledges that the US will 'prioritize openness and innovation on the internet' in contrast to governments that 'place arbitrary restrictions on the free flow of information or use it to suppress dissent or opposition activities'.[398] The UK is in broad consensus with this view. For example, in 2011 the then Foreign Secretary William Hague remarked in the London International Conference on Cyberspace that 'cyberspace remains open to innovation and the free flow of ideas, information and expression'.[399]

Another important point of disagreement is the idea that the Russians view information technologies as (Western) weapons, which could potentially challenge state sovereignty by causing social and political instability. The idea of 'internet sovereignty', which percolates

---

[395] ibid.
[396] Ministry of the Foreign Affairs of the Russian Federation, 'National Security Concept of the Russian Federation' (2000), <http://www.mid.ru/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b?OpenDocument.>
[397] supra note 89, art 4(8).
[398] US White House, *International Strategy for Cyberspace*, supra note 53, p.21.
[399] William Hague, 'Chair Statement' (2 November 2011) <http://www.fco.gov.uk/en/news/latest-news/?view=PeressS&id=68566382>.

throughout the *Draft Convention*, illustrates how deeply divided are the views of these two opposing sides. This is *inter alia*, reflected in Article 5(5) of the 2011 Draft Convention, which states that:

> [e]ach state party has the right to make sovereign norms and govern its information space according to its national laws. Its sovereignty and laws apply to the information infrastructure located in the territory of the state party or otherwise falling under its jurisdiction. The state parties must strive to harmonize national legislation, the differences whereof must not create barriers on the road to a reliable and secure information space.[400]

The idea of national control of all internet resources within states' physical borders and the associated concept of application of local legislation,[401] seems in conflict with the US approach annunciated for example, by the US Secretary of State Clinton, who in her speech of December 2011, stated that countries such as Russia wish to:

> [e]mpower each individual government to make their own rules for the internet that not only undermine human rights and the free flow of information but also the interoperability of the network. In effect, the governments pushing this agenda want to create national barriers in cyberspace. This approach would be disastrous for internet freedom.[402]

- The People's Republic of China

China has the largest population in the world and with 721 million internet users and has become increasingly dependent on various cyber assets.[403] With this increased dependency,

---

[400] Draft Convention on International Information Security, supra note 89, art 5- 'Main Principles of Ensuring International Information Security'.
[401] Keir Giles, 'Russia's Public Stance on Cyberspace Issues' (2012) NATO CCD COE <https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf>.
[402] Clinton, supra note 51.
[403] Mikk Raud, 'China and Cyber: Attitudes, Strategies, Organization' (2016) NATO CCD COE <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf>.

Chinese authorities began placing growing emphasis on cyber security measures.[404] However, China has not established an exhaustive approach to cyber issues in the form of a strategy clearly outlining the country's cyber objectives and their execution.[405] Instead, the Chinese domestic approach is characterized by complex hierarchies, command structures and various defence papers.[406]

Generally, it could be said that the Chinese understand matters relating to cyber activities as something strongly integrated within society and do not separate them from the general flow of governance.[407] Uncontrolled information is perceived as a threat to the regime and ever since the internet became publically available the question was not whether to control it, but how.[408] Consequently, the internet is built with this in mind through real-time censorship, which sharply contrasts with the idea of 'internet freedom' held by the West.[409] In addition, the Chinese government are sensitive about foreign information systems and believe that the technology that originates from the West is equipped with Trojan horses and loopholes to steal China's national secrets and prevent its economic upsurge.[410] As a result of these concerns, not only is the development and supply of high quality home grown products encouraged, but heavy controls have been imposed over the information security industry deterring foreign investors, especially from the US from seeking business opportunities in China.[411]

To appreciate the divergence in approaching cyber related issues, a useful illustration is the difference in the terminology used by China. In similar vein to the Russians, the Chinese also tend to use the phrase 'information space' rather than cyberspace[412] and consider that:

> [t]he main function of the information space [is] for people to acquire and process data […] a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases and information, forming a 'landscape' huge,

[404] ibid, p. 5.
[405] ibid.
[406] ibid.
[407] ibid.
[408] ibid, p. 6.
[409] ibid.
[410] ibid.
[411] ibid.
[412] H. B Wasuo, *Information Space* (Shanghai: Translation Publishing House 2000) in Giles and Hagestad II, 'Divided by Common Language: Cyber Definitions in Chinese, Russian and English', 5th International Conference on Cyber Conflict 2013, (2013) NATO CCD COE <http://ccdcoe.org/publications/2013proceedngs/d3r1s1_giles.pdf.>

interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space'.[413]

The Western approach holds cyberspace as a global domain covering the use of electronics, interdependent networks of information technology infrastructure including the internet and other telecommunication networks and data. In contrast, the Chinese understand cyberspace as only a subset of information space-the landscape for the largest scale communication to the world's population, which includes human information processing and cognitive space.[414] Consequently, the Chinese regard 'information space' and 'information security' holistically, unlike Western governments, who tend to approach cyberspace and cyber security separately.[415]

The main cyber security related policy goals and national strategies were first published in 2003 (the so-called Document 27) by the State Network and Information Security Coordination Small Group.[416] The Document laid foundations for formulating the necessary national cyber security policies in relation to, *inter alia*, disaster recovery, incident management and e-government security plan.[417] At its core, the Document had the concept of 'active defence', that is attacking only after receiving an attack.[418] Its aims included the protection of critical infrastructure, enhancing encryption and dynamic monitoring, together with the improving of the indigenous innovation.[419] Since 2006 all of the country's information security strategies can be linked to the 15-year grand strategy for future innovation, titled 'The National Programme for the Development of Science and Technology in the Medium and Long Term 2006-2020' (the National Strategy) issued by the State Council.[420] The document is widely perceived as a cornerstone of China's overall standardization policy and includes the protection of the internet against harmful activities directed against, or having the effect of

[413] Giles and Hagestad II, ibid p. 7.
[414] ibid.
[415] ibid.
[416] Raud, supra note 101, p. 11. This was issued in the so-called Document 27: Options for Strengthening Information Security Assurance Work (2003).
[417] ibid.
[418] Dennis Blasko, 'The Evolution of Core Concepts: People's War, Active Defence and Offshore Defence', in Raud supra note 91.
[419] ibid
[420] ibid.

undermining national security or commercial, social and individual interests.[421] To achieve these ends, a state must be able to defend itself and the society, compete fairly and productively in the national and global economic order and preserve social norms, privacy and security of the individual citizen.[422] In contrast to the Western approach, the Chinese regime places particularly strong emphasis on the challenges posed by cyber activities that threaten existing domestic social and political norms or values, such as the dissemination of false rumors, as well as the sovereignty of the nation state.[423] It is in this context that the major ideological differences lie. Thus, the Chinese authorities call for the establishment of sovereign 'virtual territory' on the internet termed 'cyber sovereignty',[424] advocating the need for a government to identify the boundaries of such a territory and protect it against cyber threats.[425] In this sense, the Chinese approach to cyber security and the administration of the internet is distinctly state-centric. This can be gleaned from the National Strategy,[426] as it made security and protection of information technology a national priority. The State Council's focus is on all information technologies, suppliers and infrastructures, civilian and military alike, including the People's Liberation Army.[427] It is a top-down, proactive and holistic governmental approach, aimed at protecting commercial enterprises and governmental entities by giving detailed instructions to civilians and government leaders as to what and how to protect information networks and the importance this plays in the overall State Council plan.[428] The recognition that the 'strategic significance of the internet lies in the fact that it has become an effective tool that transgresses national boundaries, communicates information worldwide and influences international and domestic affairs',[429] reinforces long standing Chinese concerns with social disorder and therefore the need for a strong, supervisory state to uphold societal norms and preserve social

---

[421] Micheal D. Swaine, 'Chinese Views on Cyber Security in Foreign Relations' 42 Leadership Monitor (30 July 2013) <http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf >.
[422] ibid.
[423] ibid.
[424] For example, Zhong Sheng, "Fill in 'Regulation Blank' in Cyberspace", *People's Daily,* July 9 2013.
[425] Swaine, supra note 119.
[426] Gu Fa, 'State Council Vigorously Promotes the Development of Information Technology and to Effectively Protect the Information Security', (2012) http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm, in Giles and Hegestad II supra note 110.
[427] ibid.
[428] ibid.
[429] *Liberation Army Daily,* 'Experts Discuss Prospects of 'Cyber Defence' and National Defence' (4 January 2011).

harmony.[430] The idea of 'internet freedom', whereby information flows unrestricted is viewed with suspicion. This is reflected in the concerted effort undertaken by the Chinese authorities to impose controls over internet content collectively known as the Great Firewall of China. The ideological thrust of cyber security could therefore be summarized as the 'defense and expansion of socialist ideology and culture', whereby the internet in China must reflect socialist 'cyber culture' and resist 'ideological infiltration and political instigation'.[431] Furthermore, 'both quasi and non-authoritative Chinese sources state that the US dominance and *de facto* control over internet technologies and the cyber infrastructure is unfair, presenting a source of instability and potential danger for the global cyber system'.[432] This to some extent is reflected in the National Strategy, which supports 'techno-nationalism' by calling for China not to obtain any 'core technologies in key fields that affect the lifeblood of the national economy and national security', from abroad, including next generation internet technologies, digitally controlled machine tools and high-resolution earth observation systems.[433]

The subsequently issued State Council's 2012 New Policy Opinion (NPO), translated as '*The State Council vigorously promotes informatisation development and offers several options on conscientiously protecting information security*'[434] by and large reflects these themes. However, unlike the previous documents, the NPO links developments in information security with people's economic and social improvement.[435] The document comprehensively covers the majority of essential areas of cyber security and indicates the main weaknesses in China's information security mode, pointing out the increased vulnerabilities from growing dependence on the internet.[436] The hostility towards foreign technologies was not only reflected in the NPO but is now visible in the the new China's Cyber Security Law (discussed in more detail in Chapter 5 of this thesis), which took effect on 1st June 2017. It aims at heavily regulating the Chinese technology sector[437] and thus reinforces the concerns that that country's cyberspace will become increasingly isolated from the rest of the world in the coming years.

---

[430] Swaine, supra note 119.
[431] ibid.
[432] ibid.
[433] Raud supra note 101, p. 12.
[434] The State Council Information Office, New Policy Opinion (2012) <http://politics.gmw.cn./2012-07/17/content_4571519.htm.>
[435] Raud, supra note 101, p. 14.
[436] ibid.
[437] KPMG China, 'Overview of China's Cybersecurity Law' (2017) <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>

By 2014 the Chinese governments prioritizing information security led to the establishment of the Central Leading Small Group for Internet Security and Informatisation, a new body chaired by China's President Xi Jingping.[438] The President explained the necessity for the new body stating that 'no internet safety means no national security and no informatisation means no modernization,[439] subsequently also stating that internet security and information management are 'two wings of one bird, two wheels on one car'.[440] It could be said that Chinese approach to cyber security encapsulates the need to improve the security of the domestic internet infrastructure, to reinforce the move towards indigenous innovation detailed in the 15- year plan and for China to become the leading actor on the global stage by promoting an alternative attitude to internet governance.[441] The Chinese government's approach is perhaps best expressed in its 'Seven Baselines' doctrine for using the internet introduced in 2015.[442] It requires that whatever is expressed online must respect seven elements, namely laws and regulations, the socialist system, the country's national interests, citizens' lawful rights and interests, public order and accuracy.[443]

In summary, the Chinese, Russian and other like-minded states position regarding cyber policy can be summarized as (a) a distrust in the internet as a medium for free flow of information; (b) a belief that it is the role of the government to take control and safeguard domestic 'information space' and create a 'virtual territory', thus promulgating 'cyber sovereignty'; (c) regulation of state behavior through a hard law multilateral binding treaty, in contrast to the US, which sees the development of cyber law through norms.

The conclusion that can be reached is that the Western and the Eastern approaches to cyberspace and cyber security do not sufficiently align at this stage to contribute to the development and interpretation of customary international law. These domestic policies seem to pursue disparate goals both nationally and, as will be shown in the next part of this chapter, on an international plane. This disparity may be gleaned from different attitudes to defining the basic terms relating to cyberspace (including such phrases as, cyber space and cyber security),

[438] Raud, supra note 101, p. 15.
[439] *Xinhuanet*, 'Xi Jinping Leads Internet Security Group' (27 February 2014), in Raud supra note 101, p. 15.
[440] Raud, ibid.
[441] ibid.
[442] ibid.
[443] ibid.

which at least to some extent explains a conceptual gap in information security policy.[444] It could be said that these ideologies underpin the fundamental incompatibility to cyber security and are illustrative of a much broader and opposing philosophy to cyberspace generally, namely, centralized, state-centric government command and control by the Chinese and Russian authorities versus de-centralized, self-governing model by a variety of stakeholders upheld by the US and its allies. In that sense, they mirror the differences in political ideologies of the two systems, which is present in the on-going debate regarding the future of internet governance[445] discussed next.

(b) Internet Governance

If cyberspace is described as a domain for telecommunication, then the internet is 'the networked physical infrastructure of interconnected computers that allows information to move through cyberspace and the web is simply a service that runs on the internet'.[446] The encyclopaedic definition states that the internet is 'an association of computer networks with common standards, which enable messages to be sent from any host on one network to any host on any other.'[447] The internet was originally designed by American scientists and engineers as a tool for military communications. With the funding from the US government it became fully open to commercial use in 1995 and since that time almost all its infrastructure worldwide is owned by the private sector,[448] whilst its operations are primarily overseen by The Internet Corporation of Assigned Names and Numbers (ICANN), a non-profit

---

[444] Gilse and Hagestad II, supra note 110, p. 11.

[445] Micheal Muller, 'Net Neutrality as Global Principles for Internet Governance', Internet Governance Project, (5 November 2007) <http://www.internetgovernance.org/wordpress/wpcontent/uploads/NetNeutralityGlobalPrinciple.pdf .> The term 'governance' was described by Mueller as 'coordination and regulation of interdependent actors in the absence of an overarching political authority and gained popularity in international relations theory because it was weaker than the term 'government', whereas 'internet governance is 'an inclusive label for the ongoing set of disputes and deliberations over how the internet is coordinated, managed and shaped to reflect policies'.

[446] Lance Strate, 'The Varieties of Cyberspace: Problems of Definition and Delimitation' (1999) 63 (3) Western Journal of Communications http://www.tandfonline.com/doi/abs/10.1080/10570319909374648?journalCode=rwjc20#preview.

[447] *The Penguin Encyclopaedia* (Penguin Books Ltd., 2006), p. 682.

[448] Wolfgang Kleinwächer, 'The History of Internet Governance', in C. Möller and A. Amouroux (eds.), *Governing the Internet: Freedom and Regulation in the OSCE Region* (Vienna: Organization for Security and Cooperation in Europe 2009) pp. 41-90.

organization, created to take over the responsibilities administered by Internet Assigned Numbers Authority (IANA)[449] and headquartered near Playa Vista, Los Angeles, California, with bases in Belgium and Australia.[450]

The future of internet governance is a subject of an on-going political dispute and a focal point of international conflict among states.[451] The definition by the Working Group on Internet Governance (WGIG) of internet governance states that it:

> [i]s the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures and programmes that shape the evolution and use of the internet'.[452]

In the early 1980s, when the term 'internet governance' was first introduced, its role was confined to a relatively narrow set of technological policy issues relating to the management of its global core resources: domain names, Internet Protocol (IP) addresses,[453] and the root server system.[454] Since the establishment of ICANN in 1998 and with the expansion of functions that the internet performs, which before then were delivered thorough separate technologies and governed by separate legal and regulatory regimes,[455] the meaning and scope of the term has significantly expanded. The recognition by states of the strategic importance of cyberspace in international relations, the concerns over its security in the light of some recent revelations, such as the release of the Mandiant Report,[456] Edward Snowden's leakage of US

---

[449] IANA's functions are to oversee global IP address allocation, autonomous system number allocation, root zone management in the domain name system (DNS) and other internet-protocol related systems and numbers.

[450] Mark Milian, 'Keepers of the Internet Face Their Greatest Challenges Ever' (2011) CNN, <http://edition.cnn.com/2011/12/22/tech/web/icann/>

[451] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (The MIT Press 2010).

[452] Report of the Working Group on Internet Governance (2005), <http://www.wgig.org/docs/WGIGREPORT.pdf.>

[453] Tim Fisher, 'What is an IP Address' (1 June 2017) < https://www.lifewire.com/what-is-an-ip-address-2625920>. An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with another device over an IP based network, such as the internet.

[454] Kleinwächer, supra note 146.

[455] Mueller, supra note 149, p. 9.

[456] Mandiant, 'APT 1 Exposing One of China's Cyber Espionage Units' (2011) < https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> The Report disclosed the existence of Chinese units cyber-spying on the US in which it was stated that: 'China's economic espionage has reached an intolerable level and I

government's surveillance programmes,[457] its growing military use,[458] together with the human rights concerns, to name but a few, propelled cyberspace to become an arena for strategic and global competition.[459] The range of contested issues that the internet governance is currently concerned with is expansive and varied, including: (1) censorship and content regulation; (2) intellectual property protection, trademarks and copyrights; (3) cyber security; (4) human rights protection; (5) surveillance policies; (6) control of spam; (7) cyber crime; (8) resource assignment and coordination policies of ICANN; (9) technical standards formation; (10) economic regulation of communication services.[460] This is not by any means an exhaustive list, but it merely indicates the complexities involved and the fact that even the most technical aspects of internet operations, such as the allocation of IP addresses, the introduction of domain names, or the management of root servers, have become highly politicised.[461]

There is no doubt that this list will expand with innovation and on-going technological progress. Central to the internet governance debate are two competing models underpinned by divergent ideologies described in the next section of this chapter: the multistakeholder governance model and the sovereignist model. To appreciate the global politics of cyberspace, a historical thumbnail sketch will briefly outline and bases for the rivalry among states and set out two phases of this discourse, namely the cyber libertarian versus cyber realist polemic and the global 'battle for the internet'.

---

believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy. Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge.'

[457] *The Guardian*, "UK-US Surveillance Regime Was Unlawful 'For Seven Years"(6 February 2015) < http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa>.

[458] Roscini, supra note 10, concluding on p. 280 that 'the militarization of cyberspace is not a risk, it is already a fact, with the armed forces of several states establishing cyber units and including cyber operations in their military doctrines and strategies'.

[459] Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance' (2015), 91 International Affairs p. 110.

[460] Mueller, supra note 149, p. 10

[461] Hannes Ebert and Tim Maurer, 'Contested Cyberspace and Rising Powers', (2013) 34 Third World Quarterly, p. 1058.

- The First Phase: Cyber Libertarianism versus Cyber Realism

The current multistakeholder model reflects the decentralized liberal approach envisaged by the early American internet pioneers, such as Barlow,[462] Clark[463] and Englishman Berners-Lee,[464] who held liberal views when it came to functions, design and running of this facility. It is worth outlining the early debate of the 1990s between them and their opposition, both US government and academics, which is sometimes referred to, as a discourse between cyber libertarians and cyber realists (or positivists), because it continues to resonate in the current governance discourse. This early polemic was mainly focused on whether the internet (and cyberspace) can be governed at all and what role, if any, should governments play therein. The proponents of unbridled internet freedom, sometimes referred to as cyber libertarians, believed that it was the technical architecture based on the protocol system, which ignored national boundaries, that was the main driving force behind the internet. Nation states, governments, their laws and institutions had no role to play in this new virtual domain and all disputes created in the emergent, self-governing virtual communities could be resolved via consensus through freedom of association.[465] For Barlow, for example, a quintessential internet pioneer expressing his view in the *Declaration of Independence,* cyberspace was 'the new home of mind',[466] where traditionally conceived and state derived power structures had no part to play. Thus, any attempt to impose external legal controls would be futile, since in his reasoning, it is an environment with no physical borders. In any case, rules would lack legitimacy because of an absence of a rule making authority (which he rejected anyway) and *de facto* enforcement powers. Barlow's emancipated and rather naïve stance found support in Post and Johnson's 'Law and Borders-the Rise of Law in Cyberspace'.[467] Their belief was that since 'cyberspace

[462] John Perry Barlow, *A Declaration of Independence for Cyberspace,* (1996) <https://projects.eff.org/~barlow/Declaration-Final.html>.
[463] Dave Clark, 'A Cloudy Crystal Ball-Vision of the Future', Speech at Internet Engineering Task Force in 1992, where he proclaimed: 'we do not believe in kings, presidents and voting. We believe in rough consensus, factual approach and a running code' <http://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf>.
[464] Tim Berners-Lee, 'The World Wide Web and the Web of Life' <http://www.w3.org/People/Berners-Lee/UU.html>.
[465] Mueller, supra note 149, p. 2.
[466] Barlow, supra note 160.
[467] David Post and David Johnson, 'Law and Borders-Rise of Law in Cyberspace' (1996) 48 Stanford Law Review, p. 1367.

radically undermines the relationship between legally significant [online] phenomenon and physical location',[468] any attempt at regulating it would lack legitimacy. Furthermore, since cyberspace is everywhere, but nowhere in particular, it is 'a-jurisdictional' and therefore no sovereign state has a more compelling claim than any other to impose on it its own exclusive laws. It would also be unjustifiable to subject acts abroad to a domestic regulation.[469] These convictions were founded on a basic premise: the rise of the net destroyed the link between geographical location and recognizable, well-grounded characteristics of statehood: power, effective control, legitimacy and the ability stemming from physicality of statehood to give notice which sets of rules apply. Post and Johnson claimed that the 'net radically subverts a system of rule making, based on borders between physical spaces'[470] and concluded that a-territorial nature of the internet precludes any state from making a legitimate claim to regulate it. This being the case, self-governance would much better furnish liberal democratic ideas.[471] Consequently, if the internet must be regulated at all, it ought to develop its own effective governing institutions, whose legitimacy would derive from the consent of the internet users.[472] In this way, in the libertarian discourse, a new space for 'netizens' (net citizens)[473] would be created, free from traditional nation-state rules[474] and generally based on 'netiquette' (internet etiquette), whilst for business people, fashioned on rules of *lex mercatoria*.[475]

The rebuttal of this discourse was initially articulated by Goldsmith, who described it as 'cyber anarchy' and took issue with classifying cyberspace, as separate from the real world and devoid of any rules.[476] In sharp contrast to the utopian, libertarian doctrine, cyber realists firmly asserted that the political and legal institutions known collectively as a state, is the appropriate regulatory organization to oversee internet regulation.[477] Goldsmith in particular, believed that the libertarian argument suffers from three major flaws, which he called 'persistent fallacies': (1) the fallacy that cyberspace is a separate space; (2) that territorial governments cannot regulate the non-territorial net; and (3) over optimism that there will be

---

[468] ibid, p. 1370
[469] Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006) 10 Max Planck Yearbook of United Nations Law 191, p. 195
[470] Post and Johnson, supra note 165, p. 1376
[471] ibid.
[472] ibid, p. 1387.
[473] David Johnson and David Post, 'The New 'Civic Virtue', <http://www.temple.edu/lawschool/dpost/Newcivicvirtue.html>.
[474] Segura-Serrano, supra note 167, p. 194.
[475] ibid p. 196.
[476] Jack Goldsmith, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review.
[477] Segura-Serrano supra note 167, p. 197.

cheap, plentiful information.[478] The conviction that cyberspace is nothing else than an extension of pre-existing communication media and therefore susceptible to legal regulation, re-oriented the displaced role of the users, who operate in a 'real world' and are 'no more removed than telephone users, postal users, or carrier-pigeon users,[…] are in front of the screens in real space using a keyboard to communicate with someone else, often in different territorial jurisdiction'.[479] For another cyber realist, Reed, 'human and corporate actors and the computing and the communication equipment, through which the transaction is effected, all have a real-world existence and are located in one of more physical world legal jurisdiction'.[480] In addition Lessing, in *Code and Other Laws of Cyberspace,*[481] argued that the internet is 'evolving from an 'unregulatable' space to one that is highly 'regulatable'[482] through four forms of regulation: law, social norms, the market and code architecture. Further support of this stance was articulated by Goldsmith and Wu in *Who Controls the Internet?,* who displaced cyber libertarian argument by asserting that the internet will only work, if it is controlled and such control can only be provided by territorial governments.[483] Their rebuke of the libertarian doctrine was emphasised by the rejection of anarchy in place of coercive governmental power, which they justified by a simple assertion: democratic governments, with all their faults, are still

> [l]east-bad system known to history. With an open and free press, regular elections and an independent judiciary, democratic governments are the best system that human beings have ever devised for aggregating the varied interests and desires of a sovereign people into a workable governing order and for minimising or correcting the many pathologies that invariably encumber governmental systems.[484]

The cyber libertarian approach is now seen very much as a product of its times. The view that prevails now is that the internet does not constitute a distinct physical space, or a

---

[478] Jack Goldsmith, 'Regulating the Internet: Three Persistent Fallacies', 73 Chicago-Kent Law Review (1998), p. 1119.
[479] ibid p. 1121.
[480] Chris Reed, *Internet Law: Text and Materials,* (Cambridge University Press 2004) p. 188.
[481] Lawrence Lessing, *Code and Other Laws of Cyberspace* (Basic Books 2006).
[482] ibid p. 25.
[483]Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of the Borderless World* (Oxford University Press 2006), p. 142.
[484] ibid.

different jurisdiction, but is a result of advanced telecommunications technology.[485] The next phase of the debate involved not only academics, but nations reflecting the view of Goldsmith and Wu that 'many aspects of the net will be governed on a global scale' since 'many internet controversies are fast transforming into disputes among nations and classic problems of international relations'.[486] Nonetheless, both the internet and cyberspace continue in existence as a result of the original architecture by and large based on libertarian ideology, that is through the de-centralized system of networks and the laissez-faire approach to its operation and development.

- The Second Phase: Global Governance- The 'Battle for the Soul of the Internet'.[487]

The efforts to construct a global coordination and policymaking framework for the internet began in the mid 1990s and to date remain unsuccessful.[488] The internet emerged and developed, with no direction from intergovernmental processes, such as the International Telecommunications Union (ITU) and without generating rules of international law, as for example those found in the International Telecommunications Regulations (ITRs).[489] Even the creation of ICANN in 1998[490] went almost unnoticed at the time by the majority of governments. This in many respects contributed to the internet's governance development through the multistakeholder system, where state and non-state actors collaborated on managing technical and operational tasks.[491] As the internet expanded globally, many countries became concerned with this status quo, especially in the light of US dominance.[492] Their

[485] Seguar-Serrano, supra note 167, p. 199.
[486] Goldsmith and Wu, supra note 181, p. 165.
[487] Elliot Noss, 'A Battle for the Soul of the Internet' (2005), <http://www.zdnet.com/article/a-battle-for-the-soul-of-the-internet/>.
[488] Milton Mueller, John Mathiason and Hans Klein, 'The Internet and Global Governance: Principles and Norms for a New Regime', 13 Global Governance (2007) 237.
[489] David Fidler, 'Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations' 17 American Society of International Law, Insight (2013) <http://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision>.
[490] Ebert and Maurer supra note 159, p. 1061.
[491] Fidler supra note 187.
[492] ibid.

overriding aim was to bring the governance within intergovernmental processes and international law.[493]

The first major battleground was the World Summit on the Information Society (WSIS),[494] initiated by the ITU in 1998 and authorised by UN General Assembly Resolution 58/83.[495] It was held in two phases: the first one in 2003 (Geneva) and the second in 2005 (Tunis) where, in the words of one commentator 'governments, both democratic and undemocratic, felt the need to assert their belief that they should have authority over internet related public policy issues'.[496] The range of their proposals included strengthening the ITU according to the sovereignist approach, creating a new, intergovernmental-oriented entity and drafting an internet treaty.[497] The Geneva Summit's aim was to focus on information and communication technology and development. It was an outlet for countries, such as South Africa, China and Brazil to formally express their dissatisfaction with internet governance arrangements, in particular the central role of ICANN, which they portrayed as 'a unilateral creation of the United States government'.[498] This group of states was advocating a need for a more traditional intergovernmental model, or failing that, at the very least, multilateral decision by national sovereigns to confirm, or amend, the existing arrangements.[499] The opposite side (ICANN, the Internet Society and the US government) downplayed these criticisms and demands, proclaiming that the patchwork of governance arrangements among ICANN, WIPO treaties and the Internet Engineering Task Force (IETF) was fit for purpose.[500] The Geneva phase of WSIS mandated the creation of a Working Group on Internet Governance (WGIG), which was tasked with (1) development of a working definition of internet governance (referred to above); (2) identifying the public policy issues relevant to internet governance; and (3) development of a common understanding of the respective roles and responsibilities of

---

[493] ibid.

[494] ITU, *World Summit on the Information Society Geneva 2003-Tunis 2005*, <http://www.itu.int/wsis/basic/about.html>.
The WSIS was initiated by the International Telecommunications Union and held in two phases: (1) Geneva December 2003 to 'develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society'; and (2) Tunis November 2005, with an objective 'to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents.'

[495] UN GA, Resolution 56/183, 90th Plenary Meeting (21 December 2001).

[496] Mueller, supra note 149, p. 60.

[497] Fidler, supra note 187.

[498] Mueller et al, supra note 186.

[499] ibid.

[500] ibid.

governments, existing intergovernmental and international organizations and other forums, as well as the private sector and civil society from both developing and developed countries.[501] In 2005 WGIG issued a final report, in which it recommended the creation of a new multistakeholder forum to deal with internet issues,[502] the Internet Governance Forum (IGF),[503] a discussion group with no-decision making authority. The WGIG report failed to specify the working methods of the IGF. Perhaps more importantly, however, it concluded that governments should control 'public policy', but leave 'technical management', or 'day to day operations' of the internet to the private sector and civil society, as these functions are inextricably linked.[504] The overall outcome of the Geneva WSIS was an agreement on a *Declaration of Principles* and a *Plan of Action,* with an aim of their implementation.

The second WSIS Tunis phase in 2005[505] was intended to foster governments' agreement relating to the oversight of the management of critical internet resources (domain names, IP addresses, internet protocols and root servers) and to put ICANN under the regime of an Intergovernmental Internet Council.[506] The official outcome document, the *Tunis Agenda for Information Society*[507] challenged specific aspects of ICANN's regime and declared that all states, not just the United States, should have 'an equal role and responsibility for the DNS root and for internet public policy oversight'.[508] The Agenda failed however to introduce specific mechanisms for adopting the principles that it set out to achieve. Both Summits produced virtually no concrete change to ICANN and had contributed little to defining a framework for global internet governance.[509] The only solid result was the creation of the IGF, as a mechanism to continue the debate.

The same year saw the emergence of a coalition among the 'rising powers' of Brazil, Russia, India, China and South Africa, also known as BRICS, viewed by some as a 'concerted

---

[501] ibid.
[502] ibid.
[503] Fidler, supra note 187.
[504] Mueller et al, supra note 186.
[505] WSIS 2005 in Tunis was a broad based summit that covered many issues, including the digital divide, human rights, infrastructure development, cultural diversity, intellectual property, privacy, cyber security.
[506] Wolfgang Kleinwächer, "Internet Governance Outlook 2013: 'Cold Internet War' or 'Peaceful Internet Coexistence'?" (2013) CircleID <http://www.circleid.com/posts/20130103_internet_governance_outlook_2013/>.
[507] Tunis Agenda for Information Society, WSIS-05/TUNIS/DOC/6(/Rev.1)-E, (18 November 2005) <www.itu.int/wsis.>.
[508] Meuller et al, supra note 186.
[509] ibid.

counter-hegemonic movement' [510] against US dominance in cyberspace. Although all governments from the BRICS coalition show an interest in shaping cyber policy, their priorities are different and therefore the overall approach fragmented. In fact, their agendas diverge significantly. [511] The main differences lie between those states, which favour the intergovernmental approach, based on international cooperation and those preferring to adopt a strict, sovereigntist cyber policy. This is evidenced by a lack of joint BRICS proposal on information security, or a new internet governance body.[512] So far, formal proposals have been submitted, either through the collaboration of India, Brazil and South Africa, known as the IBSA coalition, who in 2003 put forward the *Brasilia Declaration,* or the Shanghai Cooperation Organization submitting the *Code of Conduct for Information Society* to the UN General Assembly in 2011 and 2015.[513]

Another significant event regarding the developments of international cooperation of internet governance was the 2012 the International Telecommunications Union World Conference on International Telecommunication held in Dubai to review the International Telecommunications Regulations 1988 (IRs), discussed in more detail below. This was a high ranking meeting that to this day is widely perceived as a fiasco. Following the disagreement in Dubai, the next two years were replete with meetings on all levels and the debate on the future regulation of the internet gained in sharpness. The main event of 2013 was the eight Internet Government Forum conference in Bali. 2014 was described as a 'year of meetings' on all levels, including the Plenipotentiary Conference of the International Telecommunications Union in Busan, South Korea.[514]

This historical thumbnail sketch to some extent explains the deeply polarized global debate and political power struggle, at the heart of which are three of the above mentioned competing models: the multistakeholder, with the central and continued role played by ICANN; the intergovernmental with the primary role of the ITU and the sovereignist, mainly supported by Russia and China. Each will be considered in turn below.

---

[510] Ebert and Maurer, supra note 159.
[511] ibid p. 1055
[512] ibid.
[513] supra note 42.
[514] Wolfgang Kleinwächer, 'Internet Governance Outlook 2014: Good News, Bad News, No News' (2014) Circle ID <http://www.circleid.com/posts/20131231_internet_governance_outlook_2014_good_news_bad_news_no_news/>.

- The Multistakeholder Model and ICANN

As a result of its historic origins, the internet is currently managed through a model known as multistakeholderism. This method of internet management has no hierarchy and consists of governments, private companies and non-governmental organizations. It has representatives from public interest advocacy groups, business associations and other parties, who all participate in intergovernmental policy deliberations alongside governments.[515] The fact that it was the US authorities that were instrumental in the internet's creation and its shaping was evidenced by a contractual relationship between the US Department of Commerce and ICANN, which operates through an Affirmation of Commitments Licence,[516] issued by the United State's Department of Commerce National Telecommunications and Information Administration (NTIA).[517] This operating licence, which in eleven clauses defines ICANN's responsibilities, was clarified and renewed in 2006. The licence expired in 2016 and the key internet domain function was transferred to ICANN on 1 October 2016,[518] discussed in more detail in Chapter 5.

The ICANN's mission 'is to coordinate, at the overall level, the global internet's system of unique identifiers and to ensure their stable and secure operation.'[519] In particular, ICANN: (1) coordinates the allocation and assignment of the three sets of unique identifiers for the internet, which are (a) domain names (forming a system referred to as DNS); (b) IP addresses and autonomous system (AS) numbers; and (c) protocol port and parameter number; (2) coordinates the operation and evolution of the DNS root name server system; (3) coordinates

[515] Mueller, supra note 149, p. 8.
[516] Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers, <https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en.>

[517] The United State's Department of Commerce National Telecommunications and Information Administration, NITA, < http://www.ntia.doc.gov>. 'NTIA is the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth'.
[518] *BBC News*, 'US Ready to Hand Over the Internet's Naming System' (18 August 2016) <http://www.bbc.co.uk/news/technology-37114313.>
[519] ICANN Affirmation of Commitments, supra note 214.

policy development reasonably and appropriately related to these technical functions'.[520] ICANN has a 16-member board of directors, selected to reflect 'diversity in geography, culture, skills, experience and perspective'.[521] Its functions were set out in the 1998 Memorandum of Understanding,[522] which aimed 'to transition management responsibility for domain name system (DNS) functions performed by, or on behalf of, the US Government to a private-sector not-for-profit entity'.[523] The principles of stability, cooperation, 'bottom-up' coordination and representation were outlined, as foundations for this process.[524] Giving the main responsibility for running and overseeing internet's workings to the private sector, multistakeholder governance organization, with an input from governments through the Government Advisory Committee in preference to national and international communications sector, where the ITU could play a role, was said to be a deliberate move on the part of the US government from the very beginning of funding the internet project.[525] Crucially, 'ICANN had not placed governments at the forefront of visible activity, but instead placed industry needs and the operation of a competitive deregulated international communications sector, as being the major thrust of coordination activities',[526] which reflects the cyber libertarian approach of its founding fathers. ICANN's main attribute is that is promulgates and works through a so-called 'bottom-up' processes. This allows the government, private sector, civil society and the technical community to develop incrementally and work together to solve internet policies. There can be no doubt that this approach has enabled in the last twenty years an incredible technical innovation and expansion of this facility worldwide. Such a way of administering the internet is not only favoured by the US, but also by its Western allies, for whom 'a free, open, borderless and secure internet can be managed only by a collaborative effort of all

[520] Bylaws for Internet Corporation for Assigned Names and Numbers, A California Nonprofit Public-Benefit Corporation, art 1- 'Mission and Core Values' <https://www.icann.org/resources/pages/governance/bylaws-en.

[521] ibid.
[522] ICANN, 'Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers' (25 November 1998) < https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en>.
[523] ibid.
[524] ibid.
[525] Mueller et al, supra note 186; The Governmental Advisory Committee is composed of representatives of national governments from 111 countries and a large number of observers.
[526] Geoff Huston, 'Opinion: ICANN, the ITU, WSIS and Internet Governance' *Cisco*, <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-1/internet_governance.html>.

concerned', [527] based on 'shared norms, programmes, protocols and decision making procedures'. [528] Nonetheless, ICANN has enjoyed a mixed level of success. It managed to establish itself, as the major admistrator of the infrastructure elements of the internet protocol in a de-regulated manner, which reflects the nature of the internet industry. [529] It has successfully restructured the generic top-level domain name business, by replacing a single monopoly operator with a system of registry operators and registrars. ICANN's stewardship and continued success in keeping the internet 'open' has been achieved however, with continued sponsorship of the US administration. [530] Critics point out that ICANN and the American government practically monopolized the global communications industry, since ICANN has not offered viable mechanisms for other national, or regional interests to be represented at a governmental level. [531] Indeed, through ICANN, the US successfully established a governance regime dominated by itself and by non-state actors. [532] This the US government has achieved, by privatizing and internationalizing key policymaking functions, whilst retaining until 2016 considerable authority for itself through ICANN and the Department of Commerce, together with asserting 'policy authority' over the domain name system's root and reserving the right to review and approve any changes to the root zone file proposed by ICANN. [533] The relationship between ICANN and the US government, which ceased in October 2016, sent for years a message to the rest of the world that the US is withholding the internet from conventional international governance processes, thereby strengthening the position of already entrenched US-based enterprises across a lucrative global internet market. [534] The criticisms of ICANN's domineering role, the lack of transparency and accountability were repeatedly voiced by those countries, which preferred to see the United Nations in charge of the web. In 2011 they were joined in this vision by the Obama administration. [535] As a result,

[527] ibid.
[528] ibid.
[529] Geoff Huston, 'ICANN, the ITU and WSIS and Internet Governance Part I' (2004) APNIC <https://www.apnic.net/community/ecosystem/igf/articles/icann-wsis-part-i>.
[530] ibid.
[531] Geoff Huston, 'ICANN, the ITU and WSIS and Internet Governance-Part II' (2004) APNIC <http://www.apnic.net/community/ecosystem/igf/articles/icann-wsis-part-ii>.
[532] Mueller et al, supra note 186.
[533] ibid p. 240.
[534] Huston, supra note 224.
[535] Ian Shapira, 'Obama Administration Joins Critics of US Non profit Group that Oversees Internet', (2011) *The Washington Post* <http://www.washingtonpost.com/wpdyn/content/article/2011/02/28/AR2011022803719.html>.

in 2014 the administration unveiled its plans to phase out ICANN's role of overseeing the IANA's contract. Consequently, the US Department of Commerce ceded its power over the the internet's naming system ending an almost 20 year process of handing over a crucial part of the internet's governance.[536]

- The Sovereignist Model and the Intergovernmental Policy

The existing US lead multistakeholderism and therefore the American cyber hegemony, has been challenged by another regime, often referred to as sovereignist model and pursued via a variety of channels, including the UN institutions and hence also called the intergovernmental model.[537] This approach, upheld by a loose coalition of disgruntled like-minded states including Russia and China, seeks to develop strategic engagement with international institutions, such as the ITU, in order to exert a degree of control in cyberspace. Their aim is to tame US leadership by transferring authority to an international governmental organization (IGO) in order to dilute the US power and set it firmly in the rules and institutions that channel and limit the ways that power is exercised. The focus of the sovereignist model is on establishing territorial control over cyberspace, reasserting a Westphalian notion of sovereignty through an IGO, such as the International Telecommunications Union (ITU).[538] Russia in particular has protested for years a 'policy vacuum' and institutional gap within the current multistakeholder model.[539] The Kremlin and other like-minded governments, wish to re-assert state sovereignty by 'shifting the balance of participation from a network-to network system to a government-to-government system, in which experts would be required to participate indirectly-through government actors [said to be] much less well informed on the issues'.[540] In November 2014 at the First World Internet Conference hosted in Wuzhen, China President Xi affirmed that under the terms of mutual respect and trust, China was willing to cooperate with other states to achieve a peaceful cyberspace and a multilaterally governed, transparent internet, emphasising however that sovereignty must be fully respected in that domain.[541] A

[536] *BBC News*, 'Has the US Just Given Away the Internet?' (1 October 2016) <http://www.bbc.co.uk/news/technology-37527719>.
[537] Ebert and Maurer supra note 159, p. 1059.
[538] ibid p. 1060.
[539] Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance', 91 International Affairs (2015) 110.
[540] ibid, p. 117.
[541] *The Economic Times*, 'Chinese President Xi Jinping Calls for International Cooperation on Cyberspace Security' (19 November 2014), in Raud supra note 101, p. 15.

year later, during the keynote speech at the Second World Internet Conference President Xi called for 'building a cyber community of common destiny and put forward the principles of respecting cyber sovereignty, safeguarding cyber security and building cyber order'.[542] The President proposed building an internet governance system based on a multilateral approach, rejecting unilateralism, whereby only a few parties discuss the future of the internet.[543] The speech indicated China's dissatisfaction with the current status quo. To that end, China's President called to reform the existing international internet governance system based on four principles, namely the respect for cyber sovereignty, openness, cooperation and good order.[544] Worthy of note is President Xi's reiterating the importance of cyber sovereignty, when he stated that:

> [w]e should respect the right of individual countries to independently choose their own path of cyber development model, model of cyber regulation policies and Internet public policies and participate in international cyberspace governance on an equal footing.[545]

The Eastern states continue to support cyber sovereignty, which aims to increase state control over cyberspace, even at the expense of open networks and defend the principle of non-intervention in internal state affairs.[546] This ideology they pursue through a variety of channels: domestically (as outlined above and in the next part of this chapter) and both internationally, via the UN organizations such as the ITU and regionally through the Shanghai Cooperation Organization (SCO).

- The Role of the International Telecommunications Union

The intergovernmental policy model sees the operations of the internet to be overseen through a cooperation of states via an international treaty, reflecting a top-down approach and

---

[542] ibid.
[543] Rui Zhang, 'China Headlines: Xi Slams 'Double Standards', Advocates Shared Future of Cyberspace' (17 December 2015) <http://news.xinhuanet.com/english/indepth/2015-12/16/c_134924012.htm >.
[544] *The Diplomat*, 'China's Emerging Cyberspace Strategy' (24 May 2016) <http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/ >
[545] ibid.
[546] ibid

the ITU as best placed for achieving their own internet governance agendas. These states adhere to a more traditional concept than the de-centralised multistakeholder mechanism, that is one based on balancing competing national interests through common regulatory measures undertaken within each national regime to regulate public-sector processes.[547] For their governments, public communications is a public-sector activity and therefore its control should be borne by national and international regulatory regimes. Therefore the ITU, as an intergovernmental venue historically linked to the telecommunications sector, is the entity best suited to redress the distorted position of one state (the US) holding a virtual monopoly over international telecommunications. The ITU is one of the oldest institutions in the sphere of telecommunications. Its origins can be traced to the 1865 International Telegraph Convention, which established the International Telegraph Union. Having combined the 1865 International Telegraph Convention with the 1906 International Radiotelegraph Convention, the International Telecommunications Convention was formed and the body's name was changed to International Telecommunication Union to reflect its full scope of responsibilities, which at that time included all forms of wireless and wireline communications. Following an agreement with the then newly formed United Nations, the ITU undertook responsibilities for international telephony, telegraphy and radio communications in 1947 and over the next four decades oversaw the expanding system of international telephony and data. Today its role includes overseeing the operations of the global radio spectrum, satellite orbits and other carrier-centric technologies. Its members comprise countries and private companies, rather than individuals and the main source of funding is through a hefty membership fee.

The ITU's involvement with the evolution of the internet has been virtually non-existent. Nevertheless, the organization has made numerous attempts to strengthen the role it plays in this process, reflecting the concerns of many countries regarding the multistakeholder governance and the US dominance. For some countries, (including China, Russia and the Arab States) it is an institution of choice to head and oversee the workings of the internet, which they believe would allow them greater say in its running and be a forum for democratic representation. This is illustrated by Russian President Vladimir Putin's announcement in 2011, prior to the 2012 Word Conference on International Telecommunications (WSIT-12) in Dubai, United Arab Emirates, that Russia would like to 'establish international control over the internet using the monitoring and supervisory capabilities of the ITU' and that the ITU

[547] Huston, supra note 224.

could become responsible for allocating at least some of the internet's addresses.[548]

The ITU initiated the process of international engagement with the future of internet governance by sponsoring the establishment of the two phase WSIS (mentioned above) and attempting to amend the International Telecommunication Regulations (ITRs)[549] at the WCIT-12 in Dubai. The ITRs, last negotiated in 1988 in Melbourne, define the general principles for the provision and operation of international telecommunications. During the two-week Dubai Conference several proposed changes on such topics, as international mobile roaming, numbering, naming, addressing fraud and the internet were discussed. The revised version of the ITRs was finalised, but only 89 out of 151 states in attendance signed it. That group of states consisted of mostly emerging countries led by Russia, China, Brazil and the Arab States.[550] The United States, Japan, Australia, United Kingdom and most of European countries declined to agree to the proposed changes. In the run up to the Dubai Conference, the supporters of the multistakeholder model argued that the ITU and some of its members were using the Conference to 'bring internet governance under governmental and intergovernmental control, with dire consequences for innovation, commerce, development, democracy and human rights'.[551] At the outset of the Conference several proposals were tabled[552] specifically relating to the internet, including: (1) to define the term 'internet' and explicitly bring the internet into the regulatory structure of the treaty; (2) to bring internet naming, addressing and identifiers into the treaty; (3) to include a provision on access to internet websites; and (4) proposals from multiple states on spam, information security and cyber security.[553] In particular, the proposed

[548] Leo Kelion, 'US Resists Control of Internet Passing to UN Agency' BBC News <http://www.bbc.co.uk/news/technology-19106420.>

[549] The original International Telecommunication Regulations were mainly concerned with the interconnection and interoperability of existing communication services, together with methods of calculating charges for traffic exchange among carriers in different countries.

[550] Robert Pepper and Chip Sharp, 'Summary Report on the ITU-T World Conference on International Telecommunications', 16 Internet Protocol Journal <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_16-1/161_wcit.html>.

[551] David Fidler, 'Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations' (7 February 2013), Insight < http://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision>.

[552] Dr Toure, the ITU Secretary-General declared that the WCIT was not about the internet or internet governance at the outset of the Conference, nevertheless the WCIT had to consider input from its member states and given that proposals relating to the internet were submitted in consequence they formed a substantive topic of discussion;

[553] Pepper and Sharp, supra note 248.

Article 1 'Purpose and Scope of the Regulations', stated that:

> [t]hese Regulations also contain provisions applicable to those operating agencies, authorized or recognized by a Member States, to establish, operate and engage in international telecommunications services to the public, hereinafter referred to as authorised operating agencies. [554]

The US viewed this provision, as an avenue for expansion of the traditional role of the ITU into the internet[555] and opposed it. The American delegation argued that it broadened the scope of the revised ITRs to include private sector internet service providers and government network operators.[556] Ambassador Kramer, the US Head of Delegation remarked that 'the United States consistently sought to clarify that the treaty would not apply to internet service providers or governments or private network operators'.[557] He also noted that 'spam is a form of content and that regulating it inevitably opens the door to regulation of other forms of content, including political and cultural speech'. [558] However, as some African states insisted on including the provision on spam, a statement was added to Article 1.1, according to which, 'these Regulations do not address the content-related aspects of telecommunications'. [559] Another new addition to the ITRs, Article 5A 'Security and Robustness of Networks', obliged state parties to 'endeavour to ensure the security and robustness of international telecommunications networks'.[560] This provision too was objected to by the US, who argued that the ITU and the ITRs were not the 'useful venue for addressing security issues and cannot accede to vague commitments that would have significant implications but few practical improvements on security'.[561] The result of the Dubai Conference was a lack of consensus among the participating states, as to whether the revised ITRs should apply to the internet and

---

[554] International Telecommunication Regulations (2015), art 1. 2A http://www.itu.int/ITU-T/itr/ .
[555] Fidler, supra note 187.
[556] ibid.
[557] Terry Kramer, US Ambassador and Head of Delegation, World Conference on International Telecommunications, 'Remarks', (13 December 2012) < http://www.state.gov/e/eb/rls/rm/2012/202040.htm>.
[558] ibid.
[559] ITRs, art 1, supra note 252.
[560] ibid, art 5.
[561] US Ambassador Kramer, supra note 255.

its governance.[562] The disagreements over the proposals relating to (1) the internet, internet governance, or information security; (2) naming or addressing; and (3) modifying the basic business models, meant that the revised treaty was not adopted by a consensus. The revised ITRs took effect on 1 January 2015 for those countries, which agreed to be bound by them. The ITU members, who do not accept the revised Regulations remain to be bound by the original ITRs. However, as it is an open treaty, any member state can still accede to it in the future.[563]

It could be said, that WCIT-12 deepened the rift among the international community and reinforced the disagreements and fragmentation about internet governance in the subsequent meetings, most notably during the ITU World Telecommunication Policy Forum in May 2013 and the ITU Plenipotentiary Conference 2014 in Busan, South Korea. The Busan Conference, in particular, resulted in another failure to 'inject' the ITU with more central role in the design and operation of the technical protocols of the internet.[564] A large number of countries proposed changes concerning internet organization. None of these changes however made it through, due to 'concerted pressure by a number of Western governments, advised continuously by the net specialists'.[565]

In summary, the Dubai Conference confirmed that the global internet will continue to work on principles devised by a broad range of groups, that governments have a lead role in deciding the network infrastructure within their own territories, but that there is a growing, international consensus that the internet works best, when governments are just one part of the decision-making process.[566] The exact nature of the future role that the ITU could play in the internet development and management is difficult to predict at this stage. It appears to have been further side-lined with the US government handing over the control over the domain name system to ICANN in 2016. However, as one commentator noted, China and/or Russia, along

---

[562] There were 144 delegations with voting rights, of which 89 signed the revised ITRs (African countries, Brazil, China, Indonesia, Iran and Russia), while 55 did not (including Australia, EU members, Canada, Japan and the U.S.).
[563] ITRs, art. 54 para 3bis, supra note 252.
[564] David Post, 'Stand Down! UN 'Takeover of the Internet' Postponed Indefinitely' (7 November 2014) *The Washington Post* <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/07/stand-down-un-takeover-of-the-internet-postponed-indefinitely/>.
[565] Kieren McCarthy, 'UN Takeover of Internet Postponed Indefinitely' (5 November 2014) *The Register* <http://m.theregister.co.uk/2014/11/05/un_takeover_of_internet_postponed_indefinitely/>.
[566] ibid.

with parts of the Middle East may regroup and try to push for more global control[567] and greater ITU involvement. For sceptics, such as Post, it is impossible to imagine any UN-style body, by design controlled by majority vote among the world's governments, many of which still adhere to 'state monopoly telephone network', to replicate and manage the existing internet.[568] Nevertheless, the debate relating to the role of governments and intergovernmental organizations in overall internet governance will continue.

- Policy Shaping Through Regional Organizations

Those states among the international community, who are dissatisfied with current status quo, also seek to challenge the historical dominance of the United States in cyberspace through regional organizations and alliances. Russia in particular has been active in this regard in the last decade and recently has increased its diplomatic efforts in promoting a more centralized, top-down agenda through the Shanghai Cooperation Organization (SCO), which has cyber security within the remit of its activities, the Collective Security Treaty Organization (CSTO) and the BRICS group.

2006 marked the start of Russia's greater engagement with the SCO,[569] which it perceives as a vehicle for the advancement of its internet governance agenda.[570] The SCO's aim is to share information and coordinate policies in cultural, economic, security and cyberspace policy areas.[571] However, experts see it as 'a regional vehicle of 'protective integration' against international norms of democracy and regime change, with shared information policies being seen as critical to that end.'[572] In 2011, four members of the SCO, (China, Russia, Tajikistan and Uzbekistan), submitted *Draft International Code of Conduct for Information Security*[573](Draft Code) to the United Nations General Assembly. The Draft Code used the phrase 'information space' rather than cyberspace and proposed, *inter alia*, 'to reaffirm all

[567] ibid.
[568] Post, supra note 262.
[569] Shanghai Cooperation Organization is a regional organization made up of China, Kyrgyzstan, Kazakhstan, Russia, Tajikistan and Uzbekistan. India, Iran, Mongolia, Afghanistan and Pakistan have an observer status, while Belarus, Turkey and Sri Lanka are considered dialogue partners.
[570] Ebert and Maurer, supra note 159 p.1067
[571] Ronald Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 Global Governance p. 339.
[572] ibid.
[573] *Draft Code of Conduct for Information Security* 2011, supra note 42.

states' rights and responsibilities to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage'.[574] It also proposed 'the establishment of a multilateral, transparent and democratic international management of the internet to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the internet'.[575] The US and its allies rejected the proposed Draft Code, opposing in particular the sovereign control idea, mainly on the grounds relating to the protection of freedom of expression, association and possibility of suppression of free speech through government control over content for the purpose of political domination. The US unequivocally disagreed with the multilateral governance.[576] It was felt that the proposed Code 'would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right, as described in the Universal Declaration on Human Rights' and that it attempted to 'replace existing international law that governs uses of force and relations among states in armed conflict with new, unclear and ill defined rules and concepts'.[577] The US stance on some of these issues is reflected in its *International Strategy for Cyberspace*, which states that:

> [t]o promote internet governance structures that effectively serve the needs of all [i]nternet users we will promote and enhance multi-stakeholder venues for the discussion of [i]nternet governance issues. The very architecture of the [i]nternet embodies a mode of social and technical organization, which is decentralized, cooperative, and layered. Each of these characteristics is fundamental to the benefits the [i]nternet has brought. That architecture fuels the freedom of innovation that enables economic growth. It fuels the freedom of expression and association that enables social and political growth and the functioning of democratic societies worldwide.[578]

---

[574] ibid, art II (5).
[575] ibid, art II (7).
[576] Statement by Delegation of the United States of America, 'Other Disarmament Issues and International Security Segment of Thematic Debate on the First Committee of the Sixty-seventh Session of the United Nations', (2 November 2012) <http://www.state.gov./t/avc/rls/200050.htm>.
[577] ibid; The Statement alleged that 'one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of *jus ad bellum* and *jus in bello* that would provide a legal framework for the way that states could use force in cyberspace, have no applicability'.
[578] US White House, *International Strategy for Cyberspace*, supra note 53, pp. 21-22.

Viewed in the light of this ideology, the Draft Code 'present[ed] an alternative view that seeks to establish international justification for government control over internet resources'[579] and sought to strengthen governmental power over the internet by invoking a multilateral governance that would replace the multistakeholder model, where all users have a voice, with top-down control and regulation by states.[580] As a response to this rejection, on 9 January 2015 the six members of the SCO (China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan and Uzbekistan) issued a revised *Draft International Code of Conduct for Information Security*[581] (Draft Code 2015) The letter accompanying it stated that it was 'revised taking into full consideration the comments and suggestions from all parties'.[582] Some of its provisions remain however practically unchanged. It restates, for example the same vision that the SCO countries share regarding state control of cyberspace governance, which was contained in the 2011 Draft Code and favours the 'establishment of multilateral, transparent and democratic international governance mechanisms, which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the internet'.[583] This provision yet again attempts to sideline the multistakeholder model and as one commentator noted,[584] it 'echoes a controversial resolution adopted at the WCIT-12',[585] which confirms that 'SCO member states' views on internet governance have not shifted and are not intended as any accommodation to the advocates of the multi-stakeholder governance model'.[586] The Draft Code 2015, like its predecessor, refers to the 'information space' and 'reaffirms rights and responsibilities of all states'[587] to protect it. Since the revised code does not include major changes, it is unlikely that it will find global support due to the ideological differences among

[579] Statement by Delegation of the United States of America, supra note 274.
[580] ibid.
[581] supra note 42.
[582] ibid.
[583] ibid, paragraph 8.
[584] Kristen Eichensehr, 'International Cyber Governance: Engagement Without Agreement?' (2015) *Just Security* http://justsecurity.org/19599/international-cyber-governance-engagement-agreement/.
[585] ibid.
[586] ibid.
[587] supra note 42, para 6.

the international community.[588] However, its principles may be implemented regionally or among the like-minded states.[589]

- Domestic Cyber Sovereignty

In tandem with pursuing the sovereignist agenda through international and regional organizations, some states are attempting to territorialize cyberspace by seeking to exert greater controls over their 'segment' of it within their borders. Some of these tendencies were discussed earlier in this chapter in the context of domestic cyber security policies. For such states as for example, Russia and China re-claiming control in this domain is not just a matter of national security, but comports with their abhorrence of broader ideology of denationalized liberalism, which to them the internet epitomizes. Russian's drive for cyberspace control to dilute continued US dominance is underpinned by a greater need, which dictates continued upholding of traditional international law principles of state sovereignty and non-intervention. These are the two core policy elements that dominate Russia's overall attitudes towards global cyberspace matters. Consequently, Russia's authorities conceive of cyberspace as a territory with virtual borders, which correspond to physical state frontiers. To realize this vision, Russian authorities wish to extend the remit of international law to that domain.[590] Having drawn conclusions from the power of digital technology, such as Twitter, YouTube and Facebook during the revolutionary processes in Tunisia, Libya and Egypt between 2010-2012, Russia's political elites regard all things digital as tools capable of undermining the political status quo, especially by the young. This 'appreciation' has resulted in law enforcement agencies monitoring closely the impact of the political use of networked technologies upon social mobilization and democratic transition.[591] The Kremlin is becoming increasingly concerned with the power of the internet, which it sees as politically disruptive, allowing citizens to circumvent government controlled traditional media, such as television and radio broadcasting. China mirrors this approach. In fact, the Chinese authorities place a particularly strong emphasis on the challenges posed by cyber activities that threaten domestic, social and

[588] NATO CCDCOE, In Brief, 'An Updated Draft of the Code Distributed in the United Nations-What's New?' (10 February 2015)
< https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>
[589] ibid.
[590] Eichensehr, supra note 282.
[591] ibid.

political norms, or values (such as the dissemination of false rumours), as well as state sovereignty.[592] The true extent of the Chinese authorities' ambitions to control the internet through delineating Chinese 'sovereign virtual territory'[593] can be gleaned from the elaborate set of government policies instigated and performed by a myriad of national agencies and requirements of self-regulation, collectively referred to, as the Great Firewall of China.[594]

China and Russia are not alone in the quest to build their own digital territories. Iran has laid down technical foundations for a national online network that could be detached from the global internet and permit tighter control over the flow of information and potentially to better manage cyber attacks.[595] This may give the Iranian authorities greater power to shut off access to the internet at times of civil unrest, as was the case in 2009 during the anti-government protests.[596] Forty other countries, including Ethiopia, Cuba and India, routinely monitor internet traffic[597] and target the unrestricted access to it through legislation, in effect performing 'virtual land grabbing'.[598] The OpenNet Initiative, an advocacy group, lists over 40 countries that block the internet content for political, social and security reasons.[599] Another illustration towards states' erecting 'cyber walls' is the 2014 German Chancellor Angela Merkel's proposal following the Snowden disclosures. The Chancellor announced plans for a European communications network to curb mass surveillance conducted by the US NSA and the UK GCHQ.[600] It is envisaged that the European communications network would be build

---

[592] Swaine, supra note 119.

[593] Wu Jianguo, 'Defending the Cyber Territory' (1 March 2000) *Liberation Army Daily*, translated by OSC, CPP20000302000067. Major Wu Jianguo stated that 'in a cyber century, the economic, political and cultural sovereignty as well as the military security of a country depend more and more on its effective jurisdiction over the 'virtual territory' […] Nowadays, a country's sovereignty can be regarded as integrated only when it has fully tapped the potential of its 'virtual territory' and effective controlled its territory'.

[594] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations* (Cambridge University Press 2014).

[595] James Ball and Benjamin Gottlieb, 'Iran Preparing Internal Version of Internet', (2012) *The Washington Post* < http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-1>.

[596] ibid.

[597] Marietje Schaake, 'Stop Balkanizing the Internet' (2012) *Huffington Post* < http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html>.

[598] ibid; One example is the Ethiopian Telecom Law, which criminalizes the use of Skype and other voice over internet protocol services, with high financial penalties, or a 15-year prison sentence for its violation.

[599] OpenNet Initiative Filtering Map <http://map.opennet.net/>.

[600] *The Independent*, 'Surveillance Revelations: Angela Merkel Proposes European Network to Beat NSA and GCHQ Spying' (16 February 2014)

inside Europe in order to prevent the emails and other internet data from automatically passing through the United States.[601]

Concerns have been raised by the devotees of the unified cyberspace, that if these trends continue, the internet would revert to a fragmented collection of more, or less connected proprietary islands reminiscent of the AOL and CompuServe days.[602] The segmentation that may result from these tendencies could be construed as part of the overall policies of those states, who would much prefer cyberspace resources be contained within their borders. A question thus arises, as to whether under international law it is possible for nations to extend territorial sovereignty in cyberspace, as discussed next.

2. SOVEREIGNTY UNDER INTERNATIONAL LAW AND ITS APPLICATION TO CYBERSPACE

(a) Sovereignty

Sovereignty and equality of states represent the basic constitutional building blocks of international law, which governs a community consisting primarily of states having a uniform legal personality.[603] The doctrine of sovereignty in international law relates to the collection of rights, powers and duties adhering to each particular state.[604] The definition is contained in Article 1 of the Convention on the Rights and Duties of States 1933, which states that:

> [t]he State as a person of international law should possess the following qualifications:
>
> (a) a permanent population;
>
> (b) defined territory;
>
> (c) government; and

< http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html >

[601] ibid.

[602] *The Economist,* 'The Future of the Internet: A Virtual Counter-Revolution', (2010) < http://www.economist.com/node/16941635>.

[603] Ian Brownlie, *Principles of Public International Law,* (Oxford University Press 2012) p. 289.

[604] Malcolm N. Shaw, 'Territory in International Law' 13 Netherlands Yearbook of International Law (1982) 61, p. 81.

(d) capacity to enter into relations with other states.[605]

The principle is also enshrined in various international treaties. For instance, Article 2(1) of the UN Charter states that:

> [t]he Organization is based on the principle of sovereign equality of all its Members.[606]

The 1970 UN *General Assembly Declaration on Principles of International Law Concerning Friendly Relations and Co-operations Among States in Accordance with the Charter of the United Nations* further elaborates on this notion by stating that 'all states enjoy sovereign equality […] Each state enjoys the right inherent in full sovereignty'.[607]

Sovereignty in international law epitomises the very essence of the state, namely the power over generally defined territory and inhabitants under its control. It is also a political concept, symbolized by Hobbes' Leviathan and described by Boldwin, as internal strength and external limitation of power.[608] Krasner[609] developed a modern definition of the term, which comprises four elements: (1) international legal sovereignty, which denotes the practices associated with mutual recognition, usually between territorial entities that possess formal juridical independence; (2) Westphalian sovereignty, which describes political organization based on the exclusion of external actors from authority structures within a specific territory; (3) domestic sovereignty, which is the ability of a state to exercise effective control within its territory and the competence to construct formal organizations of political authority within the polity; and (4) independence sovereignty, which describes the ability of public authorities to regulate the flow of information, ideas, goods, people, pollutants or capital across the borders of their state.[610] Krasner considers sovereignty as a polity of complex ideas comprised of

---

[605] Convention on Rights and Duties of States (Montevideo Convention), 26 December 1933, 165 LNTS 20, Article 1.
[606] Charter of the United Nations, San Francisco, 26 June 1945, art. 2(1).
[607] *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations,* adopted by resolution 2625 (XXV) 24th October 1970.
[608] Gbenga Oduntan, *Sovereignty and Jurisdiction in the Airspace and Outer Space* (Routledge 2012) p. 21.
[609] Stephen Krasner, *Sovereignty: Organised Hypocrisy* (Princeton University Press 1999) pp. 3-4.
[610] ibid.

separate, but related components. The international legal and Westphalian sovereignties are focused on the issues of legitimacy and authority, but exclude control, which he confines to the exercise of sovereign powers within the state. Thus, sovereignty in international relations is no longer an absolute right of states to political self-determination, but rather a set of obligations circumscribed by international treaties aimed to encourage closer cooperation to promote, *inter alia*, international peace and security,[611] economic development, trade, international finance, labour, human rights protection, health and communications.[612] To achieve these aims, states agreed to put restrictions on sovereignty and delegated some of their powers to international and regional institutions, such as the United Nations, the European Union and the African Union. This augmentation of state powers prompted some observers to express concern that sovereignty is in decline. For example, Simma and Pulkowski note, that law on international level is increasingly

> […] a spread-out web of normativity. States are shown, as inexorably losing ground. Juxtaposed pyramidal arrangements of state law are increasingly being replaced by more, or less confused and overlapping networks of normativity, arranged in tangled hierarchies-even though many residues of the former model, stay unperturbed.[613]

Others regret the erosion of omnipotent sovereignty on account of globalization[614] and attribute a variety of factors as a root cause of this trend, such as human rights protection, exchange rates, monetary policy, arms control, chemical weapons, landmines, warfare, environmental control, all of which make policy options opened to states in any real sense increasingly constrained.[615] As a consequence of these trends, the rules promulgated by intergovernmental organizations have been increased in depth and density, whereas national courts, administrative agencies and even parliamentary bodies are said to increasingly function as part of cooperative regulatory and enforcement trans-governmental networks and no longer

---

[611] Article 1(4) UN Charter specifies that one of the purposes of the United Nations is to 'maintain international peace and security'.
[612] Article 1(3) UN Charter calls for international cooperation 'in solving international problems of an economic, social, cultural, or humanitarian character and in promoting and encouraging respect for human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion'.
[613] Bruno Simma and Dirk Pulkowski, 'Of Planets and Universe: Self-Contained Regimes in International Law' (2005) 17 European Journal of International Law p. 529.
[614] Oduntan, supra note 206.
[615] ibid.

as simply parochial national institutions.[616] Krasner concurs with this analysis. His idea of sovereignty, as 'organized hypocrisy' corresponds with the mainstream opinion that with changes to the basic nature of the international legal system, the scope of activities over which states can effectively exercise control is declining.[617] Some writers take the opposite view and assert that through this diffusion, rather than weakening, sovereignty has been strengthened in recent years to become 'the new sovereignty', described as a 'right and capacity to participate in international institutions that allow their members, working tighter, to accomplish ends that individual governments alone could once never hoped to accomplish'.[618]

(i) Territorial Sovereignty

The idea of sovereignty and territory are closely related in international law and denote an exercise of governmental control over some defined, geographical space. Territory not only links the idea of sovereignty, land and people, but is an area, which can be both spatial and locational.[619] Understood as an area, territory can be maritime, aerial, or celestial 'as long as it is a space, place or sphere of physical activities capable of being occupied by use of, or passage'.[620] International law does not require any specific size of an area to be called a state- Monaco's territory for example is less than 0.5 km2.[621] Nor are the size of the population, or clearly defined boundaries a pre-requisite of statehood. This last point was affirmed by the International Court of Justice in the *North Sea Continental Shelf Case,*[622] where it was stated that:

> [t]he appurtenance of a given area, considered as an entity, in no way governs the precise delimitation of its boundaries, any more than uncertainty as to boundaries can affect territorial rights. There is for instance no rule that the land frontiers as a [s]tate must be fully delimited and defined and often in

[616] Philip Alston, 'The Myopia of the Handmaidens: International Lawyers and Globalization' (1997) 3 European Journal of International Law.
[617] Krasner, supra note 307.
[618] Ann-Marie Slaughter, 'Security, Solidarity and Sovereignty: The Grand Themes of UN Reform' 99 American Journal of International Law (2005).
[619] Stuart Eden, 'Missing the Point: Globalization, Deterritorialisation and the Space of World', 30 Transactions of the Institute of British Geographers (2005) pp. 8-19
[620] Oduntan, supra note 306, p. 11.
[621] Malcolm Evans, *International Law* (Oxford University Press 2010) p. 219.
[622] *North Sea Continental Shelf,* Judgement, ICJ Reports 1969.

various places and for long they are not.[623]

What is important though, is the right of a government to control what happens within the state to the exclusion of other states, as articulated by Judge Max Huber in the leading case on the subject, *The Isle of Palmas Arbitration,*[624] where he summarised this concept as follows:

> [s]overeignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of the state.[625]

Judge Max Huber also defined the term 'territorial sovereignty' stating that:

> [t]erritorial sovereignty […] involves the exclusive right to display the activities of a [s]tate. This right has as corollary a duty: the obligation to protect within the territory the rights of other [s]tates, in particular their right to integrity and inviolability in peace and in war, together with the rights which each [s]tate may claim for its nationals in foreign territory.[626]

Thus, territory, as a component of statehood, plays a crucial role. However, territorial sovereignty is not confined purely to land, but also comprises subterranean areas, waters, rivers, lakes, the airspace above the land (although there is no international agreement, as to the precise upper limit) and 12 miles of territorial sea adjacent to the coast.[627] In this sense, international law has extended the label 'territory' and the sovereign rights and duties that accompany it to categorize these additional resources,[628] or spaces. The demarcation of such spaces plays an important role in modern international relations, since it makes good policy in both the domestic and international legal orders for there to be distinct territories and a fundamental understanding of the juridical nature of all forms of physical and extraterrestrial

---

[623] ibid, para 46.
[624] *Isle of Palmas Arbitration* (The Netherlands v United States) 2 RIAA (1928) 829.
[625] ibid.
[626] ibid.
[627] Brownlie, supra note 301, p. 66.
[628] Duncan B. Hollis, 'Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace', CyberDialogue 2012.

territories.[629] It follows that wherever possible, the precise distinction in terms of delimitation and demarcations of all territories must always be attempted, even if not achieved.[630] Classical international law recognizes five modes of acquisition of territory, namely occupation, prescription, cession, accretion and conquest.[631] 'Occupation' is derived from *occupio*, a mode of acquisition in Roman law, by which 'a person obtains absolute title by first possessing a thing that previously belonged to no one, such as a fish in the sea, or a wild bird'.[632] Some writers believe that occupation is the acquisition of *terra nullius*-that is territory which, immediately before acquisition, belonged to no state, either because it has never belonged to any state, or has been abandoned,[633] or territory not possessed by a community having a social and political organization.[634] Very rarely can a territory be considered as belonging to no one these days, save for some islands that come about, as a result of geological activity, since most of the land areas of the globe are placed under territorial sovereignty of an existing state.[635]

The question that arises in the context of cyberspace, is whether for the purposes of acquiring sovereign rights through occupation, cyberspace could be considered as *terra nullius.* Undoubtedly, to be viewed as such was an aspiration of those among the cyber libertarians, who believed in an idea of a 'global village' of shared resources and a borderless world of global transnationalism,[636] as for instance was the case with Barlow and Johnson and Post. Their views that international law principles, such as sovereignty do not apply to cyberspace and that the internet constitutes a distinct physical space or a different jurisdiction are now very much confined to the cyber-libertarian discourse of that era. The idea that the principle of state sovereignty applies in cyberspace is now accepted[637] and evidenced in state practice. Indeed, the International Group of Experts contributing to the *Tallinn Manual 2.0* agreed that 'various aspects of cyberspace and [s]tate cyber operations are not beyond the reach of the principle of

[629] Obudan, supra note 306, p. 12.
[630] ibid.
[631] Brownlie, supra note 301, p.127
[632] *Black's Law Dictionary* (West Group 1999) p. 1106.
[633] Peter Malanczuk, *Akehurst's Modern International Law,* (Routledge 2002) p. 148.
[634] Brownlie, supra note 301 p. 135.
[635] ibid.
[636] Barlow, supra note 160. Barlow in his 'Declaration of Independence of Cyberspace' famously said that 'cyberspace is a new home of mind…where governments have no sovereignty and which does not lie within their borders…but that it is an act of nature it grows itself through a collective action'.
[637] *Tallinn Manual 2.0,* supra note 7, Rule 1.

sovereignty'.[638] To date cyberspace may not have yet been demarcated along the territorial lines, but its component parts belong to states, or private organizations. States therefore 'enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure'.[639] The principle of sovereignty applies to all three layers of cyberspace-the physical, logical and content (social). [640] Thus, the physical layer (that is the hardware and other infrastructure such as cables, routers, servers etc.,) is owned by private organizations and/or under the control of states. It follows that '[s]tates enjoy sovereignty over any cyber infrastructure located on their territory and activities associated wit that cyber infrastructure'.[641] Consequently, as observed by Buchan

> […]where computer networks are interfered with, or where information is interfered with that is located on [the] networks and those networks are supported by cyber infrastructure physically located in a state's territory, that state's territory can be regarded as transgressed and thus a violation of the principle of territorial sovereignty occurs.[642]

Irrespective of who the infrastructure belongs to (whether to government institutions, private companies, or individuals), it will be protected by the principle of territorial sovereignty, so long as it is located on the territory of that state.[643] Equally, the individuals and groups who make the internet operational and its users (the content layer) are subject to authority of states. The logical layer is a result of someone's intellectual endeavour, subject to intellectual property rights and therefore also subject to state's authority. If there was any doubt as to the fact that the internet is not free from regulation and consequently, state authority, it has been dispelled by state practice evidenced by many governments using various techniques to control, censor and filter online information, the Great Firewall of China being the obvious example. Indeed, Lessing argued that 'technology allows us to do or prevents us from doing all the things we

---

[638] UN GGE 2013 Report, supra note 5, para 20; UN GGE 2015 Report, supra note 5, paras. 27, 28(b).
[639] *Tallinn Manual 2,0*, supra note 7, Rule 1, p. 11.
[640] ibid, Rule 1, p. 12.
[641] ibid.
[642] Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage', in Anna Maria Osula and Henry Roigas (eds.,), *International Cyber Norms: Legal, Policy & Industry Perspective* (NATO CCD COE Publications, Tallinn 2016), 65-86, p. 71.
[643] ibid.

can or cannot do on the internet and technology can be shaped so as to enshrine values of liberty, or values of control'.[644] Being dependent on technology and people who run, operate and use it, it is possible in theory that cyberspace may one day cease to exist, unlike the natural areas of *terra nullius*. It could be said that cyberspace simply does not seem to fit within the legal definition of unclaimed territory, because it does not possess such attributes.

Some legal scholars, such as Brownlie, suggest however that the requirement of *terra nullius* is not the only prerequisite of acquisition by occupation.[645] In fact, 'effective occupation' is a far stronger basis of acquisition than *terra nullius*. 'Effective occupation' is, however a relative concept and varies according to the territory concerned.[646] In the *Eastern Greenland case*[647] the Permanent Court of International Justice asserted that

> [a] claim to sovereignty based not upon some particular act of title, such as a treaty of cession, but merely upon continued display of authority, involves two elements, each of which must be shown to exist: the intention and will to act as sovereign and some actual exercise or display of such authority.[648]

This has been affirmed in the *Eritrea/Yemen Arbitration* case, where it was unanimously held that

> [t]he modern international law of acquisition of territory generally requires that there be: an intentional display of power and authority over the territory, by the exercise of jurisdiction and state functions on a continuous and peaceful basis.[649]

The question that arises is therefore could states claim sovereignty in cyberspace based on effective control, that is, to re-iterate Judge Max Humber's pronouncement in the *Isle of Palmas* case, to 'exercise therein, *to the exclusion of any other state*, the functions of a state'?[650] The internet was founded on a distributed and decentralized technology and although the early days of its entrepreneurship were a testament to the spread of an unbridled global internet

---

644 Lessing, supra note 179.
645 Brownlie, supra note 301, pp. 133-135.
646 ibid.
647 *Eastern Greenland Case* (1933) PCIJ, series A/B, no. 53.
648 ibid.
649 *The Eritrea/Yemen Case*, 114 International Law Reports.
650 ibid.

freedom, the nationalistic tendencies soon crept in. These tendencies, Shultz noted, ushered in a 'greater assertion of state power and a greater control over national territories as far as information flows are concerned'.[651] Thus, the dark side of the web, which manifested itself as, for instance hate speech websites, unregulated online casinos, pornography sites and the like, triggered a movement for cultural and nationalistic withdrawal.[652] So prevalent are the domestic information controls these days (that is actions conducted in and through cyberspace that seek to deny, disrupt, manipulate and shape information for strategic and political ends), that they became a subject of a burgeoning area of cyberspace research.[653] A number of means are used and broadly speaking, comprise a variety of technologies, regulatory measures, laws, policies and tactics. They include media regulation, licensing regimes, content removal, libel and slander laws, together with content filtering.[654] Some states, such as the US and France, control local internet intermediaries: the people, equipment and services within national borders that enable local internet users to consume the offending internet communications.[655] Most important of these intermediaries are the Internet Service Providers (ISPs), search engines, browsers, the physical network and their sources of funds.[656] Such internal controls, according to Goldsmith and Wu 'make it harder for local users to obtain content from, or transact with, the law-evading content providers abroad. In this way, government affects internet flow within their borders even though they originate abroad and cannot easily be stopped at the border',[657] especially so, since content providers cannot subvert intermediaries because they cannot do without them. The most basic of cyberspace controls is internet filtering, or censorship, that is the prevention of access to information online within territorial boundaries, which is justified on a variety of grounds depending on the government involved. The rational for censorship include copyright violation, sexual exploitation of children, or promotion of hatred and violence.[658] Non-democratic regimes, such as China, filter content related to minority rights (Tibetan independence), democracy sites (Amnesty International,

[651] Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface', 19 European Journal of International Law (2008) 799 p. 801.
[652] ibid.
[653] Ronald Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls', 18 Global Governance (2012) 339.
[654] ibid.
[655] Goldsmith and Wu, supra note 181, p.68
[656] ibid.
[657] ibid.
[658] Deibert and Crete-Nishihata, supra note 351.

Human Rights Watch, Hong Kong Voice of Democracy), news sites (BBC News, CNN, Time Magazine), government (Voice of America, US Department of Defence).[659] Apart from regulatory and legal measures, states have also shown willingness to disrupt communication networks for political purposes, sometimes at the time of elections, on other occasions during public demonstrations. These activities have been named 'just-in-time-blocking' and described by the OpenNet Initiative, as denial of access to information during important political moments when the content may have the greatest potential impact, such as elections, protests, or anniversaries of social unrest.[660] Both democracies and autocracies have been known to employ such tactics: during the 2011 Arab Spring (Egypt and Libya), Nepal in 2005 and Burma in 2007.[661] In 2011 the then UK Prime Minister David Cameron said in the House of Commons in response to the 2011 riots in the UK that 'we are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via [social media] when we know they are plotting violence, disorder and criminality'.[662]

This state practice is a clear indication that states can and do exercise a degree of control over the internet content. However, as has been agreed by the International Group of Experts involved in the *Tallinn Manual 2.0* 'no [s]tate may claim sovereignty over cyberspace *per se'*, because 'much of cyber infrastructure comprising cyberspace is located in the sovereign territories of [s]tates'.[663] The reason why any given state cannot claim full sovereignty over the entirety of cyberspace lies in the inability to exercise the the exclusion of any other state, the functions of the state.[664] For example, the Russian authorities have been particularly vocal in this regard, expressing their dissatisfaction with American companies as Google, Facebook and Twitter, which in their view undermine the Russian values and the political system. Consequently, both houses of parliament called for tighter controls. Suggestions have been made that all servers, on which Russian citizens' personal data are stored should be located in Russia. A media campaign was started to bring global web platforms under Russian jurisdiction-either requiring them to be accessible in Russia by a domain name extension of .ru, or obliging them to be hosted on Russian territory.[665] Deputy Prime Minister Dmitry

---

[659] Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China', Berkman Centre Internet and Society <http://cyber.law.harvard.edu/filtering/china>.
[660] ibid.
[661] ibid.
[662] British Prime Minister's Office, 'PM Statement on Disorder in England' 11th August 2011, <www.number10.gov.uk/news/pm-statement-on-disorder-in-england>.
[663] *Tallinn Manual 2.0* supra note 7, Rule 1, p. 13.
[664] *Isle of Palmas*, supra note 322.
[665] Noscetti, supra note 237.

Rogazin stated that services, such as Facebook and Twitter, are elements of a larger American campaign against Russia, whilst President Putin in April 2014 publicly described the internet as a 'CIA project', confirming that the Kremlin is infuriated by America's stranglehold on the web in terms of both infrastructure (networks, monopoly in naming and addressing) and the pre-eminence of American companies.[666] Furthermore, as the Russians note, ten out of thirteen root servers that are essential for the functioning of the entire internet are located in the US and the other three on the territory of US allies-Japan, the Netherlands and Sweden.[667]

It seems therefore that effective control over cyberspace to the exclusion of other states is not feasible. As a consequence, states cannot claim full sovereignty in this domain. Having said that:

> [t]he fact that cyber infrastructure located in a given [s]tate's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty. Indeed, [s]tates have the right, pursuant to the principle of sovereignty, to disconnect from the [i]nternet, in whole or in part […].[668]

(ii) Other Legal Regimes

World resources are allocated their own categories under international law and governed by different types of legal regimes and institutions. As noted above, a broadly demarcated territory is the basic building block of statehood, within which a government can exercise its right to political self-determination.[669] In some cases, international law provides for full sovereignty over a territory (and/or area), as is for example the case with the airspace. Article 1 of the 1944 Chicago Convention states that 'the contracting states recognize that every state has complete and exclusive sovereignty over the airspace above its territory'.[670] In other cases, for instance the territorial waters, which cover twelve miles of the adjacent sea and seabed, state have sovereignty but treaty and customary international law allows limited rights to other states therein, such as the right of innocent passage.[671] Apart from territory,

---

[666] ibid.
[667] ibid.
[668] *Tallinn Manual 2.0*, supra note 7, Rule 1 pp. 12-13.
[669] Schultz, supra note 349, p. 800.
[670] Convention on International Civil Aviation, Chicago 7 December 1944,
[671] UN Convention on the Law of the Sea, 10 December 1982 (UNCLOS), 1833UNTS 396, art 17:

international law has also developed additional ways to categorise the Earth's resources, among them *terra nullius* (an unclaimed territory, for instance a new volcanic island) and *res communis* (things common to all, that cannot be owned or appropriated, such as light, air and the sea).[672] This categorization applies to the high seas, the outer space and the Antarctic, which despite having their own disparate legal regimes, share one thing in common, namely that states are barred from claiming sovereignty in these domains. Thus, Article 87 The Law of the Sea Convention 1982 (UNCLOS) states that 'the high seas are open to all states, whether coastal or landlocked'[673] and lists specific rights that all states may enjoy, including the right to navigate, of over flight and fishing. The Convention makes any claim to sovereignty over high seas invalid by virtue of Article 89, which reads, 'no state may validly purport to subject any part of the high seas to its sovereignty'.[674] The outer space has likewise been given status of *res communis* by virtue of Article II of the Outer Space Treaty, which provides that 'outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[675] However, the fact that sovereignty cannot be claimed over these areas, does not necessarily exclude exercise of jurisdiction. This is evidenced for example by Article VIII of the Outer Space Treaty, according to which: 'a State Party to the Treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object and over any personnel thereof, while in outer space or on a celestial body'.[676] Furthermore, there are instances, where the law allowed for the extension of sovereign rights (but not full sovereignty) and the exercise of jurisdiction in areas previously classified, as part of the *res communis*. One such example is the exclusive economic zone (EEZ), established under Article 55 the UNCLOS 1982 and described as 'an area beyond and adjacent to the territorial sea, subject to the specific legal regime […] under which the rights and jurisdiction of the coastal [s]tate and the rights and freedoms of other [s]tates are governed by the relevant provisions of this Convention'.[677] The EEZ 'confers upon coastal states sovereign rights for the purpose of exploring and

---

'subject to this convention, ships of al States, weather coastal, or landlocked, enjoy the right of innocent passage through the territorial sea.'

[672] *Black's Law Dictionary*, supra note 318, p. 1308

[673] UNCLOS, supra note 369, art 87.

[674] ibid, art 86.

[675] The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space 1968 18 UST 2410.

[676] ibid; art VIII.

[677] UNCLOS, supra note 369, art 55.

exploiting, conserving and managing, the living and non-living resources'[678] of the water column, seabed and subsoil to a distance of 200nm.[679] The regime extended costal states' rights to cover one third of ocean space and it must be stressed that it 'was conceived primarily, as a jurisdictional zone, rather than one of absolute sovereignty and therefore could not interfere with traditional high seas freedoms'.[680] Thus the EEZ has been described, as

> combining characteristics of the territorial seas and the high seas, but cannot be assimilated to either. It is a *sui generis* zone with its own distinctive regime. Unlike the territorial sea, it is not an area, in which coastal states have a plenary and *ipso jure* entitlement to sovereignty and in contrast to the high seas, it is not a zone in which other states have unfettered freedoms. It is an amalgam, or multifunctional' zone, in which coastal states enjoy sovereign rights in relation to economic resources and also jurisdiction not only in relation to these rights, but also for certain other matters including environmental protection.[681]

Article 55 of the UNCLOS 1982 gives EEZ a status of 'specific legal regime' and has been described as 'remarkably durable and free from major controversy…successfully melding aspects of both sovereign rights (ownership or *dominium*) and jurisdiction (competence or *imperium*)'.[682]

Another example of such legal innovation is that relating to the continental shelf, which in geographical terms is described, as a sloping platform of submerged land surrounding the continents and islands, normally extending to a depth of approximately 200 meters, at which point the seabed fall away sharply.[683] Its legal definition is contained in Article 76 UNCLOS 1982, which states that:

> [t]he continental shelf of a coastal State comprises the sea-bed and subsoil of the submarine areas that extends beyond its territorial sea throughout the natural prolongation of its land territory to the outer edge of the continental margin, or to a distance of 200 nautical miles from the baselines from which the breadth of the

[678] ibid, art 56(1)(a).
[679] Donald Rothwell and Tim Stephens, *The International Law of the Sea* (Hart Publishing 2014) p. 82.
[680] ibid p. 83.
[681] ibid p. 84.
[682] ibid.
[683] Obuntan, supra note 306, p. 141

territorial sea is measured whether the outer edge of the continental margin does not extend up to that distance.[684]

By virtue of Article 77(1) UNCLOS 1982 coastal states have a right to exercise sovereign rights over the continental shelf, for the purpose of exploring and exploiting its natural resources. They also have a freedom to decide whether, or not to explore or exploit it and whether, or not to grant access to other states.[685] Additionally, Article 77(4) gives coastal states sovereign rights over all natural resources, both living and non-living. Although there is a substantial overlap between the EEZ and continental shelf regimes, in that both give to coastal states essentially the same rights to exploit the non-living and living resources of the seabed and subsoil of an area of up to 200nm, they differ in that continental shelf need not be proclaimed and vests inherently in coastal states, unlike EEZ, which must be asserted.[686]

These two separate but related regimes illustrate that the legal bases for exercising sovereign rights and jurisdiction can be on occasion provided for by international law, where states cannot claim full sovereignty. Both the EEZ and continental shelf are legal constructs, which have been successfully deployed to provide means for states to explore, exploit and protect certain areas, where claiming full sovereignty is restricted. Chapter 3 of the thesis will discuss these regimes in more detail, with the view of ascertaining whether some aspects of cyberspace management could be modelled on them, whilst the next part of this chapter will show how states exercise their jurisdiction in the cyber context.

(b) Jurisdiction in Cyberspace

States' regulation and control of parts of cyberspace is not only feasible, it has been already undertaken to such an extent that some authors, fear its fragmentation.[687] The variety of means and methods outlined above to subject content of information to state control could be viewed collectively, as governments exercising sovereign rights. Such exercise of state powers within a given territory is known in international law as jurisdiction, which is defined as:

[684] UNCLOS, supra note 369, art 76.

[686] Rothwell and Stephens, supra note 377.

[687] Schultz, supra note 349; Christopher Bronk, 'Who Leads? Avoiding the Balkanization of Cyberspace' Cyber Security (2014) <http://www.ins.ethz.ch/Digital-Library/Articles/Detail/?id=181188>.

> [t]he power of the state under international law to regulate or otherwise impact upon people, property and circumstances and reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs.[688]

Whilst the term 'sovereignty' covers the total legal personality of a state, jurisdiction refers to particular aspects of the substance, especially rights (or claims), liberties and powers.[689] It is a vital and central feature of sate sovereignty, as it is an exercise of authority, which may alter, create or terminate legal relationships and obligations.[690] Jurisdiction thus pertains the power of states to subject persons or property to their laws, judicial institutions, or enforcement capacity.[691] This corresponds to three types of jurisdiction, namely legislative, judicial and enforcement.[692] Legislative jurisdiction 'refers to the supremacy of the constitutionally recognized organs of the state to make binding laws within its territory.'[693] Judicial jurisdiction empowers state's courts may try cases concerning the persons, property or events, whilst enforcement jurisdiction means that the executive has the capacity to enforce the judgments or convictions against the defendant or accused. Unlike the legislative and adjudicative jurisdiction, enforcement jurisdiction is strictly territorial. This means that generally state officials may not carry out their functions on foreign soil, unless the host state expressly consents to it.[694] Thus, if states enforce their laws abroad, this would constitute violations of the principles of territorial sovereignty and non-intervention.[695]

International law does not seem to impose restrictions on the jurisdiction of courts in civil cases, but it restricts jurisdiction in criminal cases.[696] This occurs on the basis of the territoriality, nationality, protective and universal principles.[697]

---

[688] Malcolm N. Show, *International Law* (Cambridge University Press 2008), p. 645.
[689] ibid, p. 90.
[690] ibid, p. 645.
[691] Illias Bantekas, 'Criminal Jurisdiction of States under International Law', *Max Planck Encyclopedia of Public International Law* (2011) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1021?rskey=kGhm7J&result=3&prd=EPIL>
[692] Malanczuk, supra note 331, p. 109.
[693] Show, supra note 386, p. 645.
[694] ibid. p. 651.
[695] *Isle of Palmas Arbitration*, supra note 322, para 838.
[696] Malanczuk, supra note 331, p. 110.
[697] *Max Plank Encyclopedia*, supra note 389. The nationality principle confers on states the power to subject their own nationals to judicial and legislative criminal jurisdiction for crimes they have committed abroad. The protective principle confers on a state power to prosecute

Territorial jurisdiction is the simplest and the least contentious form of criminal jurisdiction, even in respect of enforcement and usually established by the legislative and judicial practice of states in two ways.[698] The first is on the basis of the so-called subjective territoriality principle, which may be asserted by those states, where the criminal conduct commenced.[699] The second, the objective territoriality principle, allows a state to assert its jurisdiction and prosecute the offender where the criminal conduct caused injurious effect within the territory of the effected state, hence also referred to as the 'effects doctrine'.[700]

The nature of territoriality principle was examined by the Permanent Court of International Justice (PCIJ) in the well known case of *Lotus,*[701] which established a number of important rules. First, a state cannot exercise its jurisdiction outside its territory, unless an international treaty or customary law permits it to do so. The Court held that:

> [n]or the first and foremost restriction imposed by international law upon a [s]tate is that-failing the existence of a permissive rule to the contrary- it may not exercise its power, in any form in the territory of another state. In this sense, jurisdiction is certainly territorial; it cannot be exercised by a state outside its territory except by virtue of a permissive rule derived from international custom or from convention.[702]

Secondly, a state may exercise jurisdiction within its territory in any matter (civil and criminal) even if there is no specific rule permitting it to do so. It follows, that states have a wide measure of discretion, which is only limited by a prohibitive rule of international law. The PCIJ explained:

---

offenders and enforce its laws in respect of extraterritorial acts that threaten or harm its national security interests whilst universal jurisdiction applies to two categories of offences (a) certain crimes that are universally considered heinous and repugnant and (b) crimes committed in locations that are beyond the exclusive authority of any state. These are piracy and war crimes and are accepted by most countries as subject of universal jurisdiction which means that any state can prosecute an alleged offender and punish him if convicted irrespective of the place of commission of the crime and regardless of any link of jurisdiction recognized by international law.

[698] ibid, para 4.

[699] ibid.

[700] ibid, and Malanczuk, supra note 331, p. 111.

[701] *The Case of the SS 'Lotus'* (France v Turkey) [1927] PCIJ Reports, Series A, No. 10.

[702] ibid, para 45.

> [i]t does not, however, follow that international law prohibits a [s]tate from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to [s]tates to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed [s]tates to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that [s]tates many not extend the application of their laws and jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every [s]tate remains free to adopt the principles which it regards as best and most suitable. This discretion left to [s]tates by international law explains the great variety of rules which they have been able to adopt without objections or complaints on the part of other [s]tates […]. In these circumstances all that can be required of a [s]tate is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty.[703]

Thirdly, the PCIJ endorsed the 'effects doctrine' as a basis for legislative jurisdiction. The PCIJ allowed the Turkish court to exercise its jurisdiction with respect of acts committed outside its territory because 'one of the constituent elements of the offence, and more specifically its effects have taken place'[704] in that state. In doing so, the Court equated the Boz-Kourt (the Turkish vessel) to the Turkish territory and found that the effects of the French captain's actions of the Lotus were felt within Turkey and thus Turkish courts could prosecute the French captain.[705]

---

[703] ibid. para 46.
[704] Ibid.
[705] UNCLOS, supra note 369, art 97(1), which restated art 11(1) of the 1958 Geneva Convention on the High Seas, reversed this aspect of the *Lotus* decision. A ship on high seas, where a criminal offence has been committed, is treated as if it were the territory of the flag state.

The *Lotus* principle, according to which that which is not prohibited by international law is permitted, has been subsequently affirmed by the International Court of Justice (ICJ) in its 2010 Advisory Opinion on the *Declaration of Independence of Kosovo.*[706] This concerned a request for an advisory opinion from the ICJ by the UN General Assembly (UN GA) regarding the 2008 Kosovo declaration of independence from Serbia. The Court considered the legality of the declaration from three perspectives, asking *inter alia* the following question: 'is the unilateral declaration of independence by the Provisional Institutions of Self-Government of Kosovo in accordance with international law'?[707] The ICJ interpreted the request from the UN GA narrowly and provided an opinion on whether or not the declaration of independence was in accordance with international law and not the issues regarding the extent of the right to self-determination, or the existence of any right to secession.[708] In deciding that the declaration was not prohibited, the Court stated that there was no practice in general international law, which allowed it to conclude that declarations of independence are prohibited.[709] The adoption of the declaration of independence did not violate general international law, the SC Resolution 1244 (1999) or its Constitutional plan and therefore the adoption of that declaration did not violate any applicable rule of international law.[710] In order to answer this question the ICJ relied on the *Lotus* judgement stating that in relation to a specific act it is not necessary to demonstrate a permissive rule so long as there is no prohibition.[711] The ICJ focused on whether there are prohibitive rules against declarations of independence in international law and not whether international law conferred a positive entitlement on Kosovo unilaterally to declare its independence, or whether international law generally confers an entitlement on entities situated within a state unilaterally to break away from it.[712]

[706] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (ICJ Advisory Opinion) 22 July 2010.
[707] ibid. The ICJ was also considered whether the declaration was prohibited by the UN Security Resolution 1244 and the Ahrisaari plan (a proposal, which defined Kosovo's internal settlement, minority protection mechanism and allowed for independence under international supervision).
[708] ibid, para 51.
[709] ibid.
[710] ibid, para 122.
[711] ibid, para 123.
[712] ibid, para 56.

(i) State Jurisdiction in Cyberspace

The primary basis for the exercise of jurisdiction in cyberspace is territorial.[713] Thus, a state can exercise territorial jurisdiction over (a) cyber infrastructure and persons engaged in cyber activities on its territory; (b) cyber activities originating in, or completed on, its territory; or (c) cyber activities having a substantial effect in its territory.[714] This is because 'under international law, a [s]tate enjoys full territorial jurisdiction (prescriptive, enforcement and judicial) over persons and objects located on its territory, as well as conduct occurring there'.[715] Any cyber activity originating in a state's territory will be subject to the subjective territorial jurisdiction, notwithstanding whether it has an extraterritorial effect.[716] In addition, a state will be able to exercise jurisdiction on the basis of the effects doctrine (i.e. the objective territorial jurisdiction) in relation to a cyber activity that originates outside its territory, but which is completed within it, if the act concerned is directed against persons or objects located there, or is otherwise intended to culminate in that state.[717] The effects doctrine has been increasingly accepted as the basis for jurisdiction with regards to 'acts, including cyber operations that do not originate, conclude, or materially take place in the state in question, but have effect therein'.[718] However, this basis for establishing jurisdiction may cause friction among states in circumstances where, for instance, the effects of a particular cyber operation may be felt in many different states. In that sense, the doctrine remains controversial and the conditions imposed on it are not yet fully settled in international law.[719] Nevertheless, the International Group of Experts drafting the *Tallinn Manual 2.0* agreed that '[the effects doctrine] may now reasonably be said to reflect customary international law'.[720]

States have consistently asserted their right to regulate online activity using the territorial link to assert prescriptive and adjudicative jurisdiction on the basis of the effects felt in their country. An early and well known example in the criminal context is the French case

[713] The extent of extraterritorial human rights obligations regarding states' activities in cyberspace will be examined in Chapter 4 of this thesis, 'The Right to Privacy in the Digital Age'.
[714] *Tallinn Manual 2.0,* supra note 7, Rule 9, p. 55
[715] ibid, para 4, p. 52.
[716] ibid. para 5, p. 56.
[717] ibid.
[718] ibid, para 10, p. 57.
[719] ibid. para 13, p. 58
[720] ibid. para 11, p. 58.

of *LICRA & UEJF v Yahoo France.*[721] The case concerned an action brought by two French Jewish organizations against Yahoo! Inc. (an American organization) for allowing individuals in France to buy Nazi memorabilia from third parties on Yahoo's auction site. The website was hosted by Yahoo!, provided by an American server, but accessible from France and elsewhere in the world. Offering for sale such objects is protected in the US by the First Amendment, but illegal in France.[722] The Tribunal de Grande Instance de Paris found that it had jurisdiction over the case and ordered Yahoo! to take down the website and to pay a fine. The Court asserted its jurisdiction on the basis of the effects the internet behaviour had in France, stating that 'by permitting the display of these items and the possible participation of internet users in France in such an exposition/sale, Yahoo commit[ed] a wrong within French territory'. [723] Furthermore, 'the harm was suffered on the territory of France', because the site was accessible in France and therefore had to comply with French law, even though the material offered for sale was legal in the US. Thus, the French Court asserted its jurisdiction over acts adversely affecting French territory, even though Yahoo website was clearly connected with the US, having being set up and maintained on a server situated in the US.[724] Since then this reasoning has been replicated many times by other courts-'each time legitimising the right of the destination state to assert control over foreign site based on its local accessibility'.[725] For example, in *R v Perrin*[726] it was held that the UK Court of Appeal had jurisdiction to bring charges against the defendant, a French national residing in the UK and operating a US hosted website, which published obscene material accessible in England. Mr. Perrin was convicted and sentenced under the UK Obscene Publications Act 1959, but argued that because of the worldwide nature of the internet, publishers could not foresee the legal requirements in all the individual states where the material could be accessed. He also alleged that the UK had no jurisdiction to bring charges against him because the company was registered and operated legally in the US. UK Court of Appeal reasoned however that if the UK courts were not able to examine publication related cases because the place of publication did not fall under the courts' jurisdiction, that would encourage publishers to publish in countries where prosecution

[721] *UEJF et LICRA v Yahoo! Inc. et Yahoo France*, Tribunal de Grande Instance de Paris, No RG:00/05308.
[722] Article 808 and 809 of the French New Code of Civil Procedures.
[723] ibid.
[724] Kohl supra note 6, p. 38.
[725] ibid.
[726] *R v Perrin* [2002] EWCA Crim 747. Other cases include *R v Töben* BGH (12 December 2000) 1StR 184/00, LG Mannheim; *Arzneimittelwerbung im Internet* BGH (30 March 2006) 1 ZR 24/03.

was unlikely. Furthermore, as Mr. Perrin was a UK resident, UK law was accessible to him. Consequently, he should have sought legal advice since he was carrying out professional activities in that country. Finally, the Obscene Publications Act 1959 applied to the transmission of data that was stored electronically.

Similar effects based approach can be seen in the civil context, in particular in relation to the defamation cases. An early example is the *Dow Jones & Co Inc v Gutnic*.[727] The case related to an article placed in Barron's Online, a subscription website uploaded in the US, published by Down Jones and making references to Joseph Gutnic. The High Court in Australia upheld the application of the Australian defamation law to Barrons Online. It therefore held that Mr Gutnic could sue for defamation at his primary residence and the place where he was best known, that is where the damage to his reputation was most likely to have occurred. The ruling allowed the victims of the alleged defamation in Australia to issue proceedings for defamation on the internet against any defendant notwithstanding his/her location. The High Court explained that 'if people wish to do business, or indeed travel to, or live in, or utilize the infrastructure of different countries, they can hardly expect to be absolved from compliance with the laws of those countries. The fact that the publication might occur everywhere does not mean that it occurs nowhere'.[728] Similarly, in *Harrods Ltd v Dow Jones Co. Inc*.,[729] Harrods Ltd, issued proceedings against Dow Jones in respect of an online article, which appeared in the US but not the European edition of the Wall Street Journal and its website for defaming the company in the UK. The website had only few visits from the UK, nevertheless the court allowed the claim to proceed in England as the victim was an English company with a well established reputation in the UK.

What these cases illustrate is the application of the objective territoriality principle under customary international law in civil and criminal context, which facilitates states' application of their national laws to online activities. As noted by the International Group of Experts in the *Tallinn Manual 2.0* 'the effects doctrine is of particular import in the cyber context because cyber means lend themselves to causing effects in [s]tates where the operations in question neither originate nor culminate'.[730] However, since the conditions imposed by the effects doctrine are not fully settled in international law, the International Group of Experts agreed that a state exercising effects-based jurisdiction with respect to cyber-related activities

[727] *Dow Jones & Co. Inc. v Gutnic* [2002] HCA 56.
[728] ibid, per Callinan J., para 186.
[729] *Harrods Ltd v Dow Jones Co. Inc*. [2003] EWHR 1162 (QB)
[730] *Tallinn Manual 2.0,* supra note 7, para 12, p. 58.

and the personas who engage in them, must do so in a reasonable fashion and with due regard to the interests of other states.[731] Accordingly, a state may exercise effects-based jurisdiction if (a) it has a clear and internationally accepted interest in doing so; (b) the effects which it purports to regulate must be sufficiently direct and intended or foreseeable; (c) those effects must be substantial enough to warrant extending the state's law to foreign nationals outside its territory and (d) the exercise of effects-based jurisdiction does not unduly infringe upon the interests of other states, or upon foreign nationals, without a significant connection to the state that purports to exercise such jurisdiction.[732]

However, as noted previously, enforcement jurisdiction, unlike the prescriptive and adjudicative jurisdiction is strictly territorial.[733] Indeed, the International Group of Experts in Rule 11 of the *Tallinn Manual 2.0* agreed that 'a [s]tate may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects and cyber activities on the basis of: (a) a specific allocation of authority under international law; or (b) valid consent by a foreign government to exercise jurisdiction on its territory'.[734] This strict territoriality, echoes the *Lotus* approach whereby 'the first and foremost restriction imposed by international law upon a [s]tate is that […] it may not exercise its power in any form in the territory of another [s]tate'.[735] Accordingly, the exercise of enforcement jurisdiction on another state's territory constitutes a violation of that state's sovereignty, except when international law provides a specific allocation of authority to do so, or by the consent of the state concerned.[736] This may sometimes be granted by means of a treaty, as is the case with the Cybercrime Convention, which permits state parties to 'access or receive, through a computer system in its territory, stored computer data located in another [p]arty, if the [p]arty obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the [p]arty through that computer system'.[737] However, the strict territorial limits in the context of enforcement jurisdiction have proved problematic, as states' law enforcement agencies often gain access to data stored outside of their territories without seeking and obtaining consent. This is also known as 'data pulling' and will be addressed in more detail in Chapter 4 of this thesis.

---

[731] ibid. para 13, p. 58.
[732] ibid.
[733] *Lotus*, supra note 399, para 18.
[734] *Tallinn Manual 2.0*, supra note 7, Rule 11, p. 66.
[735] *Lotus*, supra note 399, para 18a.
[736] ibid, p. 67.
[737] Convention on Cybercrime, supra note 31, art 32(b).

CONCLUSION

Cyberspace is a relatively new domain of human activity, which undoubtedly contributed to the expanse in commercial, communications and social activity. By its very architectural design it can be described as borderless and ubiquitous. This aspect of cyberspace lends itself to unlawful activities, such as state sponsored mass cyber surveillance. The recognition of challenges and dangers posed by belligerent acts in this domain reinforces the need for a basic agreement among nations to govern it. To this day however, there is no consensus relating the most fundamental aspects, as to how the management of this domain is to be achieved. This is reflected in both the lack of an agreement regarding an internationally legally binding cyber treaty and emergence of customary international law rules for this domain. This chapter sought to provide reasons for this lack of consensus, which seems to be underpinned by the political power struggle in the context of internet governance and divergent domestic and international cyber security policies of the major players. On the one hand, the US and other like- minded states support the idea of 'internet freedom', which to a limited extent echoes the attitudes of the internet founders- Barlow, Clark and Berners-Lee. On the other hand, the Russians and the Chinese champion 'internet sovereignty' and try to lay claim to their 'sovereign cyber territories' seeking to establish greater state control, preferably via a treaty and with involvement from the UN through the ITU. Conversely, the US and its allies insist on continuance with the multistakeholder system, which involves private and government actors, together with ICANN. Yet, both the ITU and ICANN have their drawbacks. The latter is a typical state-dominated institution, with little experience of running a dynamic and constantly evolving internet and related digital technologies. With states, as its constituent members, decision-making regarding the day-to-day overseeing of the internet will almost inevitably be riddled with political goal scoring and bureaucracy. Equally, ICANN has been almost constantly criticized for lack of international legitimacy and the perpetuation of American dominance in the global telecommunications sector. It therefore seems that to present the future of cyberspace governance, as a choice between 'internet freedom' and 'internet sovereignty' is an oversimplification. Considering the almost total domination of the US in the telecommunication sector through the provision of the hardware (with all route servers, upon which the internet is dependent located on the US and allied territories), the software and its dominance by the giant 'application' companies, such as Google and Microsoft, it could be said that the 'internet die has already been cast'. Nevertheless, state practice shows national control over the internet content. In this sense states have territorial jurisdiction over cyber

infrastructure and persons engaged in cyber activities on their territories together with cyber activities, which have a substantial effect on their territory on the basis of the effects doctrine. This to some degree resembles the legal regimes of the EEZ and continental shelf. However, no state may claim sovereignty over cyberspace *per se*, in the sense defined by Judge Huber in the *Isle of Palmas* Arbitration. The tendencies of some states evidenced by their application of national laws and standards to the transnational internet could eventually lead to the territorial fragmentation of the internet into national cyberspace, which would inevitably undermine freedom of expression and have economic, political and cultural costs.[738]

[738] Kohl, supra note 6, p. 54.

Chapter 3: 'The Role of International Law in Cyberspace Regulation'

INTRODUCTION

Cyber operations that amount to use of force, or to acts of hostilities, which are conducted during armed conflicts do not exist in a normative void. Existing international law, both *jus ad bellum* and *jus in bello,* applies to these type of operations. This view is shared by most states and acknowledged in two reports by United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunication Technologies in the Context of International Security (UN GGE) of 2013[739] and 2015.[740] In 2015 the UN GEE agreed on rules of behaviour in cyberspace also during peacetime, stating that nations should not use information and communication technologies to attack critical infrastructure and should not allow their territories to be used for internationally wrongful acts.[741] In addition, it has been widely accepted that international human rights law applies equally online and offline.[742] The disclosures of Edward Snowden in 2013 clearly articulated the breath of the cyber surveillance operations, which as will be shown in Chapter 4 of this thesis, is highly likely to amount to an unlawful interference with the right to privacy under international human rights treaties. Recently, the International Group of Experts acting on behalf of the NATO Cooperative Cyber Defence Centre of Excellence and tasked with articulating rules of public international law governing cyber operations in peacetime agreed that bulk collection of internet traffic and cyber surveillance may implicate international law norms.[743] The proliferation of cyber

[739] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (24 June 2013) UN Doc A/68/98.
[740] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (2015) UN Doc A/70/173.
[741] ibid.
[742] UN HRC, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UN Doc A/HRC/32/L.20; UN GA, 'The Right to Privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167; UN GGE Report 2013 supra note 1, para 21; UN GGE Report 2015 supra note 2, para 13(e); Agreement between the Governments of the Member States of Shanghai Cooperation Organization on Cooperation in the field of International Information Security, Art 4(1); Michael N. Schmitt and Liis Vihul (eds.,), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017), p. 179.
[743] *Tallinn Manual 2.0,* ibid, p. 170.

surveillance, other forms of peacetime cyber espionage (discussed in Chapter 1) and various deleterious cyber operations calls for closer international cooperation. One option, explored in this chapter, is regulation of state behaviour through a hard law instrument- an international treaty for cyberspace.

This chapter aims to lay down the conceptual foundations for such an instrument. It proposes to model the treaty on the existing principles of the international law of the sea. The rationale for doing so is that some parallels can be drawn between differing forms of governance for the world's resources contained in the United Nations Convention on the Law of the Sea 1982 (UNCLOS 1982) and cyberspace and applied by analogy to that environment in order to formulate a new legal regime.

This chapter is divided into five parts. Part one makes some comparisons between the historical development of the codification of the law of the sea and the those in the area of internet governance. Part two engages with the issue of cyberspace as a global common. Part three explores the utility of the application of the principle of Common Heritage of Mankind in the context of cyberspace governance. Part four picks up the discussion begun in Chapter 2 regarding the concepts of the Exclusive Economic Zone and Continental Shelf their application to cyberspace, whilst part five offers some conclusions.

1. THE APPLICATION OF THE PRINCIPLES OF INTERNATIONAL MARITIME LAW TO THE PROBLEM OF CYBERSPACE GOVERNANCE THROUGH THE USE OF ANALOGY

A question that should be addressed at the outset of this analysis is why should states seek to subject cyberspace to any form of multilateral regulation in the first place? The reasons are numerous, but in principle boil down to the three basic needs: sovereignty, security and economy.[744] It has already been shown in the Chapter 2 that the future of the internet is in a state of flux resulting from a variety of competing interests in the power struggle for its control, at the centre of which are two opposing models of governance: the multistakeholder, championed by the US and the sovereignist supported by Russia and China. For the latter states greater say over 'their' segments of cyberspace may equate to having sovereign rights and

[744] Julija Kalpokiene and Ingas Kalpokas, 'Hostes Humani Generis: Cyberspace, The Sea and Sovereign Control' (2012) 5 Baltic Journal of Law and Politics <http://www.versita.com/science/law/bjilp>.

therefore allow a degree of autonomy, especially when it comes to the lucrative digital market place, dominated at present by American companies. As regards security, it has been observed that 'the international community has a clear interest in developing a comprehensive, multilateral cyber security framework because the widespread use of the internet in every aspect of daily life has created an almost irreversible dependency on its technological benefits and because the conceptual underpinnings of existing legal frameworks are not readily adaptable to threats emerging in cyberspace.'[745] Cyber attacks, cyber crime and economic espionage are a day-to-day reality. In addition, Edward Snowden 2013 disclosures revealed the scale and gravity of bulk collection and interception of digital communications of entire countries' populations conducted by the Five Eyes agencies. Since then, other information contained in official inquiries,[746] or unearth by other whistleblowers, academics, civil society and the private sector has provided more details about government surveillance.[747] All this has significantly amplified the concern of governments in the sphere of security.

(a) General: Use of Analogy in International Law

The use of a legal rule by analogy has been described as the application of a rule, which covers a particular case to another case, which is similar to the first, but itself not regulated by that rule.[748] This allows for a quick and effective way to close normative gaps, if a rule is seen

[745] William M. Stahl, 'Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity' (2011) 40 Georgia Journal of International and Comparative Law <http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024&context=gjic>

[746] see for example, the Parliamentary Committee of the Council of Europe, *Mass Surveillance*, Doc. 13748 (21 April 2015) <http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21625&lang=en>.

[747] for more detail on government surveillance of such countries as Russia, Columbia, Egypt, France, Germany, India, Kenya, Pakistan, South Africa and Turkey, see Douwe Korff et al., 'Boundaries of Law: Exploring Transparency, Accountability and Oversight of Government Surveillance Regime' (March 2017) University of Cambridge Faculty of Law Legal Series <https://poseidon01.ssrn.com/delivery.php?ID=994020123000099103086067018078104010116045067060095028110096086103022124108020020101018063099111026042034104124027092093015019029066004033083002076121100009027069123077022050020016011109084028094126021018116012005076122009030113086118030113074100017087&EXT=pdf>.

[748] Silija Vöneky, 'Analogy in International Law', Max Plank Encyclopaedia of Public International Law (2008).

as just and/or useful for cases, which are similar.[749] In international legal order this is seen as desirable, not only because international law lacks the normative density of a national legal systems, but because it also facilitates closing legal lacuna, often seen as counterproductive to achieving certain ends. The use of analogy can be found in decisions of international courts, as a valid tool to create new rules, or as an extension of existing rules to cases in international law and in the writings of publicists.[750] Instances, where the International Court of Justice (ICJ) applied analogy include, *Military and Paramilitary Activities in and Against Nicaragua*[751] and the *Land and Maritime Boundary between Cameroon and Nigerian* case.[752] In the *Nicaragua* case, the ICJ 'explicitly made use of analogy as a method of legal reasoning when assessing the immediate effects of the withdrawal by the United States of its declaration under Article 36(2) Statute of the International Court of Justice recognizing the ICJ's jurisdiction.[753] Article 36(2) states that:

> The states parties to the present Statute may at any time declare that they recognise as compulsory *ipso facto* and without special agreement, in relation to any other state accepting the same obligation, the jurisdiction of the Court in all legal disputes concerning:
>
> a. the interpretation of a treaty;
> b. any question of international law;
> c. the existence of any fact which, if established, would constitute a breach of an international obligation;
> d. the nature or extent of the reparation to be made for the breach of an international obligation.[754]

The ICJ concluded that the 'US could not repudiate its declaration under Article 36(2) with immediate effect. This was based on the principle of good faith (bona fide), which leads by analogy to the application of the law of treaties, where the termination of a treaty requires a reasonable period of notice if the treaty in question does not contain a provision dealing with its duration'.[755]

---

[749] ibid, p.2.
[750] ibid.
[751] *Nicaragua v United States of America*, ICJ Reports 1986 14.
[752] *Cameroon v Nigeria,* ICJ Reports 1999 13.
[753] Vöneky, supra note 10, p. 2.
[754] Statute of the International Court of Justice, 1945, Art. 36(2),
[755] Vöneky, supra note 10, p. 2

In publicists' writings, an analogous application of rules is made in disparate areas of law, for example applying rules of land warfare to air warfare and rules on the applicability of certain peacetime treaties during war to other peacetime treaties.[756] Where a need arose to govern the high seas, scholars looked towards the regimes of land and in the case of governing the outer space, the legal framework of airspace was considered.[757]

The use of analogy can only be triggered if three conditions are met within the existing legal order: (1) the creation of legal provisions must not be exclusively subjected to other enumerated sources of law; (2) similar cases have to be treated the same way legally; (3) there has to be a lacuna in the law, i.e., the case must not be covered by any rule of international law, or any general principle of law.[758] In addition, the use of analogy must be justified in each specific case, by (1) comparing the regulated and the unregulated cases; (2) identifying the similarities between them and (3) rationally deciding that the similarities of the cases compared have to be seen, as being relevant for their legal evaluation and their differences as being relevant.[759] This latter condition requires the undertaking of comparisons between the already regulated cases and the ones that are not covered by exiting rules, the identification of similarities and making a judgement that the similarities of the cases being compared are relevant for their legal evaluation and that their differences are irrelevant.[760]

(b) The Law of the Sea and its Analogous Application to Cyberspace

The United Nations Law Convention on the Law of the Sea 1982 (UNCLOS 1982)[761] is said to represent 'an unprecedented attempt by the international community to regulate all aspects of the resources of the sea and uses of the oceans and thus bring a stable order to mankind's very source of life'.[762] The UN Secretary General described the UNCLOS 1982 after signing

[756] ibid
[757] Michael Peterson, 'The Use of Analogies in Developing Outer Space Law' (1997) International Organization 51(2), pp. 245-274.
[758] supra note 10, p. 2.
[759] ibid.
[760] ibid.
[761] UN GA, Convention on the Law of the Sea, (10 December 1982) 1833 UNTS. 3.
[762] United Nations Office of Legal Affairs, Division for Oceans Affairs and the Law of the Sea', 'The United Nations Convention on the Law of the Sea. A Historical Perspective', 2012 <http://www.un.org/depts/los/convention_agreements/convention_historical_perspective.htm >.

it as 'possibly the most significant legal instrument of (the 20th) century'.[763] Broadly speaking, the treaty addresses navigational rights, territorial sea limits, economic jurisdiction, legal status of resources on the seabed beyond the limits of national jurisdiction, passage of ships through narrow straits, conservation and management of living resources, protection of the maritime environment, a marine research regime and a binding procedure for settlement of disputes between states.[764] A legal framework for cyberspace activities could reflect UNCLOS 1982 by analogy, thus setting out *inter alia* territorial limits, jurisdiction, the legal status of cyberspace beyond the limits of national jurisdiction, rules relating to mutual assistance on cyber security matters, protection of human rights and state responsibility.

The analogous application of the UNCLOS 1982 as a tool to model future cyberspace governance regime can be justified on at least two grounds. First, there is no international law treaty for cyberspace that deals in one document with cyber operations falling within and below the use of force threshold as set out in Article 2 of the Charter of the United Nations. This therefore satisfies the first criteria for the use of analogy, as these activities are not exclusively subjected to other enumerated sources of law. In the case of cyber operations meeting the 'use of force' criteria it has been confirmed that both *jus ad bellum* and *jus in bello* provisions apply to such situations.[765] However, the international community has thus far failed to agree on a hard law international instrument dealing with all those operations that meet the 'use of force' criteria, despite the attempts from the Shanghai Corporation Organization. As regards cyber activities that fall below this threshold, there is no treaty specifically dealing with them on the international level. Rather, there are a number of regional treaties that address cyber crime, including the Budapest Convention on Cybercrime,[766] the Arab Treaty on Combating Cybercrime[767] and the African Union Convention on Cybersecurity and Personal Data Protection.[768] The latter, adopted in July 2014, is broader in scope and relates to such matters as electronic transactions, personal data protection, cyber security and cyber crime. No attempt

[763] ibid.
[764] ibid.
[765] supra note 1 and 2; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014).
[766] Council of Europe, Convention on Cybercrime, Budapest 23 November 2001, ETS 185.
[767] This is an Arab League international agreement adopted in December 2010 and entered into force in February 2014. The members that ratified the treaty include Jordan, United Arab Emirates, Sudan, Iraq, Palestine, Quarter, Kuwait and Oman. <http://www.riyadh.om/wp-content/uploads/2015/03/2015-005.pdf>.
[768] African Union Convention on Cybersecurity and Personal Data Protection (EX.CL/846 XXV) < https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf >.

has yet been made to approach the issue of regulating cyber surveillance/cyber espionage on an international level through a binding treaty. This fulfils another requirement for use of analogy, as it exposes a lacuna in the law.

Secondly, some comparisons can be drawn between the development of the international regime for the seas and that for cyberspace. These similarities seem to satisfy the requirement for the use of analogy, according to which like cases must be treated in the same way legally. The history of the development of the law of the sea is in some respects comparable to the current debate regarding the status and future of cyberspace. This is because, the seas in similar vein to cyberspace, had been subject to fragmented regulation[769] (although for much longer than cyberspace), prior to the eventual codification in the UNCLOS 1982 and likewise, replete with criminal activities, such as piracy. Furthermore, one of the founding principles of the law of the sea was the idea of the 'open seas', which in time proved unsustainable, as states sought greater security and control over their 'fixed and floating' assets. Similarly, the current quest for the control over cyberspace, both domestically and through international and regional forums outlined in the previous chapter, shows that some states find the idea of 'internet freedom' and openness unacceptable and wish for greater control in this domain, often due to national security concerns. The quest for increased security and the distrust created by the revelations of mass surveillance and bulk data collection suggest cyberspace's possible future segmentation, which may lead to its 'balkanization'.[770]

Thirdly, the current international regime governing the seas does not classify the maritime regions as a single environment, but has a menu of options to deal with its various constituent parts, such as territorial waters, high seas and the deep seabed. The success of this framework is due to its flexibility to treat these areas differently. Some are subject to full sovereignty, as in the case of the territorial seas and air space above, others sovereign rights and jurisdiction, for example in the case of continental shelf and exclusive economic zone, whereas such regions as the high seas are open to all states, whether costal or land locked.[771] These arrangements proved successful in answering divergent needs of states and the environments they regulate

---

[769] 1958 Geneva Conventions on the Law of the Seas: The Convention on the Territorial Seas and the Contiguous Zone (CTS); The Convention on the High Seas (CHS); The Convention on Fishing and Conservation of the Leaving Resources of the High Seas (CFSLR) and The Convention on the Continental Shelf (CCS) <http://legal.un.org/avl/ha/gclos/gclos.html>.

[770] Christopher Bronk, 'Who Leads? Avoiding the Balkanization of Cyberspace', The International Relations Security Network (2014) < http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=181188>.

[771] UNCLOS, supra note 23, art. 87.

and therefore their possible application to cyberspace must not be overlooked in favour of a totally new regulatory regime, as advocated by some writers.[772]

(i) The Development of the International Law of the Sea and Cyberspace Governance- Some Parallels

The international law of the sea has its origins in determining the status and control over ocean space, which progressed to encompass a variety of interests and regimes including the deep seabed, high seas, fish stocks, maritime scientific research, military uses of the ocean and environmental protection.[773] Several distinctive phases could be identified with regard to the history of sources of the international law of the sea, ranging from theoretical debates among scholars relating to the status of the oceans, the freedom of the seas doctrine, gradual codification of the law throughout the twentieth century to the ongoing regulatory efforts to meet such challenges, as climate change and high seas fishing.[774] Early maritime history is dominated by the activities of the European sea powers, which not only developed naval technology that allowed them the exploration of far flung parts of the globe, but it also facilitated the establishment of the trade routes, which led to usurping control over activities on the oceans. Thus the initial Roman law, according to which the sea was free and common to all, gave way by the Middle Ages to various forms of appropriation and control by powerful states.[775] It was the Papal Bulletin of Pope Alexander VI, given effect in the 1494 Treaty of Tordesillas, which divided the then world into an area of Portuguese expansion to the east and the Spanish to the west, which as a consequence impacted on the adjoining seas.[776] Attempts

[772] see for example, Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 International Journal of Law and Information Technology- proposing regulating cyberspace the same way that real space is regulated; Graham Greenleaf, 'Regulating Cyberspace: Architecture vs Law?' (1998) 21 The University of New South Wales Law Journal- proposing new self-regulatory system for cyberspace; Warren Chik, 'Customary Internet-tional Law: Creating a Body of Customary Law to Cyberspace. Part 1: Developing Rules for Transitioning Custom into Law' (2001) 26 Computer Law and Security- arguing for cyberspace regime based on customary international law; Nicholas W. Cade, 'An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code' (2010) 37 Brooklyn Journal of International Law- advocating global cyber security system and cyber court.

[773] Donald R. Rothwell and Tim Stephens, *The International Law of the Sea,* (Hart Publishing 2014), p. 1.

[774] ibid.

[775] ibid.

[776] ibid.

to reconcile the competing interests thus created were made by some publicists, among them the Dutch scholar Hugo Grotius and an Englishman John Selden. The main thrust of their work related to conceptualizing the status of the seas and the debate over the access and ownership of the oceans. The most significant contribution in this regard was made by Grotius in his 1608 work *Mare Liberum.*[777] His doctrine of the free seas was based on two assumptions, namely that the seas' immeasurable vastness makes it impossible to occupy, control or exhaust by navigation and fishing, coupled with the general right to travel and trade expressed under the law of nations.[778] In Chapter V of *Mare Liberum*, Grotius observed that under the law of nations the sea had at various times been given the status of property of no one (*res nullius*), a common possession (*res communis*) and public property (*res publica*).[779] These early deliberations regarding the status of the sea are not dissimilar to the current debates regarding cyberspace. As with the Grotian description of the seas, which in his view was impossible to confine within fixed boundaries, cyberspace was also at first considered as borderless, vast and uncontrollable by governments, as exemplified by the debate of the cyberlibertarians and cyberpositivists in the previous chapter of this thesis. Furthermore, similarly to the Grotian concept of the sea being a facilitator of exchange and interchange, cyberspace is also considered an enabler in terms of information flow, trade and communication. Grotius concluded that oceans could not be appropriated, because 'that which cannot be occupied, or which has never been occupied, cannot be the property of anyone, because all property has arisen from occupation'.[780] He compared the sea to the air, which in his view was not susceptible to occupation and is for the use of all. This reasoning has been widely accepted, as the freedom of the seas. It could be said that this stance is similar to that advocated by United States in relation to cyberspace, found in such proclamations as the one made by Mrs Clinton in her speech, *Remarks on Internet Freedom*[781] and the 2005 *US Department of Defence Strategy for Homeland Defence and Civil Support* (the Defence Strategy),[782] referred to in Chapter 2 of this thesis. In the *Remarks on Internet Freedom*, the then Senator Clinton supported the free access to and free flow of information on the internet for everyone. Her

[777] Hugo Grotius, *The Freedom of the Seas or the Right which Belong to the Dutch to Take Part in the East India Trade* (OUP, 1633 trans, 1916 rep).
[778] Kalpokiene and Kalpokas, supra note 6.
[779] Rothwell and Stephens, supra note 35.
[780] Grotius, supra note 39, p. 27.
[781] Hillary Rodham Clinton, 'Remarks on Internet Freedom', US Department of State, (21 January 2010) <http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.
[782] US Department of Defence, 'Strategy for Homeland Defence and Civil Support', (2005) < http://www.defense.gov/news/Jun2005/d20050630homeland.pdf>.

address bears some resemblance to the observations made by Grotius, according to which 'for the same reasons the sea is common to all, because it is so limitless that it cannot become a possession of anyone and because it is adapted for the use of all, whether we consider it from the point of view of navigation or of fisheries'.[783] Similarly, the Defence Strategy in similar manner to the Grotian idea of 'limitless sea' refers to the idea of a limitless nature of cyberspace declaring that 'the global commons consist of international waters, and airspace, space and cyberspace'[784] and more recently reiterated by Mrs Clinton, who referred to it, as the 'global network commons'.[785]

The most substantive challenge to *Mare Liberum* came from English scholar John Selden, who in his work *Mare Clausum* (The Closed Sea) not only sought to assert the sovereignty and the dominion of the crown of England in British seas, but also to prove longstanding state practice of dominion over the oceans.[786] It was the view of the 'open seas' however, that prevailed in the end and which was adhered to for the next 300 years. Over time, the absolute freedom of the seas was challenged, as it was incompatible with the states' needs to defend themselves. Cyberspace, as an 'open space' has also been challenged in a variety of forums, including the two World Summits in 2003 and 2005 and the Conference in Dubai in 2012 referred to in the previous chapter.

With respect to regulating the seas, coastal states began gradually to assert their rights to control the waters adjoining their coasts. At the end of nineteenth century the area of the sea adjacent to state territory emerged, gaining a similar legal status to that of land territory.[787] This gave coastal states the power to exercise jurisdiction and control, initially for security and subsequently in relation to exploitation of resources, such as fisheries.[788] However, as these emergent rights remained undefined, there was a clear need to accommodate them within the predominant paradigm of the freedom of the seas. Although various attempts were made by the League of Nations, no agreement was reached, most notable among these was the failure at the 1930 Hague Codification Conference. Following the creation of the International Law Commission by the United Nations, the first United Nations Conference on the Law of the Sea (UNCLOS I) was held in Geneva in 1958 and resulted in the codification of customary law in four conventions, namely the Convention on the Territorial Sea and Contiguous Zone, the

[783] supra note 39, p. 28.
[784] supra note 44.
[785] Clinton, supra note 43.
[786] Rothwell and Stephens, supra note 35.
[787] ibid.
[788] ibid.

Convention on the Continental Shelf, the Convention on the High Seas and the Convention on Fishing and Conservation of the Living Resources of the High Seas.[789] This was a significant development, as 'it provided the foundation for the contemporary law of the sea'.[790] However it did leave some 'gaps', which states sought to fill in through rapidly developing at the time customary international law. Subsequent 1960 Geneva Conference (UNCLOS II) focused on two issues, the breadth of the territorial sea and fishery limits, but failed to reach agreement on the important issues, such as the limits of maritime zones. To some extent it could be said that the two-phase World Summit on the Information Society held in 2003 in Geneva and 2005 in Tunis, referred to in the previous chapter, bears some similarities to UNCLOS I and II, in that the WSISs were the first major attempt by the international community to start the process of negotiation regarding the legal mechanisms to manage cyberspace. However, the UNCLOS I was a major success, because it initiated the codification process, which both phases of WSIS did not achieve with regards to the codification of cyberspace.

The 1960s witnessed a development of state practice in international law of the sea, which was 'filling in the voids' left by the Geneva Conventions and purported to create new coastal state rights. An example of these developments was the quest of the coastal states for the establishment of other resource-type claims, such as the Exclusive Fishing Zones (EFZ). These were recognized in bilateral agreements, such as the 1964 London Fisheries Convention to be of 12 nautical miles (nm). Other important developments included the US attempt by way of a unilateral declaration, to exercise jurisdiction and control over the natural resources of the subsoil and seabed of the contiguous continental shelf, through the so-called Truman Proclamation of 1945, [791] discussed further below. Additionally, in 1967 the Maltese Ambassador Arvid Pardo proposed to the United Nations General Assembly that both the seabed and the ocean floor should be given a status of 'common heritage of mankind'.[792] The reasons for this assignation was that the Geneva Conventions did not address these issues together with a growing interest among the international community to establish a distinct legal regime for these areas, spurred by technological advances made, which would have enabled unrestrained mineral exploration of the deep seabed. In 1970 the General Assembly adopted Resolution 2749 (XXV) tilted *Declaration of Principles Governing the Sea-Bed and Ocean*

[789] ibid. p. 6.
[790] ibid p. 9.
[791] United States Presidential Proclamation No. 2667: Policy of the United States with Respect to the Natural Resources of the Subsoil and Sea Bed and the Continental Shelf, Basic Documents No. 5.
[792] ibid p. 11.

Floor and the Subsoil Thereof, Beyond the Limits of Notional Jurisdiction,[793] which proclaimed the seabed and the ocean floor as part of the common heritage of mankind and called for Third United Nations Conference on the Law of the Sea (UNCLOS III). In the same year the Montevideo Declaration on the Law of the Sea proposed the development of the new regime, which would recognize the 'right of the coastal states to avail themselves of the natural resources of the sea adjacent to their coasts'.[794] Latin American states developed this concept further and endorsed an idea of 200nm over which sovereignty could be exercised with respect of the natural resources of the sea. This, together with the proclamation in the Montevideo Declaration and the debates over the EFZ, formed the bases for the recognition of the Exclusive Economic Zone (EEZ).

One of the most important developments at the end of the Second World War was the 1945 United States Presidential Proclamation No. 2667,[795] also known as the 1945 Truman Proclamation. This was an attempt on the part of the US by way of a unilateral declaration, to exercise jurisdiction and control over the natural resources of the subsoil and seabed of the contiguous continental shelf.[796] The Truman Proclamation asserted that:

> [t]he exercise of jurisdiction over the natural resources of the subsoil and sea bed of the continental shelf by contiguous nations is reasonable and just [because] continental shelf may be regarded as an extension of the land-mass of the coastal nation and thus naturally appurtenant to it.[797]

The Proclamation was described as 'the first substantive claim by a coastal state to a distinctive off-shore resource zone, which was completely separate from the territorial sea',[798] albeit it remained undefined as to its outer limits.

This period also marked an emergent jurisprudence of the International Court of Justice (ICJ), with two cases of particular note. In the *Corfu Channel* case,[799] the ICJ discussed the developing regime of territorial sea and in particular navigation rights and freedoms through

[793] UN GA Resolution 2749 (XXV) (1970), Basic Documents No. 17.
[794] S Houston Lay, Robin Churchill and Myron Nordquist (eds), *New Directions in the Law of the Sea* (Dobbs Ferry, NY, Oceana 1973).
[795] United States Presidential Proclamation No. 2667, supra note 53.
[796] Rothwell and Stephens supra note 35, p. 5.
[797] US Presidential Proclamation, supra note 53.
[798] Rothwell and Stephens, supra note 35.
[799] *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep. 4

international straits during peacetime.[800] In the *Fisheries* case[801] the capacity of a coastal state to draw a so-called 'straight baseline' around the outer edge of the coast from which the territorial sea was proclaimed, was deliberated in the context of territorial sea regime.[802]
In 1973 the United Nations commenced its third conference UNCLOS III, which resulted in the United Nations Convention on the Law of the Sea 1982 (UNCLOS 1982),[803] following a nine-year period of negotiations. The Convention achieved what the previous UNCLOS I and II failed to do, that is the setting of the limits of territorial waters to 12nm, within which 'states are in principle free to enforce any law, regulate any use and exploit any resources'.[804] Before the conclusion of the Convention was reached however, it was challenged by the US Reagan administration, who objected to Part XI. This Part relates *inter alia* to the deep seabed exploration and exploitation consistent with common heritage of mankind principle.[805] The Administration argued that these provisions were unfavourable to American economic and security interests. Nevertheless, the Convention came into force in 1994 and has been ratified by 166 states, excluding the US.[806] The UNCLOS 1982 can be regarded, as marking a turning point from the paradigm championed by Grotius that the sea was immeasurable and impossible to control, to one effectively controlling the ocean resources through adoption of a variety of legal mechanisms and finding compromise through a 'package deal' Convention.[807]

The proceeding section drew a number of similarities between the historical developments of the codification of the law of the sea and the on-going discourse relating to a future cyberspace regime. This includes the determining of the status and control over these domains in the early stages, which meant in both cases turning away from the concept of an ungoverned space to greater sovereign controls. Whilst the UNCLOS 1982 is one of the principal legal frameworks regulating the maritime areas, there is an array of other treaties, state practice and instruments for the governance and management of the world's oceans, which go beyond matters relating to state sovereignty and jurisdiction and reflect contemporary challenges, contributing to continued evolution of the law in this area.[808] Likewise, an 'umbrella

[800] Rothwell and Stephens supra note 35, p. 5
[801] *Fisheries (United Kingdom v Norway)* [1951] ICJ Rep. 116
[802] Rothwell and Stephens, supra note 35.
[803] supra note 23.
[804] The UN Convention on the Law of the Sea, A Historical Perspective, supra note 24.
[805] UNCLOS, supra note 23, Part XI.
[806] Status of the UN Convention on the Law of the Sea as at 10 October 2014 <http://www.un.org/depts/los/reference_files/status2010.pdf >.
[807] Rothwell and Stephens, supra note 35, p. 13.
[808] ibid, p. 1.

convention' for cyberspace setting out the rights and obligations of states might be a good starting point on a conceptual journey of cyberspace governance. Once the broad principles are defined, the detail may follow. The historical insight into the law of the sea illustrates how the international community successfully met the challenge posed by global governance of a new domain. Three related concepts warrant more detailed analysis in this context, namely the position adopted by some states that cyberspace is a global common; the utility (if any) of the common heritage of mankind principle; the regimes governing the exclusive economic zone and the continental shelf and their application to cyberspace. Each of these aspects of the law of the seas regulation will be addressed below.

2. CYBERSPACE AS A GLOBAL COMMON

It was proposed in the previous chapter that cyberspace could not in all probability be classed in international law as a *terra nullius*, because as an artificially constructed environment, private and public ownership rights have always played a part therein. Furthermore, despite it being considered initially by the cyberlibertarians to be an environment free from the 'real' world governmental laws and controls, these attitudes were duly dispelled and national regulation soon followed. Current state practice points to tendencies of many nations to both seek to protect their vital infrastructures from cyber attacks and to exert greater controls over information flows within their borders.[809] In particular, China and Russia through the Shanghai Cooperation Organization actively pursue the path of assert sovereignty rights over the internet and regard it as part of its sovereign territory, that is as an extension of the airspace, which in their view they are entitled to protect, as part of their 'cyber territory'.[810] Despite the fears that this quest for tighter cyberspace regulation and the underling ideology of asserting the principles of sovereignty and non-intervention may lead in the future to segmentation, states would have to entirely separate themselves from the global internet

[809] for example, the US has a sizable number of internet related laws, including Computer Fraud and Abuse Act (18 U.S.C. 1030 2012); Electronic Communications Privacy Act (18 U.S.C 2510-2522 2012).

[810] UN GA, 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (13 January 2015) UN Doc A/69/723.

network, in order to gain full sovereignty. It is doubtful that many would choose to pursue this course of action, but that does not mean that they will not continue to exert tighter controls therein.

Assuming that cyberspace does not fall within the category of *terra nullius*, nor is a part of states' sovereign territory (despite some movement in this direction), could it be considered a *res communis*? The idea that cyberspace is a global common has been mainly formulated and advocated by the US, although it is also featured in documents of other nations, such as the Canadian *Cyber Security Strategy* 2010.[811] It is at the opposite end of the spectrum from the sovereign-based model championed by Russia and China. The strong support for the idea that cyberspace is a global common can be gleaned from *inter alia, Remarks on Internet Freedom* in 2010, in which Mrs Clinton called cyberspace a 'global network commons' and stated that 'the US stands for a single internet, where all of humanity has equal access to knowledge and ideas'.[812] The US government's view on cyberspace in the context of national security coincides with the description of 'global network commons' articulated by Mrs. Clinton. For example, the 2005 *US Strategy for Homeland Defense and Civil Support*[813] was stated to achieve the Defense Department's main goal of securing the US from direct attack.[814] To that end, it unveiled a ten-year timeframe, requiring 'an active, layered defenses',[815] which 'is global, seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the United States'.[816] The subsequent 2008 US *National Defense Strategy*[817] lacks direct mention of cyberspace, as a 'global network commons', but continues the previous theme with oblique references to this domain as a global common.[818] Similarly, the May 2011 Obama

---

[811] 'Canada's Cyber Security Strategy' (2010) refers to cyberspace, as a global commons at p. 2 <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf>.
[812] Clinton, supra note 43.
[813] US Department of Defence, supra note 44.
[814] ibid p. 1
[815] ibid
[816] ibid
[817] US Department of Defence, 'National Defence Strategy' (2008) < http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.
[818] ibid p. 16:

> [f]or more than sixty years, the United States has secured the global commons for the benefit of all. Global prosperity is contingent on the free flow of ideas, goods, and services. The enormous growth in trade has lifted millions of people out of poverty by making locally produced goods available on the global market. Low barriers to trade also benefit consumers by reducing the cost of goods and allowing countries to specialize. None of this is possible without a basic belief that goods shipped through

Administration document *The International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*,[819] stated that the US government's main goal in cyberspace is to:

> [w]ork internationally to promote an open, interoperable, secure and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security and fosters free expression and innovation. To achieve that goal, [the Administration] will build and sustain an environment, in which norms of responsible behavior guide states' actions, sustain partnerships and support the rule of law in cyberspace.[820]

In releasing *International Strategy*, the US unveiled its plans for the future of cyberspace, governed by the rule of law, where cyber security is addressed and which, at the same time views cyberspace, as a global political space. Furthermore, the Administration's international cyberspace policy was said to 'reflect (our) core commitments to fundamental freedoms, privacy and the free flow of information'.[821] By combining economic, security, human rights and political concerns, the *International Strategy* gave support to the earlier, Secretary Clinton's 2010 rhetoric contained in the *Remarks on Internet Freedom*.[822] The same approach to cyberspace as a global common is also shared by some think-tanks, for example the US Centre of New American Security 2010 Report *America's Cyber Future: Security and Prosperity in Information Age*, stated that sea, air, space and cyberspace all form global commons because they share four broad characteristics, namely (1) they are not owned nor controlled by any single entity; (2) their utility as a whole is greater than if broken down into smaller parts; (3) states and non-state actors with the requisite technical capabilities are able to

---

> air or by sea, or information transmitted under the ocean or through space, will arrive at their destination safely. The development and proliferation of anti-access technologies and tactics threatens to undermine this belief.

< http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.

[819] The White House, 'International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World' (16 May 2011) <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

[820] ibid p. 8.

[821] ibid p. 5.

[822] Clinton, supra note 43.

access and use them for economic, political, scientific and cultural purposes.[823]
The North Atlantic Treaty Organization seems also to support this view, as it claims in one of its Reports that 'cyber domain could be considered, as one of the global commons, as it exists in an international space that is usable by everyone'.[824]

In terms of international law, for a resource to be so perceived, it must be part of enumerated domains, classified as the commons and satisfy the requirements of existing frameworks regulating those environments. Simply calling cyberspace a global common does not make it so. Therefore, what needs to be ascertained is whether, or not cyberspace falls within any of these regimes.
It could be said that in international law, *res communis*, or 'thing of the entire community',[825] is the opposite to the idea of territorial sovereignty. International law lacks a specific definition of the term 'global commons', however the Organization for Economic Cooperation and Development refers to them, as 'natural assets outside national jurisdiction, such as the oceans, outer space and the Antarctic'.[826] The concept of the global commons denotes limits to state sovereignty in certain parts of the world, as it opens these spaces to be used by the international community, but closed to exclusive appropriation by treaty, or custom.[827] They therefore do not fall within the jurisdiction of any one country and are unique, in the sense that they have their own 'geographical, economic, legal and administrative attributes'.[828] Further, the commons cannot be regarded as states, because they lack characteristics of statehood, such as permanent population and government. Therefore, as such, they are administered through a mixture of regulations at multiple levels, including multilateral treaty regimes, regional accords and national regulations.[829] Thus, the areas of the high seas, the outer space and the Antarctic

[823] Centre for a New American Security, 'America's Cyber Future: Security and Prosperity in Information Age', (2010) <http://www.cnas.org/publications/reports/america-s-cyber-future-security-and-prosperity-in-the-information-age#.VQb_0SjudFI>.
[824] Maj. Gen. Mark Rarrett, Dick Bedford, Elizabeth Skinner and Eva Vergles, 'Assured Access to the Global Commons', Supreme Allied Command Transformation (2011) <http://www.act.nato.int/globalcommons-reports>.
[825] *Blacks' Law Dictionary* (West Group 1999), p. 1308.
[826] Organization for Economic Co-operation and Development, Glossary of Statistical Terms, 'Global Commons' <http://stats.oecd.org/glossary/detail.asp?ID=1120>.
[827] Kamal Baslar, 'The Concept of Common Heritage of Mankind in International Law', in Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations* (Cambridge University Press 2014).
[828] Christopher Joyner, *Governing the Frozen Commons: The Antarctic Regime and Environmental Protection* (University of South Carolina Press 1998) p. 222.
[829] supra note 89, p. 59.

are regulated respectively by: The United Nations Convention on the Law of the Sea 1982 (UNCLOS), The Treaty on Principles Governing the Activities of States in the Exploration and use of Outer Space 1967 (The Outer Space Treaty) and The Antarctic Treaty 1959. These are disparate legal regimes, which apply differently to each domain they seek to govern, but with the common aim of ensuring the resources' reasonable use and their sustainability. In this sense, they complement each other, because they confer rights and duties on all states. They also have three features in common, that is they allow for little, or no role for private parties in their governance, they are all controlled by a treaty and are subject to limits in terms of militarization, although in varied degrees. They also seek to protect individual states' rights to use the domain of the common, provided that such use does not interfere with others' freedom.[830] This gives every state such rights as the freedom to navigate, overfly, lay submarine cables and pipelines on the high seas,[831] together with the 'the exploration and use of outer space'.[832] Some of the above mentioned conventions feature the principle of the 'common heritage of mankind', which will be considered more fully later in this chapter. Due to the rapid economic and technological developments in the late 20th and early 21st century, coupled with increasing international trade, the global commons have been confronted with new challenges and competing interest from a variety of stakeholders (states, non-state actors and international organizations) resulting in two different approaches to the issue of their governance and future, on the one hand the security/military and on the other hand, the environmental focus. The security and/or military perspective generally identifies three/four domains as global commons: the high seas, airspace, outer space and cyberspace (the latter mainly by the US).[833] In the security discourse, the primary concern is safeguarding the access to these domains for commercial and military purposes. This is to some extent echoed in the policy stance of the US and other like minded states, reflected through the idea of 'internet freedom'. Conversely, the international organizations and groups with an environmentalist focus, are increasingly concerned with the damage to the condition of the commons from

[830] Duncan Hollis, 'Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace' (2012) Cyberdialogue <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038523>.
[831] Article 87(a)-(c) UNCLOS 1982, supra note 23.
[832] The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, (the Outer Space Treaty), 1967, 18 UST 2410, art 1.
[833] Gerald Stang, 'Global Commons: Between Cooperation and Competition' (2013) European Union Institute for Security Studies <http://www.iss.europa.eu/uploads/media/Brief_17.pdf>.

overuse and depletion of the natural resources (for example, ocean fish stocks) and damage done to these shared areas, such as Antarctica and the atmosphere.[834] Their principle aim is to preserve the condition of these resources, in the spirit of sustainable development.[835]

As there is no overarching definition of the global commons, each of these domains and their governing regimes must be examined separately in order to determine if cyberspace fits into the legal definition of any of these environments.

(a) The High Seas

Despite the gradual erosion of the geographical extent of the high seas in favour of other maritime zones, such as the continental shelf, fisheries zones and the exclusive economic zone, they remain the largest of the maritime areas and retain many of the characteristics of the Grotian doctrine of the freedom of the seas.[836] One such aspect, which continues to be adhered to, is the idea that high seas are beyond national appropriation and not subject to state sovereignty. A considerable body of customary and conventional international law relating to the high sea was codified in the 1958 Geneva Convention on the High Seas, which was 'generally declaratory of established principles of international law'.[837] Eventually the provisions under the Geneva Convention were incorporated into the UNCLOS 1982, which deals with the high seas in Part VII. Article 86 provides a definition of the high seas, which are 'all parts of the sea that are not included in the exclusive economic zone, in the territorial sea, or and archipelagic state'.[838] Article 89 precludes any state from seeking to subject any part of the high seas to its sovereignty, stating that 'no state may validly purport to subject any part of the high seas to its sovereignty'.[839] The provision regarding the freedom of the high seas is contained in Article 87(1), whereby:

> [t]he high seas are open to all states, whether coastal or land-locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and

[834] ibid.
[835] Declaration of the United Nations Conference on the Human Environment (Stockholm Declaration), adopted 16 June 1972 11 ILM 1416, Principle 21.
[836] Rothwell and Stephens supra note 35, p. 145
[837] Geneva Convention on the High Seas, Preamble, 1958 13 UST 2312.
[838] UNCLOS 1982, art 86, supra note 23.
[839] ibid, art 89.

by other rules of international law. It comprises, *inter alia*, both for coastal and land-locked states:

(a) freedom of navigation;
(b) freedom of over flight;
(c) freedom to lay submarine cables and pipelines subject to Part VI;
(d) freedom to construct artificial islands and other installations; permitted under international law, subject to Part VI;
(e) freedom of fishing, subject to the conditions laid down in section 2;
(f) freedom of scientific research, subject to Parts VI and XIII.[840]

The list is not exhaustive and recognizes states' capacity to engage in other activities consistent with the freedoms, but for peaceful purposes only, as specifically noted in Article 88. Further, since the freedom of the seas is no absolute, any activity must be conducted consistently with the 1982 UNLOSC and other rules of international law, having 'due regard to the interests of other states in their exercise of the freedom of the high seas'.[841]

Part VII of the Treaty contains provisions, which address the state of ships and their obligation whilst on the high seas. Article 91 recognizes states' rights to sail ships under their flag[842] and that states must exercise jurisdiction and control over ships flying their flag.[843] The Convention also lists activities that are strictly prohibited, namely piracy, slavery, drug trafficking and unauthorized broadcasting.

---

[840] ibid, art 87.
[841] ibid, art 87
[842] UNCLOS 1982 art 91:

1. [e]very State shall fix the conditions for the grant of its nationality to ships, for the registration of ships in its territory, and for the right to fly its flag. Ships have the nationality of the State whose flag they are entitled to fly. There must exist a genuine link between the State and the ship.
2. Every State shall issue to ships to which it has granted the right to fly its flag documents to that effect.

[843] UNCLOS art 92(1):

[s]hips shall sail under the flag of one State only and, save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas. A ship may not change its flag during a voyage or while in a port of call, save in the case of a real transfer of ownership or change of registry.

(b) *The Outer Space*

The 1957 launch of the USSR's artificial satellite Sputnik 1 marked the dawn of human activity in outer space. The event triggered a discussion among the international community regarding the development of principles and laws to govern that domain. In 1959 the United Nations created a Committee on the Peaceful Uses of Outer Space (COPUOS), whose mission was to 'review the scope of international cooperation in peaceful uses of outer space, to devise programs in this field to be undertaken under United Nations auspices, to encourage continued research and the dissemination of information on outer space matters and to study legal problems arising form the exploration of outer space'.[844] COPUOS created two sub committees: the Scientific and Technical Subcommittee and the Legal Subcommittee, which helped to negotiate and discuss a suite of international treaties relating to outer space including: The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the 'Outer Space Treaty)'[845] and the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the 'Moon Treaty').[846]

The legal status of outer space and celestial bodies at the time of negotiation was subject of disagreement between opposing camps. At one end of the spectrum was the U.S., together with some Western states, who analogized outer space to the high seas and at the other, the Soviet block, preferring an analogy to airspace, which is subject to territorial sovereignty.[847] Ultimately, a consensus was reached and the legal status of the outer space was crystallized in the 1961 General Assembly Resolution 1721 (XVI), according to which 'outer space and celestial bodies are free from exploration and use by all states in conformity with international law and are not subject to national appropriation'.[848] The 1967 Outer Space Treaty was subsequently arrived at and forms the bases of the international space regime. It codified the status of outer space, as free from state sovereignty by specifically proclaiming in Article II

[844] General Assembly Resolution 1472 (XIV) U.N. Doc. A/43/51 (1959).
[845] The Outer Space Treaty, supra note 94.
[846] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, (The Moon Treaty) 1979, United Nations, Treaty Series, vol. 610, no. 6643.
[847] M. J. Peterson, 'The Use of Analogy in Developing Outer Space Law' (1997) 51 International Law Organization <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=173181>.
[848] General Assembly Resolution 1721 (XVI) Art. A. 1(b). U.N. Doc. A/5026 (1961).

that ‘outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means’.[849] Article I provides that the exploration and use of outer space must be carried out ‘for the benefit and the interests of all countries, irrespective of their degree of economic or social development and shall be the province of all mankind’.[850] Other important provisions relate to prohibition imposed on states relating to certain military uses, among them under Article IV ‘placing in orbit, installing on celestial bodies, or stationing in outer space nuclear weapons or other weapons of mass destruction’.[851] The Article further states that:

> [t]he Moon and other celestial bodies shall be used by all states parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited.[852]

Articles VI-VII assign states international responsibility:

> for national activities in outer space [whether such activities are carried on by governmental agencies, or by non-governmental entities and for ensuring that national activities are carried out in conformity with the provisions set forth in the present Treaty.[853]

The 1979 Moon Treaty is another important instrument, which specifically provides that the Moon is not subject to sovereignty claim. Article 11(2) states that ‘the Moon is not subject to national appropriation by any claim of sovereignty, by means of use or occupation, or by any other means’,[854] whilst Article 11(1) proclaims the Moon and its natural resources, as common

[849] The Moon Treaty, supra note 108, art II.
[850] ibid, art I.
[851] ibid, art IV.
[852] ibid.
[853] ibid, art VI.
[854] The Moon Treaty, supra note 108, art 11(2).

heritage of mankind.[855] It obliges states 'to establish an international regime, including appropriate procedures, to govern the exploitation of the natural resources of the Moon, as such exploitation is about to become feasible.'[856] Similarly to the Outer Space Treaty, military activities on the Moon and other celestial bodies are also subject to restrictions and must be 'carried out in accordance with international law, in particular the Charter of the United Nations'.[857] Any activity on the Moon may only be carried out for 'peaceful purposes',[858] 'any threat or use of force or any other hostile act or threat of hostile act' is prohibited,[859] as is placing or using nuclear or other weapons of mass destruction on or in orbit around the Moon, establishing military bases, or conducting weapons tests.[860]

The regimes created by the Outer Space Treaty and the Moon Treaty confirm that the outer space and the celestial bodies cannot be subject to sovereign claim by states and similarly to the law of the sea, they also rely on governance by treaty. Furthermore, they specifically either limit and regulate military activities (the Moon Treaty), or altogether prohibit use of certain weapons (Outer Space Treaty).

(c) Antarctica

Prior to the signing of the Antarctic Treaty in 1959, seven states made territorial claims to parts of that continent between 1908-1943.[861] During the International Geophysical Year 1957-8, 12 countries established their bases on Antarctica, mainly for scientific research purposes. Subsequently the Antarctic Treaty was signed in 1959.[862] The Treaty comprises 14 Articles and obliges the countries active in Antarctica to consult on the uses of a whole continent. In Article 1 the Treaty specifically stipulates that 'Antarctica shall be used for peaceful purposes only. There shall be prohibited, *inter alia*, any measure of a military nature, such as the establishment of military bases and fortifications, the carrying out of military manoeuvres, as

[855] ibid, art 11(1).
[856] ibid, art 11(5).
[857] ibid, art 2.
[858] ibid, art 3(1).
[859] ibid, art 3(2).
[860] ibid, art 3(3)-(4).
[861] 'Evolution Of Arctic Territorial Claims And Agreements: A Timeline (1903-Present)' (15 September 2013) Stimson Centre <http://www.stimson.org/infographics/evolution-of-arctic-territorial-claims-and-agreements-a-timeline-1903-present/>.
[862] These countries are Argentina, Australia, Belgium, Chile, France, Japan, New Zealand, Norway, South Africa, United Kingdom, United States and USSR.

well as the testing of any type of weapon.'[863] The Treaty sets aside the potential for sovereignty disputes between Treaty parties by providing that no activities will enhance, or diminish previously asserted territorial claims and stipulates that no new, or enlarged claims can be made.[864] This is set out in Article IV, which states that:

1. [n]othing contained in the present Treaty shall be interpreted as:
   a renunciation by any Contracting Party of previously asserted rights of or claims to territorial sovereignty in Antarctica;
   a renunciation or diminution by any Contracting Party of any basis of claim to territorial sovereignty in Antarctica which it may have whether as a result of its activities or those of its nationals in Antarctica, or otherwise;
   prejudicing the position of any Contracting Party as regards its recognition or non-recognition of any other State's rights of or claim or basis of claim to territorial sovereignty in Antarctica.
2. No acts or activities taking place while the present Treaty is in force shall constitute a basis for asserting, supporting or denying a claim to territorial sovereignty in Antarctica or create any rights of sovereignty in Antarctica. No new claim, or enlargement of an existing claim, to territorial sovereignty in Antarctica shall be asserted while the present Treaty is in force.

Thus, the Antarctic Treaty puts aside the potential for conflict over sovereignty by providing that nothing that occurs while the Treaty is in force will enhance or diminish territorial claims.[865] Furthermore, Article V 'prohibits nuclear explosions and the disposal of radioactive waste', Article II protects the 'freedom of scientific investigation', whilst Article VII provides for inspection by observers, designated by any party, of ships, stations and equipment to ensure the observance of and compliance with the Treaty. The observers are subject to the jurisdiction of the state that they represent, by virtue of Article VIII.

[863] The Antarctic Treaty, 1 December 1959, 12 UST 794 402 NNTS 71; art 1.
[864] British Antarctic Survey, 'The Antarctic Treaty Explained', <http://www.antarctica.ac.uk/about_antarctica/geopolitical/treaty/explained.php>.
[865] Australian Government Department of Environment and Energy, 'Antarctic Territorial Claims' < http://www.antarctica.gov.au/law-and-treaty/history/antarctic-territorial-claims>.

The Treaty has 46 signatories[866] and provides in Article XIII that any member of the United Nations can accede to it. It entered into force on 23rd July 1961 and since then has been recognized, as one of the most successful international agreements.[867] It declares Antarctica as non-sovereign, putting aside any differences over territorial claims and providing for a disarmament regime, but at the same time enabling Treaty parties to protect their essential Antarctic interests.[868] The governance regime, similarly to that of the high seas and the outer space, is treaty based and developed through multilateral negotiations. The two outstanding features of the Antarctic Treaty are the use for peaceful purposes only and the continent's total de-militarization.

(d) Cyberspace as a Global Common?

Apart from the assignation of cyberspace as a global common by a handful of states, this categorization has been adopted by some journalists, especially in regards to the challenges of the internet governance.[869] The academic opinion however, is divided on the issue. Some scholars believe that it does have such a status,[870] others disagree and support only some aspects of such reasoning,[871] whilst another group reject it entirely.[872]

At the outset, it could be said that the 'old' global commons share some unique characteristics, namely (1) they cannot be subject to sovereignty; (2) they are all natural environments, which acquired the status of global commons by discovery; (3) they are all

[866] ibid.
[867] ibid.
[868] ibid.
[869] For example, Bill Davidow, 'The Tragedy of the Internet Commons' (May 2012) *The Atlantic* <http://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/>; Dominic Basulto, "The 'Doomsday' Virus and the Tragedy of the Internet Commons" (July 2012) *Washington Post* <http://www.washingtonpost.com/blogs/innovations/post/the-doomsday-virus-and-the-tragedy-of-the-internet-commons/2012/07/>.
[870] Gerald Stang, 'Global Commons: Between Cooperation and Competition' (2013) European Union Institute for Security Studies <http://www.iss.europa.eu/uploads/media/Brief_17.pdf>; Kamlesh Bajaj, 'Cyberspace as Global Commons: The Challenge', (2012) Cyber Security <https://www.dsci.in/sites/default/files/Cyberspace%20as%20Global%20Common_DATAQUEST_0.pdf>.
[871] for example, Sean Kanuck, 'Sovereignty Discourse on Cyber Conflict Under International Law' (2010) 88 Texas Law Review.
[872] for example, Patrick Franzese, 'Sovereignty in Cyberspace: Can it Exist?' (2009) 64 Air Force Law Review.

governed by international treaties; (4) each of these treaties provides for specific permissible uses, such as peaceful purposes and scientific research; (5) each prohibit certain belligerent behaviour of states, such as use of nuclear weapons; (6) each area that constitutes the common is well defined by its treaty, thus: (a) The Antarctic Treaty defines global commons as 'south of 60 degrees South Latitude, including all ice shelves';[873] (b) high seas extend to 'all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a state, or in the archipelagic waters of an archipelagic state',[874] therefore where a coastal state has claimed an EEZ of 200nm, the high seas commence from that point;[875] (c) the Outer Space Treaty proclaims global commons to be 'all outer space, including the Moon and other natural celestial bodies';[876] finally (6) the global commons are shared by all.

Cyberspace is often referred to as one, monolithic domain, when in fact it is formed of layers, which comprise the hardware (referred to as the physical layer), the logical infrastructure layer and the content layer.[877] Some commentators point to a fundamental flaw in categorizing cyberspace as a common, drawing attention to the fact that at least some of cyberspace's physical layer is located within sovereign territories, which makes it fundamentally incompatible with the idea of the 'commons'. Thus, Kanuck wrote that:

> [e]very component of every information and telecommunications network around the world, under the sea and in the air is subject to proprietary interests-whether that of a private company, a sovereign government, or possibly both. Each copper wire, fiber-optic cable, microwave relay tower, satellite transporter, or internet router has been produced or installed by some entity, whose legal successors not only maintain ownership of that physical asset but also expect protection of the same by sovereign authorities.[878]

This is a compelling argument, which also reinforces another fundamental difference between the global commons and cyberspace: the former are entirely natural environments, whilst the

[873] The Antarctic Treaty, supra note 125, art IV.
[874] UNLOSC 1982, supra note 23, art 86.
[875] Rothwell and Stephens, supra note 35, p. 155.
[876] The Outer Space Treaty, supra note 94, art II.
[877] Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access' (2000) 52 Federal Communications Law Journal, <http://www.yale.edu/lawweb/jbalkin/telecom/benklerfromconsumerstousers.pdf>.
[878] Kanuck, supra note 133.

latter is a wholly artificial one. The global commons would continue existing without human support. Indeed, it could be argued that the human activities on the oceans, the outer space and the Antarctic are detrimental to the very existence of these spaces. In that sense, continued human presence therein has been termed as the 'tragedy of the commons', because the 'freedom of the commons brings ruin to all'.[879] The same cannot be said about the physical assets of cyberspace, which are entirely dependent on human management and maintenance. Admittedly, some parts of the physical infrastructure of cyberspace are located within the ambit of the global commons, such as the fiber-optic cables laid on the ocean floor, but this alone does not qualify them as a 'common', since proprietary rights have already been vested in them.

Assuming that this is the case, could the content layer be classified as a global common? It is the information flow, the ether, which is so often characterized, as ubiquitous, 'a common knowledge common', or a 'common pool of resources', that has the ability to travel almost without restriction across borders and jurisdictions. In all probability the ether itself may not be owned, however legal structures can be imposed on the means, by which wireless communications and media broadcasts are propagated, both by the national authorities and international organizations. The International Communications Union for example, performs such a role in allocating electromagnetic frequencies among users and proscribe unauthorized interferences. Equally, states have demonstrated willingness to restrict, censor and on some occasions, ban entirely the information flow and content by a variety of means, including filtering techniques, self-regulation and legislation. Such delimiting of what should, or should not form part of the content layer of cyberspace shows that it is not free from sovereign rights, unlike the global commons, which by definition must be.

There are other differences between cyberspace and the domains of the global commons. As the latter were subject of discovery, a concerted effort was made by international community to subject them to a governance regime laid down in the treaties. Cyberspace has been constructed, not discovered and thus far lacks an internationally agreed governance structure solidified in an international document. Finally, whilst the areas of the global commons are designated for peaceful purposes, cyberspace has been and continues to be used for belligerent ends (alleged Russian attacks on Estonia and the Staxnet worm being the most frequently invoked examples). It is also subject to progressive militarization, both for defensive

[879] Garrett Hardin, 'Tragedy of the Commons', (1968) 162 Science 1243 < http://cecs.wright.edu/~swang/cs409/Hardin.pdf>.

and offensive purposes. For example, in 2011 the US Deputy Secretary of Defense Lynn, observed that 'the Pentagon has formally recognized cyberspace as a new domain of warfare' and that 'many militaries are developing offensive capabilities in cyberspace'.[880]

The *Tallinn Manual 2.0* International Group of Experts was also skeptical with respect of assimilating cyberspace to the high seas, international airspace, or the outer space in the sense of constituting a global common.[881] The Group noted that although such characterization may be useful in other than legal context, adopting such a nomenclature for cyberspace would 'disregard the territorial features of cyberspace and cyber operations that implicate the principle of sovereignty'.[882] The Group particularly observe that 'although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more [s]tates'.[883]

Nevertheless, there are clear unifying factors between cyberspace and the 'old' domains, one being that none of them is currently partitioned along territorial lines. This however, could be a matter of necessity rather than design. By their nature, the high seas and the outer space are impossible to carve up into separate territories. Admittedly Antarctica, being a continent, is subject to territorialization along the Wesphalian lines, as some states have already established their presence there. Therefore, the suspension of further sovereign claims has been achieved by agreement, rather than necessity. Similar reasoning could be applied to cyberspace. Although it may be argued that it is susceptible to segmentation, to do so would undermine its very purpose, thus 'non-sovereignty' could be partially a result of an international agreement and partially of an inability to totally enclose it within any given territorial boundary.

Another similarity between cyberspace and the global commons relates to the governance challenge. One of the reasons behind entrusting the global commons to the care of the whole of the international community, as shared resources, was a recognition that these spaces are just too big and too challenging to be looked after by any individual state alone and therefore their stewardship was entrusted to a collective.[884] The same could be said of cyberspace. Governments have demonstrated an ability to regulate some aspects of cyberspace and its

---

[880] William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy' (2010) Foreign Affairs < http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
[881] *Tallinn Manual 2.0*, supra note 4, para 5, p. 12.
[882] ibid.
[883] ibid.
[884] Hollis, supra note 92.

effects within their territories. Arguably, states acting in isolation cannot effectively resolve challenges posed by such activities, as cyber crime.[885] It was this realization that prompted the 2001 Council of Europe Convention on Cybercrime, which entered into force in 2004 and its open to any state. To date, the Convention has been ratified by forty-four states, including non-Council of Europe members, such as Australia, Japan and the United States. Its Preamble specifically recognizes 'the value of fostering co-operation with the other States parties to this Convention and it is 'convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cyber crime, *inter alia*, by adopting appropriate legislation and fostering international cooperation'.[886]

In summary, the current mechanisms for the management of the global commons are a good starting point and a useful analogy for guiding any future cyberspace governance. However, the differences outlined above between the global commons and cyberspace are such, that cyberspace as a whole does not meet the internationally accepted legal criteria to be construed as a global common under the existing international law. This necessitates a *sui generis* regime for that domain.

3. CYBERSPACE AND THE COMMON HERITAGE OF MANKIND

The term 'global commons' denotes international domains, which hold common-pool resources and include the high seas, the Antarctic and the outer space. 'Common heritage of mankind' by comparison, is a principle of international law, which applies to 'the parts of the Earth and cosmos that can be said to belong to human posterity, without regard for geographical location. The term embraces the ocean floor and its subsoil and outer space'.[887] While cyberspace, on the face of it, seems not to be one of the areas of the global commons for the reasons outlined above, it will be shown here that the principle of the common heritage of mankind, applied by analogy, may be of value in this context.

Over time international law has developed a number of different types of legal regimes to govern natural resources, which include: (1) according states exclusive permanent sovereignty over some resources derived from the idea of territoriality; (2) sharing resources, for example international rivers and migratory species; (3) recognizing common property rights, as in the

[885] ibid.
[886] Convention on Cybercrime, The Preamble, supra note 28.
[887] *Black's Law Dictionary*, supra note 87, p. 269.

case of high seas, where no one user has exclusive rights to resources and no one can exclude others from exploiting them; (4) recognizing property, as a common heritage of mankind, whereby all manage resources and share in the rewards of exploiting them, even if they are unable to participate in that exploitation.[888]

(a) Common Heritage of Mankind in International Law

The principle of common heritage of mankind (CHM) was adopted in Article 1 of the 1970 *Declaration of Principles Governing the Sea-Bed and the Ocean Floor and the Subsoil Thereof, Beyond the Limits of National Jurisdiction*[889] (also known as the Declaration of Principles 1970), which states that 'the sea bed and ocean floor and the subsoil thereof, beyond the limits of national jurisdiction (hereinafter referred to as an area), as well as the resources of the area, are the common heritage of mankind'.[890]

The international treaties, explicitly mentioning the CHM are:

(1) The 1967 Outer Space Treaty, which states in Article 1 that

> [t]he exploration and the use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interest of all countries, irrespective of their degree of economic or scientific development and shall be the province of all mankind.[891]

(2) Article 11 of the 1979 Moon Treaty explicitly refers to CHM principle, by stating that 'The Moon and its natural resources are the common heritage of mankind'.[892]

(3) Part XI of the 1982 United Nations Convention on the Law of the Sea, which in Article

[888] John E. Noyes, 'The Common Heritage of Mankind: Past, Present and Future' (2012) 40 Denver Journal of International Law and Policy, 447.
[889] Declaration of Principles Governing the Sea-Bed and the Ocean Floor and the Subsoil Thereof, Beyond the Limits of National Jurisdiction, A/RES/2749 (XXV) of 17th December 1970.
[890] ibid, art 1.
[891] The Outer Space Treaty, supra note 94, art 1.
[892] The Moon Treaty, supra note 108, art 11.

136 provides that 'the area and the resources are the common heritage of mankind'.[893] The 'area' is defined in the Convention as 'the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction'[894] and 'resources' are enumerated as 'subsoil, liquid or gaseous mineral resources in situ in the area at or beneath the seabed, including polymetallic nodules';[895]

The 1959 Antarctic Treaty does not refer to the CHM, but there is a broad consensus that the Treaty provides normative bases for its application to that environment.[896]

The common heritage concept is embodied in great detail in the 1982 UNCLOS, Part XI and as such, has been hailed as 'one of the most advanced frameworks ever articulated, with the aim of achieving the equitable sharing of resources among states and peoples'.[897] The elements often associated with the CHM principle include: (1) a prohibition of acquisition of, or exercise of sovereignty over the area or resources in question; (2) the vesting of rights to the resources in question in humankind as a whole; (3) reservation of the area in question for peaceful purposes; (4) protection of the natural environment; (5) an equitable sharing of benefits associated with the exploitation of the resources in question, paying particular attention to the interests and needs of developing states; and (6) governance via a common management regime.[898]

The CHM has been the subject of debate and controversy since it was first introduced in the 1960s and it remains so to this day. The uncertainty relates to its scope, content and status. This is for an number of reasons, one being that no one global forum reached a consensus on its meaning at the early development stages and consequently its 'fleshing out' was left to the commentators, who disagree about its legal status and elements.[899] In addition, CHM questions the regimes that apply to resources of global significance, irrespective of where they are situated and therefore challenges traditional international law concepts, such as acquisition of territory, sovereignty, sovereign equality and international personality as well as the

[893] UNLOSC 1982, supra note 23, art 136.
[894] ibid, art 1(1).
[895] ibid, art 133(a).
[896] Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law', 10 (2006) Max Plank Yearbook of United Nations Law, 191 p. 235.
[897] Felipe Paolillo, 'The Institutional Arrangements for the International Seabed and Their Impact on the Evolution of International Organizations' RdC 188(1984)
[898] Noyes, supra note 150, p. 450-451.
[899] ibid, p. 459.

allocation of planetary resources and consent-based sources of international law.[900]

As regards its legal status, academic opinions vary as to whether it constitutes a principle of international law, a theory, a doctrine, or just a political and philosophical notion.[901] Some confine it to the realm of 'politics, philosophy and morality',[902] others point out to the undeniable fact that the CHM is contained in international treaties,[903] which have effectively prevented developed countries' private enterprise from starting to exploit CHM spaces until now.[904] There is some support for the argument that the common heritage principle, since it was introduced by the UN General Assembly Resolution 2574,[905] sets out a fundamental and non-derogable norm, constituting *jus cogens* obligation.[906] In fact, it was the subsequent 1970 Declaration of Principles,[907] which followed on from the original CHM that provided for the principles of non-appropriation, peaceful use, universal participation in its management and exploitation, equitable sharing in the benefits flowing from the exploitation of the seabed (especially benefiting developing countries), scientific cooperation and protection of the environment.[908] However, whether these principles amount to *jus cogens* is uncertain, as they may merely be of *lex ferenda* value.[909]

As for its content, an example of what the CHM comprises can be found in Part XI on the United Nations Convention on the Law of the Sea.[910] Part XI of the UNCLOS 1982 represents a comprehensive legal regime, setting out the norms and institutional arrangements for regulating the seabed as common heritage of mankind, a fact which in itself was interpreted as a major landmark and an important departure from traditional liberal international law.[911]

---

[900] Kemal Basler, *The Concept of Common Heritage of Mankind*, (Kluwer Law International 1997).
[901] Segura-Serrano, supra note 158.
[902] S. Grove, "The Concept of 'Common Heritage of Mankind': A Political, Moral and Legal Innovation?" 9 (1972) San Diego Law Review 390.
[903] Arnaldo Cocca, 'The Common Heritage of Mankind: Doctrine and Principle of Space Law', in Seggura-Serrano, supra note 158 p. 237.
[904] ibid.
[905] General Assembly Resolution 2574 A/RES/2574 (XXIV) of 15 December 1970
[906] Third United Nations Conference on the Law of the Sea Official Records, UN Sales No. E.82.V. (1980) (statements of representative of India, Trinidad and Tobago, Argentina, Iran, Jamaica and Niger).
[907] 1970 Declaration of Principles, supra note 151.
[908] Segura-Serrano, supra note 158, p. 238.
[909] ibid.
[910] A/RES/48/263 of 28 July 1994.
[911] Felipe Paolillo, 'The Institutional Arrangements for the International Seabed and Their Impact on the Evolution of International Organizations' RdC 188(1984).

Four norms comprise the CHM regime applicable to the seabed. Fist, Article 137 states that 'no state shall claim or exercise sovereignty or sovereign rights over any part of the area or its resources, nor shall any state or natural or juridical person appropriate any part thereof'.[912] Secondly, Article 140 (1) provides that:

> [a]ctivities in the area shall […] be carried out for the benefit of mankind as a whole, irrespective of geographical location of states, whether coastal, or land locked and taking into particular consideration the interests and the needs of developing states and of peoples who have not attained full independence or other self governing status […][913]

and in subsection (2) calls for 'equitable sharing of financial and other economic benefits derived from activities in the area through any appropriate mechanism, on a non-discriminatory basis'.[914] Thirdly, Article 141 obliges states to explore and exploit the area 'exclusively for peaceful purposes';[915] and finally (d) Article 145 sets out a duty 'to ensure effective protection for the marine environment from harmful effects which may arise from (activities) in the area'.[916]

Article 156 established the International Seabed Authority, an organization through which all states 'shall organize and control activities in the area',[917] a provision, which calls for common governance and management of the area.

The regime set out in the 1979 Moon Treaty resembles Part XI of the UNCLOS 1982 in the following ways. It prohibits occupation, or appropriation. Thus, Article 11(2) of the Moon Treaty provides that 'the Moon is not subject to national appropriation by any claim of sovereignty, by means of use or occupation, or by any other means'.[918] It also considers utilization of the Moon and its resources to be for the benefit of the mankind. In this context, Article 4 provides for the 'exploration and the use of the Moon [to be] a province of all mankind and shall be carried for the benefit and the interest of all countries'.[919] Furthermore, it obliges peaceful use- Article 3 states that 'the Moon shall be used by all parties exclusively for peaceful

[912] UNCLOS, supra note 23, art 137(1).
[913] ibid art 140(1).
[914] ibid art 140(2).
[915] ibid art 141.
[916] ibid art145.
[917] ibid art 157.
[918] The Moon Treaty, supra note 108, art 11(2).
[919] ibid art 4.

purposes'.[920] It protects the environment.[921] Finally, it makes provision for a common administration through setting up of 'an international regime, including appropriate procedures, to govern the exploitation of natural resources of the Moon'.[922]

To summarise, the CHM principle is a product of the 1960s and 1970s political climate and incorporates several norms including non-appropriation, equitable sharing, peaceful purposes, environmental protection and cooperation in the management of common resources. The controversy surrounding the concept relates to its undefined content and legal status. However, its successful application to the areas specified in the treaties is a testament to its success and continued utility. It has also undergone a revival in recent years in the context of its proposed application to cyberspace governance.

(b) Common Heritage of Mankind and Cyberspace Governance

Since there is no agreement among the international community regarding the nature of cyberspace, deciding on the legal framework that is acceptable to all states is inevitably going to be challenging. Achieving such framework could be informed and inspired through analogy to the principle of common heritage of mankind. Admittedly, the reality of state practice and the elements of the CHM are not a perfect fit, however that does not mean that the principle should not be a guide to inform the cooperation among states to resolve the current political impasse, resulting from the Dubai 2012 Conference, as outlined in the previous chapter. Before analysing how CHM relates to the current state practice in cyberspace, it is worth reiterating that the physical infrastructure of cyberspace, which is located within state's territory is subject to that state's territorial sovereignty. It is the content layer of cyberspace, which may benefit from applying CHM by analogy.

Despite the fact that there is no definition of CHM and therefore no agreement on its component parts, four core elements (some outline above) are commonly perceived to comprise the principle.

The first dictates that the area under consideration cannot be subject to appropriation. Assuming that the internet's methods of establishing communication are non-territorial, because names and addresses create a virtual space that is often independent of geography and

[920] ibid art 3.
[921] ibid art 7.
[922] ibid art 11(5).

usable by anyone without paying a fee,[923] then the principle of non appropriation may be satisfied. It is true that private and public companies own the internet infrastructure, but it is doubtful that they own its content, which is created by everyone who uses the facility. This does not preclude state's control and there are sufficient examples of practices, some of which were outlined in the Chapter 2 of this study, relating to content regulation. Such practices however do not equate with content 'appropriation'. On the other hand, although the internet is decentralized, it is under a great influence of one state, namely the US. This is due to a number of factors, such as almost total domination over the internet service provision by the American technology giants, the US government's having had the ultimate control over the entire world's domain name and numbering system until October 2016[924] and the internet architecture giving US intelligence agencies access to data of millions of non-US citizens. It is in this sense and through US privately own companies, such as cable owners, the hardware and software developers and the commercial enterprises (Google, Amazon, Instagram, Facebook, Ebay etc.,), which dominate the word telecommunication sector that the idea of non-appropriation comes under strain. It is their almost total domination of that market place, which could be equated with 'appropriation'. Even this logic however, should not preclude the CHM from forming the basic building block of future governance. In this sense, the idea of non-appropriation could reinforce the aspirations behind internet governance articulated by the Working Group on Internet Governance, defined as 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the internet'.[925] If the content layer of cyberspace were to have the status of the common heritage of mankind set out in a legally binding treaty, this could hypothetically preserve the internet as a open forum for exchange of information, while at the same time recognizing sovereign rights of states and involve all community from both developing and developed nations.[926]

---

[923] Milton Mueller, John Mathiason and Hans Klein, 'The Internet and Global Governance: Principle and Norms for a New Regime' (2007) 13 Global Governance 237.
[924] Edward Moyer, 'US Hands Internet Control to ICANN' (2 October 2016) <https://www.cnet.com/uk/news/us-internet-control-ted-cruz-free-speech-russia-china-internet-corporation-assigned-names-numbers/>.
[925] Report form the Working Group on Internet Governance, World Summit on the Information Society, Geneva 2003-Tunnis 2005 (3 August 2005), Doc. WSIS-II/PC-3/DOC/5E, 3 para 10.
[926] Sugera-Serrano, supra note 158.

The second element of the CHM principle is that all countries must share in the management of the resources. For such management to become a reality in the context of cyberspace, a specialist agency would need to be established to coordinate shared management policies. International Seabed Authority (ISBA) could be seen as an example of an international institution with clear delineation of powers and responsibilities, which made it a successful guardian of deep seabed resources, that would have otherwise been open for exploitation by the states with the best technological leverage. By designating the area as a common heritage of mankind site, the international community recognized a need for establishing the International Seabed Authority as a central institution, through which according to Article 157 (1) of the UNCLOS 1982, 'state parties shall organize and control activities in the area, particularly with a view to administering the resources of the area'.[927] The ISBA does not have an absolute power over the seabed, rather its competence relates only to mineral resources on the seabed's surface. This means that activities that have an impact on the seabed, but which are unconnected with the mineral resources are unregulated by that organization.[928] Consequently, the ISBA does not have any general environmental jurisdiction over the seabed. Although Article 145 of the UNCLOS 1982[929] expressly states that the authority shall adopt appropriate rules, regulations and procedures to protect the marine environment from damage from prospecting, exploring and mining resources on the seabed, it is only in the context of mitigating the environmental impact of mining the minerals and does not relate to all activities on the seabed. The ISBA structure is set out in the UNLOSC 1982 and made up of three principal organs, the Assembly, the Council and the Secretariat. There are a further three bodies that make up the ISBA, that is the Enterprise, is an organ through which the ISBA carries out

[927] UNLOSC, supra note 23, art 157(1).
[928] Rothwell and Stephens, supra note 35.
[929] UNLOSC, supra note 23, art 145 *Protection of the Marine Environment:*

1. [n]ecessary measures shall be taken in accordance with this Convention with respect to activities in the Area to ensure effective protection for the marine environment from harmful effects, which may arise from such activities. To this end the Authority shall adopt appropriate rules, regulations and procedures for *inter alia*:
   (a) the prevention, reduction and control of pollution and other hazards to the marine environment, including the coastline, and of interference with the ecological balance of the marine environment, particular attention being paid to the need for protection from harmful effects of such activities as drilling, dredging, excavation, disposal of waste, construction and operation or maintenance of installations, pipelines and other devices related to such activities;
   (b) the protection and conservation of the natural resources of the Area and the prevention of damage to the flora and fauna of the marine. environment.

its capacity to engage with seabed mining directly and two subsidiaries, Legal and Technical Commission and the Finance Committee. Decision-making is by consensus and only when that fails, decisions may be taken by vote. Applying by analogy some of these ideas and structures to the content layer of cyberspace by establishing a body modelled on the ISBA may help to diffuse the disproportionate influence over this domain by the US. The fact that such an authority will not have a general jurisdiction over all matters relating to the entirety of cyberspace, but be a guardian in protecting the content layer from exploitation by a handful of wealthy and technologically advanced states to the detriment of the rest of the international community, could contribute to equitable sharing. The International Telecommunications Union continues to be the UN organization of choice for some states, such as the Russian Federation and the People's Republic of China to oversea the functioning of the internet. However, in the light of the US government's handover of the naming of the domain name system to ICANN in 2016, the role of the ITU as the leading body overseeing the workings of the internet seems to have been side-lined and appears now to be even more aspirational then before. Nevertheless, the ITU continues in its role of allocating globally of the frequency bands of the electronic spectrum for various wireless telecommunications systems, such as mobile telephony or GPS. Whether or not its role as a guardian protecting the content layer of the internet will ever materialize is highly speculative. The added uncertainty also relates to the ITU's role as a standard setting body handling such issues as mass cyber surveillance and privacy protection.

The third element of the CHM dictates that there must be an active sharing of the benefits reaped from the exploitation of the area resources. This relates in many respects to the previous idea of shared management, but its main thrust is on making sure that developed and developing countries benefit equally. The 2003-2005 World Summit on the Information Society in the Declaration of Principles, referred to in the previous chapter, made a 'commitment to build a people-centred, inclusive and development-orientated information society'[930] central to its common vision of information society. This commitment arose out of

[930] Declaration of Principles of the World Summit on the Information Society, *Building the Information Society: A Global Challenge in the New Millennium*,
Principle 1:

> [w]e, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and

the recognition contained in paragraph 10 of the Declaration, 'that the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries and within societies. We are fully committed to turning this digital divide into a digital opportunity for all, particularly for those who risk being left behind and being further marginalized'.[931] This is why 'the representatives of the people of the world'[932] who gathered at the WSIS pledged to continue to 'pay special attention to the particular needs of people of developing countries'[933] through 'building an inclusive information society, which requires new forms of solidarity partnership and cooperation among governments and other stakeholders, i.e. the private sector, civil society and international organizations'.[934] The idea of equitable sharing, for example in the context of deep seabed mining, has long been contested by the US. Although the principle seems to be well suited in the context of cyberspace, its future may be confined to an aspiration, rather than reality and perhaps should be subsumed, at least for the time being, within the concept of common management, as a more realistic solution.

Finally, the area subject to the CHM must be reserved for peaceful purposes. In this context, 'the militarization of cyberspace is not a risk, it is already a fact, with the armed forces of several states establishing cyber units and including cyber operations in their military doctrines and strategies'.[935] Cyberspace, as a 'fifth battlefield', is a reality and the existing rules of *jus ad bellum* and *jus in bello* are not only applicable, through the notion of evaluative interpretation of treaties, but also flexible enough to meet the challenges of new cyber realities.[936] It is in this sense that the CHM could serve a particularly useful purpose, as a principle to help foster cyberspace disarmament and promote knowledge, information and communication, education and political participation.[937]

---

improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.

Document,WSIS-03/Geneva/Doc/4-E <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

[931] ibid, paragraph 10.

[932] ibid paragraph 1.

[933] ibid paragraph 16.

[934] ibid paragraph 17.

[935] Roscini, supra note 27.

[936] ibid.

[937] Segura-Sorrano, supra note 158.

The common heritage of mankind, as a set of principles could play a useful role in the future of internet governance. It is true to say that at present its constituent elements are not quite the perfect fit. However, it has a successful track record in the context of the exploitation of deep sea bed resources. Therefore, in spite of its limitations, the common heritage of mankind 'applies reasonably well to the internet's core resources', albeit 'it has not been mentioned to date in the context of internet governance negotiations'.[938]

4. THE REGIMES GOVERNING THE EXCLUSIVE ECONOMIC ZONE/ CONTINENTAL SHELF AND THEIR APPLICABILITY TO CYBERSPACE

There are examples in international law, where an alternative categorization of the Earth's resources has been utilized providing a legal framework for areas that are neither a sovereign territory, nor a global common. In fact, sovereignty and *res communis*, according to Hollis, operate as two poles, with a spectrum of other resources and governance frameworks lying between them.[939] Two examples of such regimes are the Exclusive Economic Zone (EEZ) and the Continental Shelf (CS). It is submitted that some aspects of cyberspace share the characteristics of EEZ/CS regimes and could be classified as such a hybrid domain for the purposes of legal classification.

The rationale for establishing the EEZ was two-fold. First, it was dictated by the ambition of the southern states to obtain their fair share of coastal maritime living and non-living resources. Secondly, there was an expectation that it would address the tragedy of the ocean commons resulting from the unregulated exploitation of marine living resource through their enclosure within the 200nm zone and therefore better its management.[940] It could be said that for over thirty years the EEZ/CS have successfully merged sovereign rights in relation to economic resources and jurisdiction in relation to these and other rights, such as environmental protection. They are distinct regimes that combine the characteristics of territorial sovereignty, with those of *res communis.*[941]

The definitions of both the EEZ and the Continental Shelf contained in Article 55 and Article 77(1) of the 1982 UNCLOS respectively have been referred to in Chapter 2. The EEZ

[938] ibid p. 260.
[939] Hollis, supra note 92.
[940] Rothwell and Stephens, supra note 35, p.83.
[941] ibid p. 84.

is the water column, seabed and subsoil of a outer limit of 200nm, whereas the Continental Shelf is a shallow area of the seafloor adjacent to the coast, where the so-called continental margin slopes down gradually from the landmass into the sea until it begins to drop more sharply towards the deep ocean floor[942] and also extends to 200nm. This creates some overlap between the two regimes. The precursor to the EEZ was the assertion by some states (mainly Iceland) of the fisheries jurisdiction in the Exclusive Fishing Zone, which until 1971 extended to 50nm.[943] In parallel, other states, such as the US through the 1945 Truman Proclamation also claimed jurisdiction over economic resources on appurtenant continental shelves.[944] State practice in the years prior to the negotiations of the UNCLOS 1982 firmly established 200nm as the breath of the EEZ, which was by that time generally recognized as part of customary law.

The legal framework governing the EEZ is set out in Part V of the 1982 UNCLOS, whereas that applicable to the Continental Shelf, in Part VI. A feature that is worth noting, is that the EEZ is a 'claimable' maritime zone.[945] By contrast, the continental shelf is a resource zone that does not need to be claimed. In line with Article 57 of the 1982 Convention, the EEZ extends from the baseline of the territorial sea to cover the area not exceeding 200nm.

Part V of the UNCLOS 1982 draws a distinction between two categories of states, that is, coastal states and other states. The former are afforded (1) sovereign rights for the purpose of exploring, exploiting, conserving and managing natural resources of the seabed, subsoil and water column; together with (2) jurisdiction in relation to artificial structures, marine scientific research and environmental preservation and protection.[946] Non-costal states have the freedom

---

[942] ibid p. 98.
[943] ibid.
[944] ibid.
[945] UNLOSC 1982, art 5 *Breadth of the Exclusive Economic Zone*:

> '[t]he exclusive economic zone shall not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured.'

[946] UNCLOS art 56 *Rights, Jurisdiction and Duties of the Coastal State in the Exclusive Economic Zone:*

1. [i]n the exclusive economic zone, the coastal State has:
   (a) sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources, whether living or non-living, of the waters superjacent to the seabed and of the seabed and its subsoil, and with regard to other activities for the economic exploitation and exploration of the zone, such as the production of energy from the water, currents and winds;
   (b) jurisdiction as provided for in the relevant provisions of this Convention with regard to:
      (i) the establishment and use of artificial islands, installations and structures;

of navigation and overflight, the laying of submarine cables and pipelines and 'other internationally lawful uses of the sea related to these freedoms'.[947]

(a) Sovereign Rights of Coastal States

The sovereign rights in the EEZ of coastal states extend to both living and non-living resources.

In the case of living resources these rights verge on absolute,[948] since by virtue of Article 56 UNCLOS 1982, coastal states are given exclusive sovereign rights over fisheries and exclusive jurisdiction to regulate fishing in the EEZ.[949] The rights allocated under Article 62 UNCLOS 1982 relate to virtually every aspect of fishing, which places it under coastal state's close scrutiny. For example, coastal states have sole discretion in setting allowable catch of the living resources in their zone.[950] However, they are under a duty to ensure that the living resources are not exhausted by over exploitation through proper conservation and management measures.[951] In principle, when the coastal nations do not have a capacity to harvest the entire allowable catch, they must give other states access to its surplus.[952] This right, as noted by Rothwell and Stephens, in practice is not enforceable because 'coastal state decisions determining the allowable catch, the extent of harvesting capacity and the allocation of surpluses, fall within one of the few exceptions to the compulsory dispute resolution system set out in Part XV'.[953]

There is a total overlap between the regimes of the EEZ and the CS regarding the non-living resources found in the seabed and subsoil. Both regimes confer on coastal states exclusive rights of exploitation and exploration for non-living seabed resources, such as hydrocarbons and minerals, without any obligation of conservation, or judicious use.[954] In this sense, the rights over the non-living resources are full and exclusive, as they place no requirement on

---

(ii) marine scientific research;
(iii) the protection and preservation of the marine environment;

[947] ibid, art 58(1).
[948] Rothwell and Stephens, supra note 35, p.88.
[949] UNCLOS, art 62(4):

> [n]ationals of other States fishing in the exclusive economic zone shall comply with the conservation measures and with the other terms and conditions established in the laws and regulations of the coastal State.

[950] UNCLOS, art 61.
[951] UNCLOS, art 61(2).
[952] ibid, art 62(2).
[953] Rothwell and Stephens, supra note 35, p. 88.
[954] ibid p.89.

these countries to share access, not to mention any benefits, from their exploitation, as could be gleaned from the wording of Article 77 UNCLOS.[955]

(b) Jurisdiction of Coastal States

Article 56 of the UNCLOS 1982 confers on states jurisdiction in relation to specified activities, namely (1) establishment and use of artificial islands, installations and structures; (2) marine scientific research (3) the protection and preservation of marine environment and (4) other rights and duties as specified under the Convention.[956]

With regard to artificial islands, installations and structures, the jurisdictional rights under the regime of EEZ (Article 60) substantially overlaps with that set up under the CS (Article 80). According to Article 60, states have exclusive jurisdiction to construct, authorise and regulate the construction and operation of artificial islands, installations and structures for economic purposes.[957] Moreover, they also have exclusive jurisdiction in relation to customs,

---

[955] UNCLOS, art 77 *Rights of the coastal State over the continental shelf*

1. [t]he coastal State exercises over the continental shelf sovereign rights for the purpose of exploring it and exploiting its natural resources.
2. The rights referred to in paragraph 1 are exclusive in the sense that if the coastal State does not explore the continental shelf or exploit its natural resources, no one may undertake these activities without the express consent of the coastal State.
3. The rights of the coastal State over the continental shelf do not depend on occupation, effective or notional, or on any express proclamation.
4. The natural resources referred to in this Part consist of the mineral and other non-living resources of the seabed and subsoil together with living organisms belonging to sedentary species, that is to say, organisms which, at the harvestable stage, either are immobile on or under the seabed or are unable to move except in constant physical contact with the seabed or the subsoil.

[956] UNCLOS, art 56(1)(b).

[957] UNCLOS, art 60 *Artificial Islands, Installations and Structures in the Exclusive Economic Zone*

1. [i]n the exclusive economic zone, the coastal State shall have the exclusive right to construct and to authorize and regulate the construction, operation and use of:
   (a) artificial islands;
   (b) installations and structures for the purposes provided for in article 56 and other economic purposes;
   (c) installations and structures which may interfere with the exercise of the rights of the coastal State in the zone.
2. The coastal State shall have exclusive jurisdiction over such artificial islands, installations and structures, including jurisdiction with regard to customs, fiscal, health, safety and immigration laws and regulations.

fiscal, health, safety and immigration laws and regulations.[958] This provision allows facilities to be constructed to take advantage of all economic resources both in and on the seabed and the water column.[959] Of particular note is the fact that coastal states jurisdiction extends only to those installations and structures, which have economic purpose, with no mention made to military installations. However, since there is no restriction on jurisdiction for economic purposes only on artificial islands under Article 60(1)(a) and no definition of 'artificial islands', 'installations' and 'structures', states presumably may regulate any substantial infrastructure within the EEZ notwithstanding its purpose.[960]

The provisions of jurisdictional rights regarding the marine scientific research stipulate that other states and international organizations may only carry out such activities within the EEZ with the consent of the relevant coastal state,[961] which shall in normal circumstances grant the consent.[962] This may however be withheld, if the marine research relates directly to the search for living and non-living resources and/or involves the construction, operation or use of artificial islands, installations and structures.[963]

Finally, coastal states have extensive rights and powers to protect the entire maritime environment within the EEZ in an integral manner. Part XII UNCLOS confers on these nations prescriptive and enforcement jurisdiction in relation to three heads of maritime pollution: pollution from seabed activities and in relation to artificial structures,[964] pollution by dumping,

---

[958] ibid.
[959] Rothwell and Stephens, supra note 35.
[960] ibid p. 91.
[961] UNCLOS, art 246 *Marine Scientific Research in the Exclusive Economic Zone and on the Continental Shelf*

1. [c]oastal States, in the exercise of their jurisdiction, have the right to regulate, authorize and conduct marine scientific research in their exclusive economic zone and on their continental shelf in accordance with the relevant provisions of this Convention.
2. Marine scientific research in the exclusive economic zone and on the continental shelf shall be conducted with the consent of the coastal State.

[962] UNCLOS, art 246(3).
[963] ibid, art 246(5)(a),(c).
[964] UNCLOS, art 208 *Pollution from Seabed Activities Subject to National Jurisdiction*

1 [c]oastal States shall adopt laws and regulations to prevent, reduce and control pollution of the marine environment arising from or in connection with seabed activities subject to their jurisdiction and from artificial islands, installations and structures under their jurisdiction, pursuant to articles 60 and 80.

which cannot be carried out 'without express prior approval of coastal state'[965] and incidental pollution from vessels.[966]

(i) 'Creeping Jurisdiction'

The extent, to which the UNCLOS 1982 grants sovereign and jurisdictional rights to coastal states categorises the EEZ zones as as *sui generis*, not to be assimilated with the concepts of territorial sea or the high seas.[967] The invention of these mechanisms, together with the codification of the whole of the maritime regime in a single international treaty achieved within one generation, has been recognized as one of the major successes of the United Nations.[968] Indeed, most countries (125 out of 152 coastal states) and those who are not party to the UNCLOS 1982, have claimed the EEZ. However, in recent years a number of coastal states have tried to gradually extend the scope of their jurisdiction in the EEZ, a phenomenon described as 'creeping jurisdiction'. The term in the maritime context, sometimes also referred to as 'Craven's Law',[969] denotes a dichotomy between the territorial sea and the high sea and suggests 'that any coastal state extension of jurisdiction into the contiguous high sea, even if functionally limited, tends over time to extend to include more claims, until it becomes the functional equivalent of a territorial sea, in substance, if not in name'.[970] The word 'creeping' in this context denotes the idea of unilateral action directed at upsetting a legal framework adhered to by the majority of other states.[971] In the sphere of maritime law, the transgression of states' competences relates to 'spatial creeping' beyond 200nm limit. There is some evidence of state practice to suggest that since the UNCLOS 1982 came into force a number of states made attempts at claiming jurisdiction over the living resources beyond the 200nm limit. There is some evidence of activities of few nations in the period following the signing of

---

[965] ibid, art 210(5).
[966] ibid, art 211(5).
[967] Erik Franckx, 'The 200-mile Limit: Between Creeping Jurisdiction and Creeping Common Heritage?' (2007) 39 George Washington International Law Review 467.
[968] ibid.
[969] The term 'creeping jurisdiction' was coined by Dr John Craven, Special Projects Officer of the US Navy Department, who in the mid-1960, confronted with the speed of technological developments in relations to operations on he seabed predicted that sovereign rights claimed by coastal states over it would soon be followed by similar claims over the water column above. John Craven, *Sea Power and Sea Bed* (US Naval Inst. Porc. 1996).
[970] Richard Bilder, 'The Anglo-Icelandic Fisheries Dispute', (1973) 48 Wisconsin Law Review 37, 104.
[971] Franckx, supra note 229 p. 487.

the 1982 Convention, which illustrates instances of 'creeping jurisdiction' undertaken both unilaterally and as part of multilateral action. Examples of unilateral state action include the introduction in 1990 of a new concept in the law of the sea by Chile (the *mar presencial*, or 'presential' sea), which allowed that country, in a designated large zone beyond the Chilean EEZ, to assume enhanced presence, so that it could participate in activities undertaken by others, while at the same time trying to control them.[972] Similar legislation was enacted by Argentina in 1991 and its subsequent behaviour confirmed that these unilateral actions have some impact in extending the competence beyond the 200nm zone. Multilateral practices include coastal states' undertaking measures, which restrict the rights of third states with respect of living resources outside their 200nm limit. The establishment of pockets of high seas totally surrounded by maritime zones by a small number of coastal states, such as the Donut Hole in the Bering Sea, which is totally enclosed within the maritime zones of the Russian Federation and the U.S, not only undermines the effectiveness of maritime living resources management system, but also has a spill over effect into other areas of the law of the sea, such as fisheries.

However, not everyone agrees that creeping jurisdiction has undermined the freedom of the high seas. There are some authors, who are quite critical of the concept and consider this notion as 'conceptually unproven, probably invalid and largely irrelevant'.[973]

(c) The Applicability of the EEZ/CS Regimes to Cyberspace Governance

The importance of cyberspace in national security terms, its prolific use as a domain replete with criminal, espionage and subversive activities led some states to realize that to continue without closer international cooperation to govern this domain is unsustainable. In this regard, as already outlined in the previous chapter, some members of the Shanghai Cooperation, namely the governments of Russia, China, Tajikistan and Uzbekistan, submitted in 2011 to the UN Secretary General *Draft Code of Conduct for Information Security*, which was rejected by the US and subsequently re-drafted and re-submitted it in January 2015.[974] As with its predecessor, the revised *Code* called for 'enhanced state cooperation in addressing common threats and challenges in the information space in order to establish an information

[972] ibid.
[973] Robert Krueger, 'An Evaluation of the United States Ocean Policy', (1971) 17 McGill Law Journal 603.
[974] *Draft International Code of Conduct for Information Security,* supra note 72.

environment that is peaceful, secure open and founded on cooperation'[975] and emphasised throughout the need to maintain international peace and security. Several earlier attempts at regulating cyberspace through a treaty were made, including French proposals for adopting a 'Charter for International Cooperation' made in 1996.[976] Fundamental disagreements among governments relating to the nature of cyberspace and the modalities for its governance have made such cooperation nothing more than a 'pipe-dream'[977] and fueled continued skepticism among some scholars.[978]

On the domestic level, some states such as the United States has long recognized the need for norm development in the sphere of cyber security and in such documents as the *International Strategy for Cyberspace*[979] set out the vision for the future of cyberspace. Accordingly, secure cyberspace, *inter alia:*

> [r]ewards innovation and empowers individuals; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. To sustain this environment, international collaboration is more than a best practice; it is a first principle'.[980]

To achieve these goals, the document pledges that:

> [t]he United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation […] it we will build and sustain an environment in which norms of responsible

[975] ibid, paragraph 1 Purpose and Scope.
[976] Jack Goldsmith and Timothy Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2008).
[977] Adam Segal and Matthew Waxman, 'Why a Cybersecurity Treaty is a Pipe Dream' (2011) Council on Foreign Relations <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>.
[978] for Example, Jack Goldsmith, 'Cybersecurity Treaties: A Skeptical View' (2011) <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.
[979] White House, 'International Strategy for Cyberspace: Prosperity, Security and Openness in the Networked World' (2011), supra note 81.
[980] ibid.

behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[981]

In the light of the continued lack of consensus regarding a possible legal regime, one solution could be through applying the modalities of the EEZ/CS by analogy to meet half way the needs of the opposing 'cyber sides', that is the states, who wish to continue with the existing model of governance based on multistakeholder system and those wishing for greater state involvement, supporting the sovereign based approach. The EEZ/CS share some parallels with cyberspace, in that fundamentally full sovereignty is not possible either by design (in case of the EEZ/CS through a treaty), or the nature of its construct (cyberspace's main component, the internet relies on reticulation of networks, whose architecture defeats the notion of states' control through total border sealing). As noted above, the sovereign rights that are enjoyed by coastal states in the EEZ/CS are extensive. Similar provisions could be made in an umbrella treaty regime for cyberspace, so that states would have sovereign rights for specific purposes, such as economic and commercial exploration and exploitation of activities in their designated 'exclusive cyber zones'. However, the content layer, designated the status of the common heritage of mankind, could be protected against unlawful exploitation through *inter alia* mass surveillance and bulk collection activities of the most technologically advanced states. Equally, states would have to manage and preserve their digital resources in the same manner as some coastal states are obliged to do with respect to living resources in the EEZ/CS environments. Furthermore, individual states could have greater leverage over the individual service providers and search engines through conferring on them jurisdiction in relation to specified activities. In case of the EEZ/CS in certain instances specified in Article 56 of the UNCLOS 1982 jurisdiction is conferred exclusively on coastal states to conduct, authorize and regulate certain artificial constructs. Similarly, this could apply to all national telecommunications, where internet provision is subsumed within exclusive national jurisdictions. For example, in the UK the responsibility for the planning, assignment, management, development and regulatory framework of telecommunications is borne by OFCOM, an Independent Regulator and Competition Authority for the UK Communications Industry.[982] Its range of complex technical coverage includes the bandwidth, or frequency range allocated for land based ground terminals to Earth orbiting satellites, together with their operating protocols for world- wide

[981] ibid.
[982] OFCOM http://www.ofcom.org.uk/.

communications. Allocating such an authority with powers to manage development and regulatory framework for the UK 'exclusive cyber zone' may give greater autonomy, whilst at the same time force other states to act within that zone only by strictly respecting international law, including human rights obligations.

States' have extensive powers within both the EEZ and CS zones, but that power is strictly limited beyond it. However, evidence has shown some disregard of this delimitation in the form of use of maritime resources beyond the specified limit. To avoid the dangers of 'creeping jurisdiction' in cyberspace, lessons could be learned from the practical application of jurisdictional provisions in the 1982 Convention with respect to specifically delineating the scope and extent of states' jurisdictional competences, to avoid spill over effects. In the words of one commentator 'states' exclusive jurisdictions can only creep forward if the contraposed community interests withdraw before them. A failure of will should not be disguised behind pseudo-law'.[983] Furthermore, should any fine-tuning be required, this could be achieved through multilateral, regional or bilateral agreements among states. Equally, any dangers of 'jurisdictional creep' should serve as an incentive to become a party to the treaty.

Achieving the solution for cyberspace governance through a treaty modelled on the UN Law of the Sea Convention, which recognizes different areas, such as the 'global common knowledge area' akin to the high seas and 'exclusive cyber zones', similar to the exclusive economic zone, avoids treating cyberspace as a single environment and accommodates differing needs of nations. Like the UNLOSC 1982, cyberspace treaty could also be a 'package deal'. In this way, states wishing for greater sovereignty rights could enjoy such rights within their own boarders and have almost unfettered jurisdiction, whereas the common areas could continue to be run by the amalgam of private/public partnership.

Maritime life, the deep sea bed, electricity and radio frequencies are all naturally occurring Earthly phenomenon. Each is a natural raw material and converted by mankind for subsequent use. This commonality of being a product of nature lends support to the idea propagated in this chapter that the radio frequencies, which make communication via the internet possible should be given a status similar to the non-living resource in the EEZ regime and the content layer of cyberspace that of the common heritage of mankind and be based on similar principles that underpin this principle.

[983] L. Goldie, 'International Principles of Responsibility for Pollution' (1970) 9 Columbia Journal of Transnational Law 283.

CONCLUSION

This chapter has argued that the global governance of cyberspace is possible through modelling an international convention regulating state-to-state cyber activities on the already existing regimes, in particular the law of the sea. The governance of this domain requires greater coordination of sovereign states to tackle hostile and unlawful cyber operations, such as cyber crime, cyber espionage and mass surveillance through an international up- to- date legal framework.

There is a commonality between the nature of already existing taxonomy of various regimes of the sea and the developments in the sphere of cyberspace. It could be said that both environments are not monolithic but are comprised of various segments. Chapter 1 identified that cyberspace is considered to consist of three layers. The physical layer, as far as legal taxonomy is concerned, is the least problematic. When located within state's territory, it is subject to territorial sovereignty. Even if parts of the infrastructure, such as cables, are located within the area of high seas, they are still subject to sovereign rights. Chapter 2 argued that cyberspace does not fall within the criteria of *terra nullius* and asserting of territorial sovereignty over the entirety of cyberspace per se to the exclusion of all other states is in all probability not achievable. This chapter built on these assumptions and contended that cyberspace's content layer does not fall within any of the regimes of the 'old' global commons. Assuming that cyberspace is not a *terra nullius*, *res communis*, nor a sovereign territory, analogy was made to other hybrid regimes of exclusive economic zone and continental shelf. It has been concluded that by examining the practice of states in cyberspace, it seems that this domain bears more characteristics of the legal regimes of the EEZ, CS, than to the *res nullius*, *res communis,* or the sovereign territory. The chapter expanded this reasoning by proposing a legal framework for cyberspace that would adopt the concept of exclusive economic zone, investing in states sovereign rights and jurisdiction within their 'exclusive cyber zones'. Continued freedom and unrestricted information flow of the internet could be safeguarded by analogizing the common parts of the content layer of cyberspace to the regime of the deep sea bed and regarding it as the common heritage of mankind. Such underpinning would reinforce the principles already articulated by the WSIS, outlined in Chapter 2, of common management of the shared parts of the internet, equitable sharing, equal access, non-militarization, protection of on-line privacy.

The success achieved by the Law of the Sea Convention 1982 shows that gaining consensus to codify a multifaceted area is not only desirable, but achievable. Similarities could be drawn

between the early approaches taken to the vast expanses of the oceans and cyberspace, which were both initially considered as free and open, in Grotian *Mare Liberum* and in Barlow's *Declaration of Independence* respectively. State practice dictated a need for international law to devise differing maritime regimes for different spaces that emerged over the centuries and thus a checkerboard of territorial sea, the high seas, the deep seabed and other areas, such as the exclusive economic zone and the continental shelf were created, each with a distinct legal regime, but all subsumed within one umbrella Law of the Sea Convention. Admittedly, the oceans and the seas were subject to human activities for centuries and therefore the legal regime arose incrementally, unlike cyberspace, which by comparison is very new and riddled with disagreement and controversy. Furthermore, the obvious difference between these environments is that the former is natural, the latter entirely man made and underpinned by private enterprise. Nevertheless, both are used for commercial, economic and military purposes. Cyberspace, being a crucial part of civilian and military infrastructure of most nations, is coming under a ferocious strain from harmful activities emanating from state actors. It is also subject to increasing state control. At the same time, its very architecture dictates interconnectivity, which means that no single state could claim exclusive sovereignty over it. This calls into question categorization of cyberspace as a global common. The internet is largely an American invention and classifying it as a global common reflects a broader ideological approach of that country relating to the governance of the 'old' global commons, which is by and large perceived from a military perspective and therefore dictates continued access.

Greater state cooperation is desirable and needed but questions, such as what legal framework may best suit the state-to-state relationships in cyberspace remain unanswered. This chapter proposed a 'package deal' convention modelled on the UNCLOS 1982 to close this normative gap. Continued international disagreement casts doubt over a successful treaty being negotiated any time soon. However, both the success of the system for regulation of the seas as a whole and the provisions relating to the EEZ/CS in particular could be a guiding template for such an instrument. Moreover, lessons learned from the successful negotiations of other regimes regulating the outer space and the Antarctic must not be forgotten, for together with the law of the sea they share three fundamental principles: governance by treaty, limits on militarization and minimal involvement of private parties. The next chapter of this thesis will focus on mass cyber surveillance and transborder data access to show that they constitute violation of international human rights and the principle of territorial sovereignty. This emergent practice of states is one of the reasons why a hard law solution is urgently needed.

Its feasibility of coming to fruition will be the subject of discussion in Chapter 5. The next chapter will turn to the question of the lawfulness of mass untargeted cyber surveillance of the selected Five Eyes states and 'pulling off data' without consent by the Law Enforcement Agencies.

Chapter 4: 'The Right to Privacy in the Digital Age'

INTRODUCTION

The previous chapters of this thesis argued that far from being an unclaimed territory, or a global common, cyberspace is a domain susceptible to state regulation and therefore subject to exercise of sovereign powers. Chapter 3 discussed some of the methods of asserting territorial sovereignty in that environment, through various methods of censoring the information content and blocking of cross-border data flows. Another way, examined in this chapter, is states exercising their domestically mandated powers of surveillance to intercept and bulk collect data that flows through their territories and intercept them abroad. The chapter also examines states exercising of enforcement jurisdiction by directly accessing data stored on servers, or in a cloud located in a foreign territory for the purposes of criminal investigation. These practice is also known as transborder searches. This chapter with demonstrate that together with unrestricted and untargeted cyber surveillance, certain methods of transborder data searches breach individuals' right to privacy within and outside territories of the states involved in these activities. The chapter will also discuss that some forms of transborder data searches may also breach the international law principle of territorial sovereignty.

The chapter consists of five parts. Part one sets out its scope and will focus on the activities of the Five Eyes coalition of states, with an emphasis on the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ). This part will also discuss the legality of the Law Enforcement Agencies (LEAs) accessing data located outside their jurisdictions without recourse to the existing Mutual Legal Assistance processes (MLA) in the light of international law principles of sovereign territoriality, conducted *inter alia* on the basis of Article 32 of the Cyber Crime Convention 2001.[984] It will also consider the lawfulness of these practices in the light of the right to privacy of communication contained in the International Covenant of Civil and Political Rights 1966 (ICCPR)[985] (Article 17), the European Convention on Human Rights 1950 (ECHR)[986] (Article 8) and the Convention for

[984] Council of Europe, Convention on Cybercrime (Budapest Convention, Budapest 23 November 2001), ETS 185.
[985] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.
[986] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) 1950.

the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (Convention 108)[987] (Article 1). Part two shall address certain mass cyber surveillance programmes (such as PRISM, Tempora, Upstream and Boundless Informant) and the right to privacy of communications under the aforementioned key international and regional legal instruments, namely the ICCPR, the American Convention on Human Rights 1969 (ACHR)[988] (Article 11) and the European Convention on Human Rights. As cyber surveillance and transborder searches affect the right to privacy of those who are both within and outside the territories of the Five Eyes and state parties to the Budapest Convention, part three makes a case for extraterritorial application of human rights treaties in the extraterritorial context. Part four demonstrates that cyber surveillance and transborder searches constitute an interference with the right to privacy under international law, whilst part five examines limitations to that right and justifications for conducting surveillance, including on national security grounds. This part outlines the legal parameters and applies those to some of the cyber surveillance programmes mentioned previously. The chapter concludes by finding no grounds for justification of mass untargeted communications surveillance and consequently renders these activities unlawful under international human rights law.

PART I: GENERAL

1. Cyber Surveillance and Transborder Searches

The technology available to some states, in particular the US and the UK, makes it possible for the intelligence and law enforcement agencies of these and other countries to monitor, access, store and use an incredible amounts of data produced every day by millions of people world-wide for a variety of purposes from within the confines of their own territories. This chapter focuses on two such methods, that is surveillance of communications and unrestricted access to data located on servers in foreign countries and/or in 'a cloud' (also referred to as transborder data searches).

To analyse the legality of cyber surveillance operations, four programmes run predominantly by the NSA and GCHQ have been selected as the focal point for consideration in this chapter.

[987] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981, CETS No. 108.

[988] American Convention on Human Rights, (adopted at the Inter American Specialized Conference on Human Rights, San Jose, Costa Rica, 22 November 1969).

These are PRISM, Tempora, Boundless Informant and Upstream and form the focus of the analysis for the following reasons. First, they enable these intelligence agencies to intercept all communications as they transit through their territories and then share it with their Five Eyes partners. This gives an open access to conduct surveillance on the previously unheard of scale of everyone in almost every country in the world. Secondly, Tempora and PRISM are representative of the true technical capacity of GCHQ and the NSA. Thirdly, at least some of the surveillance programmes seem to operate pursuant to domestic legislation, which is important from the point of view of legal scrutiny and will be discussed later in this chapter. Finally, the ability to share the collected data among the Five Eyes intelligence agencies means that even if their national legal frameworks restrict direct surveillance of communications of their own nationals, they could have access to that data because it had been intercepted by the partner agencies. This practice has been termed 'collusion for circumvention'.[989]

This second method known as transborder data searches is defined as 'unilateral access [to] computer data stored in another party without seeking mutual assistance'[990], pursuant to criminal investigations, including on the basis of the Cyber Crime Convention 2001.[991] It will be shown that both these methods pose a serious threat to the right of privacy of communications and as discussed in the next, may also in some circumstances undermine the principles of territorial sovereignty under international law.

a. Transborder Searches as Breach of Territorial Sovereignty

As discussed in Chapter 2 of this thesis, territorial sovereignty is an exclusive right of a state to exercise its powers within the boundaries of its territory.[992] The concept of jurisdiction is closely related to that of territorial sovereignty, according to which, a state may not perform any government functions in the territory of another state without the latter's consent.[993] It follows that in exercising of enforcement jurisdiction for the purposes of criminal justice, any investigatory measures taken outside the domestic jurisdiction to obtain extraterritorially

[989] Parliamentary Assembly of the Council of Europe, 'Mass Surveillance. Report' Doc 1374 (21 April 2015) < http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21694&lang=en>.
[990] Council of Europe Cybercrime Convention Committee (T-CY) 'T-CY Guidance Note 3 Transborder Access to Data (Article 32)' (5 November 2013),< http://coe.int/TCY>, paragraph 3.2, p. 6.
[991] Convention on Cybercrime 2001, supra note 1.
[992] *Island of Palmas* case (1928) 2 RIAA 829.
[993] ibid.

located evidence must be in compliance with international law obligations to seek consent of the state concerned and be supported by domestic legislation and procedures.[994] Such consent may be based for example on bi-, or multilateral agreements, or when this right derives from international customary law. However, if there is no positive rule, a well established principle declared by the Permanent Court of International Justice (PCIJ) in *The Case of the Lotus*[995] (*Lotus Case*) provides that, states have the right to do whatever is not prohibited by international law.

A number of international and regional cybercrime instruments contain cooperation provisions and either set out broad, general obligations on states to cooperate[996] and/or provide for particular cooperation mechanisms, including extradition and mutual legal assistance (MLA).[997] By far the most widely used method of cooperation in cybercrime investigations is the latter process. MLA are the classical treaty-based mechanisms allowing for foreign law enforcement cooperation in ongoing criminal investigations, while respecting the jurisdiction and national sovereignty. As legally binding tools, the MLA provide the rules, through which third country authorities can lawfully issue requests for assistance in relation to gathering evidence from foreign jurisdictions.[998] Yet, in the context of obtaining/securing digital

---

[994] Michael Evans, *International Law* (Oxford University Press 2010), p. 331.
[995] *The Case of the S.S. Lotus*, Fr. v Turk, 1927 PCIJ (Ser. A) No. 10.
[996] The United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime', (February 2013) < https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Comprehensive%20Study%20on%20Cybercrime.pdf>. The study lists for example the Commonwealth of Independent States Agreement (September 1995), art. 5; Convention on Cybercrime, supra note 1, art. 23; The Agreement Between the Governments of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security (16 June 2009), art 3-5; African Union Convention on Cyber Security and Personal Data Protection 2014 (EX.CL/846 XXV), art 28(2).
[997] ibid. These include Commonwealth of Independent States Agreement, art 6; Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (25 October 2007) CETS No. 201, art 25, 17; Convention on Cybercrime, supra note 1, art. 25, 27 and the Arab Convention on Combating Information Technology Offences, art. 32, 34.

[998] 'Cooperative Study on Cybercrime', supra note 13, p. 201. The global survey conducted in 2013 reported that 'the use of formal cooperation mechanisms in transnational cybercrime cases is predominant over other forms of cooperation […] over 70 per cent of law enforcement authorities reported that formal mutual legal assistance was most often used to obtain a range of evidence types from other jurisdictions. Less-used mechanisms were reported to include informal police cooperation, direct contact with a service provider, and the use of 24/7 contact points'.

evidence, the MLA methods have been criticised for being inefficient and ineffective. This is mainly because of a long processing time of requests (often taking a year), very short time of data availability and the fact that states may simply not answer a request to cooperate. The Cybercrime Committee's detailed assessment of the functioning of the MLA based on replies from 36 state parties to the Cybercrime Convention and three observer states attested to this reality stating that:

> [t]he MLA process is considered insufficient in general and with respect to the obtaining electronic evidence in particular. Response times to requests of six to twenty-four months appears to be the norm. Many requests and thus investigations are abandoned. This adversely effects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.[999]

As a result of the insufficiency of the MLA mechanisms, many LEAs increasingly abandon the formal channels in favour of informal access. Given the apparent scale of the problem, the question that needs to be addressed is whether the current trend of conducting transborder searches outside the MLA is lawful under international law and whether these searches comply with human rights obligations. The first question will be considered in this part of the chapter, whilst the second in part three. It must be noted at the outset that not all transborder searches are illegal. Therefore, a distinction has to be made between two methods of obtaining evidence, namely those relating to generally accessible data in a server, or in 'a cloud' of a foreign country (transborder searches of open source data) and those that are not freely available, for example when only accessed via a password, also know as protected data (transborder searches of protected data). Each of this methods will be addressed below.

[999] Cybercrime Convention Committee, T-CY, 'T-CY Assessment Report. The Mutual Legal Assistance Provisions of the Budapest Convention on Cyber Crime Adopted by the T-CY of its 12th Plenary' (2-3 December 2014), <https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf>, p. 14.

i. Transborder Search of Open Source Data

This category of data is comprised of all data, which are not subject to any special pre-conditions and can be accessed by everyone, including LEAs of a foreign country. The Cybercrime Convention represents the first agreement in international law regarding the question of transborder search generally and in the context of open source data in particular. Article 32 of the Convention 'Transborder Access to Stored Computer Data with Consent or Where Publically Available' provides:

> [a] Party may, without the authorisation of another Party:
>
> a. access publically available (open source) stored computer data, regardless of where the data is located geographically; or
> b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.[1000]

Therefore, the transborder search of an open source data is not only explicitly permitted by Article 32(a), but appears to be widely practiced without creating controversy and objection by states. That being the case, the T-CY acknowledged that 'Article 32 is the most relevant provision with regard to unilateral transborder access to data. Transborder access to publically available data (Article 32(a)) may be considered accepted international practice and part of international customary law even beyond the Parties to the Budapest Convention.'[1001] Article 32(a) simply codifies this existing practice and it could be concluded that this search method is permissible under international law, as long as the access it to the generally available data.

[1000] Convention on Cybercrime, supra note 1, art 32.
[1001] Cybercrime Convention Committee (T-CY), 'Report of the Transborder Group Adopted by the T-CY. Transborder Access and Jurisdiction: What are the Options?' (6 December 2012), para 293, p. 56. <http:/www.coe.int/TCY>.

ii. Transborder Search of Protected Data

The type of data that the LEAs are most interested in from the point of view of criminal investigation are rarely freely available online. The current practice of the LEAs of obtaining such data includes two models. The first is accessing data on computers of other states pursuant to Article 32(b) (transborder access with consent), whilst the second goes beyond the methods envisaged by the Budapest Convention[1002] and may involve directly approaching internet service providers in foreign countries by way of court orders. Both of these methods are controversial and, as will be shown below, are highly likely to be in breach of the principle of territorial sovereignty and and human rights laws.

- Transborder Searches of Protected Data with Consent

According to Article 32(b) the precondition for direct access by the LEA of a foreign country to data stored in another state is to obtain the 'lawful and voluntary consent of the person who has the lawful authority to disclose the data'. Viewed from the perspective of practice in the field of international agreements and treaties in the context of law enforcement[1003] and

[1002] ibid. According to paragraph 9 at p. 5 'current practice regarding direct law enforcement access to data as well as access via [i]nternet service providers and other private sector entities […] illustrate that law enforcement authorities (LEA) of many states access data stored on computers in other [s]tates in order to secure electronic evidence. Such practices frequently go beyond the limited possibilities foreseen in Article 32b (transborder access with consent) and the Budapest Convention in general'.

[1003] for example, European Union Council Framework Decision 2008/977/JHA (27 November 2008) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, art 11 'Processing of personal data received from or made available by other Member States' provides that:

> [p]ersonal data received from or made available by the competent authority of another Member State may, in accordance with the requirements of Article 32(b), be further processed only for the following purposes other than those for which they were transmitted or made available:
>
> (a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available;
>
> (b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
>
> (c) the prevention of an immediate and serious threat to public security; or

according to the principle of national sovereignty this means obtaining such consent by way of an authorisation of an independent court, or judicial authority. However, neither the Budapest Convention, nor its Explanatory Report[1004] explicitly provide that the appropriate consent must come from such a body, nor do they define who is the person with the authority to disclose the data. The only indication in the Explanatory Report is to the service providers as such authority.[1005] This seems to be in conflict with, *inter alia*, the EU data protection laws, in particular Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive (DPD)). On 25 May 2018 the DPP will be replaced by the General Data Protection Regulation. (GDPR).[1006] By Articles 25 and 26 of the DPD, consent can only be given by data subjects[1007] and therefore private service providers

---

> (d) *any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law* (emphasis added)

The competent authorities may also further process the trans mitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as, for example, making the data anonymous.'

[1004]The Council of Europe Explanatory Report to the Convention on Cybercrime, (23 November 2001), ETS 185.

[1005] ibid, paragraph 294, p. 53:

> Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is 'lawfully authorised' to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

[1006] General Data Protection Regulation (GDPR) (EU) 2016/679. The GDPR will be directly applicable in all EU Member States without the need for implementing national legislation.

[1007] Directive 95/46/EC art 26:

1. [b]y way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on

cannot lawfully disclose them. Article 29 Working Party commented on this point in the following terms:

> [a]ccording to [the] Directive 95/46, consent can only be given by data subjects. Therefore, companies acting as data controllers usually do not have the 'lawful authority to disclose the data', which they possess […] They can normally only disclose the data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required. Data controllers cannot lawfully provide access or disclose the data to a foreign law enforcement authorities that operate under different legal and procedural framework from both a data protection and a criminal procedural point of view.[1008]

Frequently, LEAs cooperate with service providers, or other private sector entities to obtain access to data stored abroad.[1009] Reportedly, in some European states, a number of US-based service provides with branch offices in Europe have made voluntary arrangement ('criminal compliance programmes') between their European offices and the LEA of specific European governments, to disclose data under certain conditions and without requiring these European LEAs to go through a mutual legal assistance procedure via the US Department of Justice.[1010]

---

condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer;'

[1008] Council of Europe Article 29 Data Protection Working Party, 'Article 29 Working Party's Comments on the Issue of Direct Access to Third Countries' Law Enforcement Authorities to Data Stored in Other Jurisdiction, as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime' (5 December 2013) (Ares.2013) 3645289-05/12/2013, p.3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf>.

[1009] Cybercrime Convention Committee (T-CY), 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY' Report Prepared by the Ad-hoc Subgroup on Tranborder Access and Jurisdiction Adopted by the 12th Plenary of the T-CY (2-3 December 2014), p.44 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf>.

[1010] ibid. The conditions for voluntary compliance with requests may typically include:

Given the loophole created by the ambiguous meaning of 'lawful authority' and the possibility for accessing data through such methods as 'criminal compliance programmes', a provisional conclusion can be reached that transborder searches with consent pursuant to Article 32(b) are likely to violate the international law principle of territoriality, when LEAs carry out investigations in foreign jurisdictions without seeking prior approval of appropriate state organs. This is because, as discussed in Chapter 1 of this thesis, states cannot exercise unauthorised extraterritorial enforcement jurisdiction. It is worth reiterating that the the International Group of Experts responsible for the drafting of the *Tallinn Manual 2.0* agreed in Rule 11 that:

> [a] [s]tate may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects and cyber activities on the basis of:
>
> (a) a specific allocation of authority under international law; or
>
> (b) valid consent by a foreign government to exercise jurisdiction on its territory.[1011]

The comment to Rule 11 explains that 'the exercise of enforcement jurisdiction on another [s]tate's territory constitutes a violation of that [s]tate's sovereignty (Rule 4) except when international law provides a specific allocation of authority to exercise enforcement jurisdiction extraterritorially or when the [s]tate in which it is to be exercised consents'. [1012] The commentary states that 'the consent may be granted on an *ad hoc* basis or by means of a treaty'. [1013] The International Group of Experts agreed that a state's law enforcement authorities may not hack into servers [i.e. modify or alter computer software and/or hardware to

- the request would need to be lawful and come from a competent authority that has jurisdiction over the case being investigated, based on clear legal framework to investigate cyber crime;
- the data requested may need to be related to the territory of the requesting LEA (such as IP addresses, the country top-level domain of a webmail account);
- the conduct investigated would also constitute an offence in the USA;
- only data owned and controlled by the providers-such as traffic data and subscriber information- would be disclosed but not consent generated by users;
- the criminal justice system of the state is trusted to respect international human rights and rule of law standards, including the protection of privacy.

[1011] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) Rule 11, p. 66.
[1012] ibid, para 1. pp. 66-67.
[1013] ibid, para 7, p. 68.

accomplish a goal that is outside of the creator's original objective] in another state to extract evidence or introduce so-called white worms to disinfect bots [i.e. a self-replicating malware] there that are being used for criminal purposes without the territorial state's agreement.[1014] The International Group of Experts also commented that sometimes consent to enforcement jurisdiction may be grated by means of a treaty, as is the case with Article 32(b) of the Cybercrime Convention.[1015] The Group observed that 'in this case, [s]tates that are Parties to the Convention have consented in advance to the acquisition of the computer data by the process set forth therein. Thus, *lit.* (b) [of Rule 11] is satisfied.'[1016] This is rather surprising bearing in mind the controversy surrounding Article 32(b) and the notion of consent, in particular in relation to who is lawfully authorised to give such consent. As noted above, both the EU data protection laws and Article 29 Working Party are adamant that consent can only be given by data subjects and not by the companies acting as data controllers. However, evidence suggests that the decisions regarding the disclosure of personal data and the assessment of their probative value for the purposes of criminal investigations appear to be 'outsourced' to data controllers. This does not comply with the requirement for appropriate judicial authorisation and verification of such requests. Article 29 Working Party was very specific on this issue- a private sector entity functioning as data controller would not be able to disclose data voluntarily, but only upon presentation of a judicial order.[1017]

The Russian Federation, has been particularly vocal on the issue of violation of territorial sovereignty through actions on the basis of Article 32(b), which was the reason for that country refusing to join the Budapest Convention.[1018] A representative of the Ministry of Foreign Affairs speaking at the India Conference on Cyber Security and Cyber Governance in 2013 was emphatic on the Russian Federation's stance regarding the Budapest Convention, stating that Article 32(b) in particular contradicts and violates Council of Europe Convention 108 and national laws of many states, including Russia's.[1019] This is because Article 32(b) access-

[1014] ibid.
[1015] ibid, para 9, p. 68.
[1016] ibid.
[1017] T-CY Report, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY', supra note 26, p. 6.
[1018] Boris Vasiliev, Office of the Special Coordinator of the Ministry of Foreign Affairs, 'Sovereignty, International Cooperation and Cyber Security', CYFY 2013 Conference Transcript < http://cyfy.org/speaker/boris-vasiliev/>.
[1019] ibid.

> […] takes place without any notification to the competent authorities of the state and the territory on which the source of information is. This creates conditions for illegal entry into the information space of the other countries and so [..] violates the [rights] of states that are in it. Article 32(b) also creates a fertile ground for violation of fundamental rights and freedoms, in particular right to privacy'.[1020]

The Cybercrime Committee did not go so far as to declare Article 32(b) to be illegal. However it did described the provision as an exception to the principle of territoriality, because it permits 'unilateral transborder access without the need for mutual assistance under limited circumstances'.[1021] The T-CY recognized that:

> [p]ractice, procedures as well as conditions and safeguards vary considerably between different Parties. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or 'in the cloud' as well as national sovereignty persist and need to be addressed'.[1022]

However, the T-CY did not agree with the view of the Article 29 Working Party that service providers can never voluntarily disclose personal data, as this would discount emergency situations, controller's becoming aware of an offence, or ISP being attacked.[1023] The 2012 T-CY report showed that the legislation and practices of a number of states go beyond the provisions of Article 32(b) in terms of direct transborder access to data, or access via private sector entities. [1024] The disparity in practice among states in situations where LEAs primarily access stored computer data directly was illustrated by examination of domestic legal frameworks of a small sample of states.[1025] What became apparent from this study is that most

---

[1020] ibid.
[1021] Council of Europe Cybercrime Convention Committee, 'T-CY Guidance Note 3. Trasborder Access to Data (Article 32)' (5 November 2013), p.3 <https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf>.
[1022] ibid.
[1023] ibid.
[1024] T-CY Report, 'Transborder Access and Jurisdiction: What are the Options?', supra note 18, p. 11.
[1025] ibid, pp. 32-44. These are Belgium, the Netherlands, Norway, Portugal, Romania, Serbia and US.

countries do not have very clear rules on transborder access. What rules there are, vary considerably in scope. At one end of the spectrum, some domestic laws allow access to data stored on remote systems. In Serbia for example, transborder access through lawfully obtained password and with consent is lawful on the presumption that data would temporarily, or permanently be stored within the territorial jurisdiction of the Serbian authorities.[1026] The Portuguese Law on Cybercrime[1027] allows for an 'extension' of a lawfully authorised computer search obtained during an investigation to apply to remote systems located within and outside Portuguese borders. This means that it is lawful for a Portuguese law enforcement officer to access data physically stored in a remote system in a foreign state if a proper order was obtained from a prosecutor, or a judge.[1028] Conversely, other states, such as Norway, have only general provisions relating to the LEA access to evidence, including electronic evidence.[1029] There are few specific rules, which state that LEAs may obtain customer information directly from the service provider without a court order.[1030] Nothing is said about the possibility of conducting the searches transborder. At the other end of the spectrum is the Dutch Cyber Crime Act, which in its explanatory note explicitly stipulates that searches on systems outside the Netherlands are not allowed and that this can only be conducted through methods of public international law, which in practice means that LEAs should resort to MLA.[1031]

In addition to these disparate state approaches, the T-CY recognized that there is a practical need for law enforcement to have timely access to data stored extraterritorially, thus attempting to relax the remaining constraints on the foreign LEA. To that end, the T-CY proposed an Additional Protocol supplementary to the Cyber Crime Convention putting forward five new draft elements:

1. transborder access with consent without the limitation to data stored 'in another Party'
2. transborder access without consent but with lawfully obtained credentials
3. transborder access without consent in good faith or in exigent or other circumstances
4. extending a search without the limitation in its territory in Article 19.3

[1026] ibid, p. 42.
[1027] Portuguese Law on Cybercrime No. 109/2009.
[1028] supra note 18, p. 38.
[1029] The Norwegian Criminal Procedures Act 1981; the Dutch Code of Penal Procedures 2006 was drafted to conform to the Budapest Convention.
[1030] Norwegian Electronic Communications Act ss. 2-9.
[1031] T-CY 2012 Report, supra note 18, p. 34.

5. the power of disposal as connecting factor.[1032]

These proposals were however swiftly rejected by a number of EU bodies, including the Article 29 Working Party and the representatives of national and European data protection authorities. The conclusion reached was that all five draft elements may expand extraterritorial jurisdiction, breach the key principles of data protection, some ignore national jurisdiction and sovereignty (draft element 1 and 4), are too vague (e.g. the legal meaning of 'lawfully obtained credentials' in draft element 2), provide for no guarantee of upholding the concepts of necessity and proportionality (e.g. 'good faith' and 'exigent or other circumstances' in draft element 3) and breach the principle of territoriality (draft element 4 and 5).[1033] The attempt at amending Article 32(b) has thus far largely failed, which led the T-CY to conclude that the 'negotiations of a Protocol on transborder access to data would not be feasible'.[1034]

In the light of the above findings, it could be said that under international law, transborder searches with consent of service provider undertaken under Article 32(b) by the LEAs in principle breach territorial sovereignty and therefore are not lawful under international law. This, at least for the time being, creates a lacuna in the law, as there seems to be lack of a positive rule prohibiting these searches. The question is therefore whether such access could be allowed on the basis of the principle set out in the *Lotus* case.[1035] Accordingly, international law leaves to states 'a wide measure of discretion which is limited only in certain cases by prohibitive rules [and in the absence of such rules] every State remains free to adopt the principles which it regards as best and most suitable'.[1036] The upshot of the *Lotus* approach is that if no limits are established, a state remains free to act as it wishes. This, it is submitted, cannot apply in the context of Article 32(b) searches for two reasons. First, the T-CY recognized that Article 32(b) creates a situation that needs to be further addressed. In particular, its 2014 Report acknowledged the need for clearer and more transparent regulation of transborder access.[1037] Therefore, despite the setbacks described above to the Additional

[1032] Cybercrime Convention Committee (T-CY), '(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (9 April 2013) <https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)14transb_elements_protocol_V2.pdf.>.
[1033] Article 29 Working Party Comments, supra note 25, p. 7.
[1034] T-CY 2014 Report, supra note 16, pp 12-13.
[1035] *The Lotus*, supra note 12.
[1036] ibid, paragraphs 16-17.
[1037] T-CY 2014 Report, supra note 16.

Protocol, the work relating to the establishing of the parameters to the operation of Article 32(b) is ongoing. Secondly, some states, most notably the Russian Federation, object completely to Article 32(b) and if more states voice similar views, this could eventually become a positive rule casting doubt on the legality of Article 32(b) access in its current form. Until such time, as an international consensus is reached regarding the parameters of the lawful searches with consent, foreign LEAs must always seek the necessary approvals of state authorities to avoid both breaches of international law and procedural difficulties relating to the probative value of evidence obtained illegally.

- Transborder Searches of Protected Data without Consent

There also appears to be an emerging practice on the part of some LEAs outside the provisions of Article 32 Budapest Convention, which involves the retrieval of protected data without the consent, or authorisation of the affected country's authorities and/or the data controller, which may violate the principle of territorial sovereignty. Two examples of this practice are the recent cases of *Re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation* [1038] (*Microsoft Ireland*) and the so-called *FBI-Apple Encryption Dispute*.[1039]

The *Microsoft Ireland* case concerned an order made by the US Department of Defence by way of a search warrant under the US Stored Communications Act 1986[1040] (SCA) that sought to compel Microsoft to disclose the content of emails in connection with criminal investigation concerning drug trafficking. The emails were stored by Microsoft's wholly owned subsidiary in a data centre in Dublin, Republic of Ireland. Microsoft refused to comply and disclose the contents of the account on the basis that the US court could not enforce such an order as the data were stored extraterritorially and were not owned by Microsoft, but rather belonged to the email user. Therefore, the Company contended, the order represented a conflict of laws and an impermissible exercise of extraterritorial authority. Notwithstanding, the order was granted in the US Magistrate court by Judge Francis, who decided that the warrant obliged

[1038] *In the Matter of a Warrant to Search a Certain E-Mail Account: Controlled and Maintain by Microsoft Corporation,* 15 F. Supp. 3d 466 (S.D.N.Y. 2014).
[1039] *In the Matter of the Search Warrant of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus* IS300, California Licence Plate 35KGD203.
[1040] U.S.C § 2703. The 1989 Stored Communications Act allows the government to obtain a warrant that compels an Internet Service Provider to disclose customer information, emails and other data on showing a probable cause.

Microsoft to produce the requested information irrespective of its location.[1041] The reason for granting the order was that the government's request was not based on a conventional warrant, but rather on a hybrid- part subpoena and part warrant. The Judge reasoned that the SCA warrant acts as a subpoena and therefore does not require the government to conduct a physical search and seizure. In cases of a subpoena, the location of the requested documents is irrelevant, what matters is that the party on whom such an order was served has control over the information sought. Therefore requiring an Internet Service Provider, such as Microsoft, to produce its records held abroad 'does not implicate principles of extraterritoriality',[1042] but is merely an extension of the court's power toward a party over whom it has personal jurisdiction. As the data is 'within Microsoft's control', the request would not be an extraterritorial application of US law. The Judge also stressed that clearly US Congress had intended the Stored Communications Act to compel electronic communications providers to disclose any information under their control, including information stored abroad,[1043] as such orders could not have been meant to apply only to data stored in the United States.[1044] Had that been the original intention of the Congress, criminals could simply provide false information and have their data sored overseas thereby avoiding the reach of US law enforcement altogether.[1045] Furthermore, if SCA warrants did not allow for the production of data stored abroad, the government would have to resort to the US-Ireland Mutual Legal Assistance Treaty (MLAT),[1046] which procedures the Judge noted, are lengthy, cumbersome and unreliable.[1047] Based on this reasoning, an order was entered against Microsoft for the continuing refusal to comply with the subpoena and the Company appealed to the District Court for the Southern District of New York in 2014, but with no success as the decision of the Magistrate was affirmed. Another appeal followed, this time to the US Court of Appeal for the Second Circuit and an Amicus Brief was filed by Digital Rights Ireland, Liberty and Open Rights Group in

[1041] supra, note 55.
[1042] ibid, p 472. The Judge stated that 'it has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information', citing *In re Marc Rich & Co. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983)).
[1043] ibid.
[1044] ibid, pp. 474-5.
[1045] ibid, p. 474.
[1046] U.S.-Ireland Treaty on Mutual Legal Assistance January 18 2001, T.I.A.S. No. 13137 (2001).
[1047] supra, note 55, pp. 474-75.

support of Microsoft.[1048] The Brief criticised the United States for ignoring the Mutual Assistance Treaty, which provides precisely for this type of situations, namely to balance the interests of the United States in law enforcement matters with those of Ireland in data privacy protection.[1049] The submission emphasised that under Irish law the data content of the email account maintained in Ireland belongs to the author and the owner of the account and may not be exported from Ireland by a Microsoft subsidiary.[1050] Therefore, the decision of the US District Court requiring Microsoft to do that notwithstanding Irish law was wrong, as it disregarded the MLAT, i.e. treated it as non-obligatory.[1051] Consequently, if the District Court's decision were to be allowed to stand, MLAT simply would not have to be adhered to, in the absence of some further pronouncement from the US Congress to the contrary.[1052] As the aim of mutual assistance mechanism is to facilitate inter-state cooperation with a view of respecting territorial sovereignty of states, by- passing these obligation would not only constitute a breach of international law but also remove the balancing of states' interests from the authorities mandated to do so under the MLATs and simply shift it to the IPSs. In 2016 the Court of Appeal agreed that Microsoft did not have to handover the data.[1053] It was held that the US Stored Communications Act does not authorise US courts to issue and enforce against US based service providers warrants for seizure of customers' email contents that are stored exclusively on foreign servers. The Second Circuit Court of Appeal considered that the proper channels for obtaining data pursuant to conducting criminal investigations abroad remain through the Mutual Legal Assistance Treaty, despite the US government's plea that this is too cumbersome. The decision can therefore be seen as a victory for the protection of privacy of many Europeans, bearing in mind that as much as 90% of their personal data is processed by US services and 82% of Facebook's European data passes through Ireland.[1054] Admittedly,

[1048] Brief of Amici Curiae Digital Rights Ireland Limited, Liberty and the Open Rights Group in Support of the Appellant Microsoft Corporation (15 December 2014) 14-2985-cv.
[1049] ibid, p. 3.
[1050] ibid, p. 4.
[1051] ibid, p. 7.
[1052] ibid.
[1053] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* The US Court of Appeals for the Second Circuit (14 July 2016) Docket No. 14-2985 < http://pdfserver.amlaw.com/nlj/microsoft_ca2_20160714.pdf>.
[1054] The Register, 'Microsoft Wins Landmark Irish Data Slurp Warrant Case Against the US' (14 July 2016) <https://www.theregister.co.uk/2016/07/14/microsoft_wins_landmark_irish_warrant_case_against_usa/>.

the law enforcement needs are of legitimate state interest. However, had the US won the case on appeal, the result would have meant that any data centre, whose headquarters are located in the US, could be ordered to surrender their customers' information to any US LEAs on the latter showing a probable cause in a US court. The Second Circuit Court of Appeal made it clear that:

> [the US] Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorise a US court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland.[1055]

This is undoubtedly a landmark decision. In the words of Microsoft's president and chief legal advisor Brad Smith, 'it ensures that people's privacy rights are protected by the laws of their own countries, it helps ensure that the legal protection of the physical world apply in the digital domain and it paves the way for better solutions to address both privacy and law enforcement needs.'[1056] Furthermore, it brought into a sharp focus the need for legal solutions on domestic and international level that would address both the protection of privacy and the needs of law enforcement.

Another example of an attempt by a LEA to exercise its enforcement jurisdiction in contravention of territorial sovereignty relates to the cases concerning the encryption dispute between the US Federal Bureau of Investigation (FBI) and Apple. Following Edward Snowden disclosures in 2013 some technology companies began integrating encryption of digital communications into their products and enabling this as a default setting, for example Apple iOS 8 and Google Android.[1057] This creates a particular problem for law enforcement, who may obtain a court order to search and seize nearly anything, except for the encrypted data which will not be accessible without a pass code. This is the basis of the dispute in the *In a*

[1055] supra note 70.
[1056] supra note 71.
[1057] ibid.

Matter of the Search Warrant of an Apple iPhone[1058] (*The San Bernardino* case*)*, where the FBI applied for a court order to compel that Company to gain access to a password protected iPhone recovered from a suspected terrorist in connection with San Bernardino attacks on 15 December 2015. The case is one of the highest profile clashes in the debate regarding encryption and data privacy between the US government and a technology company. It was dropped on the first day of its court hearing, as the FBI, it is claimed, was assisted by a third party to gain access to the phone's data. It nevertheless is the basis of a continued debate between technology firms and law enforcement authorities. The latter claim that the use of encryption tools by such companies as Apple hinders criminal investigations and effective prevention of terrorist attacks.[1059] The dispute also brought to the public attention a number of similar orders served on Apple under the All Writs Act 1789. One of these orders seeks to force the Company to design a new operating system that would allow to disable iPhone's certain security features.[1060] Apple refused, thus being subject of court proceedings. Its legal arguments are based on an unreasonable burden that the nature of the assistance would cause the Company, the fact that the order itself is based on an antiquated legislation and that the end result of complying would fundamentally undermine the trust in the security system of Apple products, at the same time making iPhone derived data irresistible to criminals, terrorists and hackers. The case is not argued on the basis of possible violations of international law. Nevertheless, one conclusion from this perspective is that if Apple were to be compelled by the US courts to introduce an operating system, whereby the encrypted data could be easily accessed by any LEA, this would effectively open the data of anybody in the world to their scrutiny, thus discarding the need for the official MLA mechanisms. The result could be far reaching- any LEA in a given state would be able to exercise its enforcement jurisdiction in another's territory without seeking official consent. The successful outcome for the FBI could also have very serious global ramifications for human rights. The the UN High Commissioner for Human Rights, Zeid Ra'ad Al Hussein speaking out in support of Apple, described the order made by the US authorities as tantamount to 'unlocking a Pandora's Box that could have

[1058] supra note 56.
[1059] *CNBC,* 'Apple vs FBI: All You Need to Know' (29 March 2016) < http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html >.
[1060] Lev Grossman, 'Inside Apple CEO Tim Cook's Fight with the FBI' (17 March 2017) *Time,* <http://time.com/4262480/tim-cook-apple-fbi-2/>.

extremely damaging implications for the human rights of many millions of people, including their physical and financial security'.[1061]

Cyberspace has facilitated an avalanche of personal data and made it be available for access and exploitation by both the intelligence and the law enforcement agencies. The functions of these agencies have become blurred as far as fighting cyber crime and safeguarding national security are concerned. As a consequence, the tasks that they perform are no longer circumscribed by easily discernible legal boundaries. The Snowden documents revealed that LEAs routinely access on massive scale data stored abroad, which inevitably breaches the principle of territorial sovereignty. In addition, there is a push on the part of some governments to compel data controllers in third countries to surrender the information held in their data centres on production of court orders or through undermining encryption standards. All these developments set dangerous global precedents and raise concerns with regard to privacy protection, which will form the basis of the discussion in the next part of this chapter.

PART II: THE RIGHT OF PRIVACY OF COMMUNICATIONS

1. The Right to Privacy

The legal right to privacy is said to be 'amongst the essential ingredients of modern human rights law'.[1062] Its general aim is to set limits of how far society and the state can intrude into a person's affairs.[1063] The next part of this chapter will focus on the right to privacy of communications under the International Covenant of Civil and Political Rights 1996 (ICCPR),

---

[1061] United Nations Human Rights, Office of the High Commissioner, 'Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid' (4 March 2016) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E>.

[1062] Javaid Rehman, *International Human Rights Law* (Pearson Education Limited, 2010), p. 106.

[1063] Simon Davis, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (Pan Books, 1997), p. 23. To that end, privacy could be divided into four facets, that is (a) information privacy, which concerns the rules governing the collection and handling of personal data, such as credit and medical information; (b) bodily privacy, which relates to the protection of people's physical selves against invasive procedures, such as drug testing; (c) privacy of communications, which covers the security and privacy of mail, telephone and electronic communications; and (d) territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments, such as the workplace or public space.

the European Convention of Human Rights 1950 (ECHR) and the American Convention of Human Rights 1969 (ACHR).

A. International Law and The Right to Privacy of Communications

A number of legal frameworks at international level set out that all individuals have the right to respect for their private life, home and correspondence. The 1948 Universal Declaration of Human Rights (UDHR) expressly refers to this right in Article 12.[1064] The Declaration was only intended as a proclamation of basic rights and fundamental freedoms and its purpose was described as 'setting a common standard of achievement for all peoples in all nations'.[1065] Therefore it is a non legally binding instrument. However, an explicit and binding obligation of protection for the right to privacy on all member-states is contained in the International Covenant on Civil and Political Rights 1996 (ICCPR), Article 17.[1066]

The UN Human Rights Committee's (HRC), a body of independent experts that monitors the implementation of the ICCPR by its state parties, is tasked with providing a guide to the Covenant's interpretation. This the Committee does through issuing non-country specific and non-legally binding general comments, with the purpose to, *inter alia*, promote the effective implementation of the Covenant, clarify its requirements and stimulate the activities of state parties as well as international organizations in the promotion and protection of human rights.[1067] The HRC's analysis of the content of the right to privacy contained in General Comment 16 asserts that Article 17(1) not only prohibits states from invading a person's

---

[1064] Universal Declaration of Human Rights, adopted 10 December 1948 UNGA Res 217 A(III), art. 12 states that:

> [n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.
> Everyone has the right to the protection of the law against such interferences and attacks.

[1065] ibid.

[1066] ICCPR, supra note 2, art. 17 states that:

> 1. [n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> Everyone has the right to the protection of the law against such interference or attack.

[1067] Ghandi, *The Human Rights Committee and the Right of Individual Communication: Law and Practice* (Ashgate Publishing 1998) p. 25.

privacy, but also sets out positive obligations to take positive national measures to protect it,[1068] including adequate complaints systems, as well as remedies for privacy violations. The meaning of privacy for the purposes of Article 17 has not been defined in either the General Comment 16, nor the case law of the HRC.[1069] However, the Committee did recognize its infringement in the context of confidentiality and integrity of correspondence.[1070] Furthermore, the protection in law against interference with privacy of correspondence has explicitly been made in paragraph 8 of the General Comment 16, which states that:

> [c]ompliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interception of telephonic, telegraphic and other forms of communications, wire-tapping and recording of conversations should be prohibited.[1071]

The Committee's case law has interpreted the term 'correspondence' as comprising not only written letters, but also other forms of communication, such as telephonic, facsimile and e-mail. (*Angel Estrella v Uruguay)*.[1072] The HRC also commented on such matters as telephone tapping in its Concluding Observations on Poland,[1073] interception of postal articles, or

---

[1068] UN HRC, 'CCPR General Comment No.16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence and the Protection of Honour and Reputation' (8 April 1988) UN Doc. HRI/GEN/1/Rev.1, para 1:

> Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislation and other measures to give effect to the prohibition against such interferences and attacks as well at to the protection of his right.

[1069] Sarah Joseph and Mellissa Castan, *The International Covenant on Civil and Political Rights. Cases, Materials and Commentary* (Oxford University Press, 2014) p. 534.

[1070] General Comment No. 16, supra note 85.

[1071] ibid.

[1072] *Angel Estrella v Uruguay* (74/80). In that case a prisoner received 35 out of 100 censored letters and HRC found that he should be allowed under necessary supervision to correspond with his family and reputable friends without interference.

[1073] UN HRC, Concluding Observations on Poland (1999) UN Doc CCPR/C/79/Add.110. The HRC noted at paragraph 22 that:

telegrams in the Concluding Observations on Zimbabwe[1074] and wide powers of surveillance of electronic communications for the executive as a way of combating terrorism in its Concluding Observations on Sweden.[1075] In that case the HRC stated that:

> [t]he [s]tate party shall take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant and be consistent with obligations under article 17 of the Covenant. To that effect, the [s]tate party should guarantee that the processing and gathering of information be subject to review and supervision by an independent body with necessary guarantee of impartiality and effectiveness.[1076]

Thus, electronic surveillance falls within the meaning of the term 'correspondence' under Article 17 and may be compatible with that Article, if it is strictly controlled and overseen by independent, preferably judicial, bodies.[1077] General Comment No. 16 also addresses the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, which must be subject to appropriate state regulation and safeguards.[1078]

> [a]s regards telephone tapping, the Committee is concerned (a) that the Prosecutor (without judicial consent) may permit telephone tapping; and (b) that there is no independent monitoring of the use of the entire system of tapping telephones.

[1074] UN HRC, Concluding Observations on Zimbabwe (1998) UN Doc CCPR/C/79/Add.89. The HRC stated at paragraph 25 that:

> [t]he Committee notes with concern that the Postmaster-General is authorised to intercept any postal articles or telegrams on grounds of public security or the maintenance of law and to deliver these items to a specified State employee. The Committee recommends that steps be taken to ensure that interception be subject to strict judicial supervision and that the relevant laws be brought into compliance with the Covenant.

[1075] UN HRC, Concluding Observations on Sweden (2009) UN Doc CCPR/C/SWE/CO/6.

[1076] ibid, paragraph 18.

[1077] Joseph and Castan, supra note 86, p. 548.

[1078] General Comment No.16, supra note 85, para 10:

> [t]he gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public [authorities]

Article 17(1) ICCPR prohibits 'unlawful' and 'arbitrary' interference with privacy. General Comment 16 interpreted the term 'unlawful' to mean 'that no interference can take place except in cases envisaged by the law'.[1079] This means that interference with privacy is permissible, but only if is authorized by states and if it takes place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.[1080] The HRC has elaborated on the meaning of 'law' for the purposes of Article 19 ICCPR (freedom of opinion and expression) stating that "'law' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion".[1081] Furthermore, the HRC interpreted the term 'arbitrary interference' stating that:

> [t]he expression 'arbitrary interference' is also relevant to the protection of the right provided for in Article 17. In the Committee's view the expression 'arbitrary interference' can also extend to interference provided under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[1082]

It is of note that the concept of arbitrariness is generally understood to be wider than that of unlawfulness in international law. For example, in the context of loss or deprivation of nationality, a measure will be arbitrary if it does not comply with certain conditions, such as serving a legitimate purpose, being the least intrusive instrument to achieve the desired result and being proportional to the interest to be protected.[1083] Equally, for a measure not to be

---

> or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

[1079] ibid, paragraph 3.
[1080] ibid.

[1081] UN HRC, General Comment No. 34 on Freedoms of Opinion and Expression (Article 19 ICCPR) (21 July 2011), para 25, p. 6. < http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

[1082] General Comment No. 16, supra note 85, p.4.
[1083] UN HRC, 'Human Rights and Arbitrary Deprivation of Nationality. Report of the Secretary General' (19 December 2013) UN Doc A/HRC/25/28, p. 4.

arbitrary, adequate procedural standards must be in place, such as an effective administrative or judicial review, an opportunity to appeal the decision and provision of remedies.[1084]

There are a number of cases where the HRC found unlawful and arbitrary interference with privacy of correspondence, including the intrusion into private telephone communications (Concluding Observations on the Russian Federation),[1085] phone-tapping and legal privilege communications (Concluding Observations on Jamaica, [1086] *Cornelis van Hulst v Netherlands)*[1087] and censorship of prisoner's letters (*Pinkney v Canada).*[1088] These cases show that even if the interference conforms to the Covenant, it can only take place pursuant to the 'relevant legislation [authorizing the interference] [which] must specify in detail the precise circumstances in which such interference may be permitted,'[1089] whilst a decision to make use of such authorized interference must be made only by the authority designated under the law and on a case-by-case basis.[1090]

B. Regional Human Rights Systems and The Right to Privacy of Communications

a. The European Convention on Human Rights

At the European level, the main legal instrument, which aims to guarantee civil and political rights is the 1950 European Convention on Human Rights (ECHR)[1091] and its additional Protocols. The Convention sets out the right to privacy in Article 8.[1092] The European Court of Human Rights (ECtHR) adopted a wide approach to circumscribing the contours of the 'right

---

[1084] ibid, pp. 14-17.
[1085] UN HRC, Concluding Observations on the Russian Federation (1995) UN Doc. CCPR/C/79/Add.54.
[1086] UN HRC, Concluding Observations on Jamaica, (1997) UN Doc. CCPR/C/79/Add.83.
[1087] *Cornelis van Hulst v Netherlands* (9003/00).
[1088] *Pinkney v Canada* (27/78).
[1089] General Comment No. 16, supra note 85, para 8.
[1090] ibid.
[1091] ECHR, supra note 3, art 8.
[1092] ibid, art 8:

1. [e]veryone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

to private life'. Similarly to Article 17 ICCPR, Article 8(1) ECHR explicitly refers to the right to respect of correspondence as an autonomous interest (along with home and family), which has been interpreted as the right to uninterrupted and uncensored communications with others.[1093] In this regard, the jurisprudence of the ECtHR is in line with the HRC interpretation of the term 'correspondence' and covers all forms of communications, including telephone, facsimile and email.

The extent of the interference with the right to privacy in the context of states' secret surveillance operations has been subject of an extensive analysis of the ECtHR on a number of occasions in the past. A series of early cases dealing with the interception of telephone conversations applying various surveillance techniques by law enforcement agencies helped to develop consistent principles in relation to interference with the right protected by Article 8. The cases of *Klass and Others v Germany,*[1094] *Malone v United Kingdom,*[1095] *Halford v United Kingdom*[1096] and *Liberty v United Kingdom*[1097] established, *inter alia*, that wiretapping of telephone conversations constitutes an interference with the right to privacy and the use of covert surveillance technologies invariably engaged Article 8, as the notion of 'private life' and 'correspondence' extends to the interception of telephone communications and so-called 'metering' practices.[1098] The finding that the notion of 'correspondence' covers telephone

[1093] David Harris, Michael O'Boyle, Ed Bates, et al, *Law of the European Convention on Human Rights* (Oxford University Press 2009) p. 380.
[1094] *Klass and Others v Germany* (1978) 2 EHRR 214.
[1095] *Malone v United Kingdom* (1985) 7 EHRR 14.
[1096] *Halford v United Kingdom* (1997) 24 EHRR 523.
[1097] *Liberty & Others v United Kingdom* (2009) 48 EHRR 1. In that case, a number of civil liberties organizations complained that their telephone and electronic communication had been intercepted for seven years by the UK. Ministry of Defense pursuant to the Interception of Communications Act 1985. The Act allowed for no limitations on the type of communications that could be intercepted, granting virtually unrestricted rights to capture all external communications. Nor did the Act indicate with sufficient clarity the scope of this wide discretion, or the manner, in which it was to be exercised. In particular, there was an absence of publicly available procedures as to the selection, sharing, storing and destruction of the intercepted material. The applicants claimed that once captured, the data was then filtered using an electronic search engine. The search terms, devised by officials were used, but the only legal requirement was that the data could be searched, listened to, or read if it fell within very broad categories, such as detection of crime or prevention of terrorism. The ECtHR held that there were no statutory limitations on the type of information collected, or the way in which it could be used, shared or stored and therefore there was a violation of Article 8.
[1098] *Malone*, supra note 112. 'Metering' involved the use of a meter to register the number dialed on a particular telephone as well as the time and duration of each call. The ECtHR held that there had been an interference with Article 8, as the notion of 'private life' and 'correspondence' extended to interception of telephone communications and the metering practices.

conversations had been extended in *Halford v United Kingdom*[1099] to include the interception of office telephone calls. Subsequently, in *Liberty v United Kingdom*[1100] the ECtHR explicitly stated that e-mail, in addition to written, telephone and facsimile communications, are also included in the ambit of 'private life' and 'correspondence' within the meaning of Article 8 ECHR.

The Court's subsequent jurisprudence established that not only the direct interception, but also the collection and storage of personal information in relation to an individual's use of the telephone, email and internet amounts to interference with private life and correspondence. Thus, in *Copland v United Kingdom,*[1101] the ECtHR concluded that the collection and storage of personal information relating to the applicant's use of the telephone, email and internet without her knowledge amounted to an interference with her right to respect for private life and correspondence.[1102] Likewise, Article 8 rights were breached, when the Court found that storage of communications amounted to interference in the cases of *Leander v Sweden*[1103] and *Amann v Switzerland.*[1104] In *Leander,* the ECtHR held that 'both the storing and the release of [secret police-register information], coupled with a refusal to allow [the applicant] an opportunity to refute it, amounted to an interference with his right to respect for private life'.[1105] In *Amann* the ECtHR found that the interception and/or storage of a communication constitutes a violation and the 'subsequent use of the stored information has no bearing on that finding',[1106] nor did it matter 'whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way'.[1107]

The Court also found interference with Article 8 in a number of cases relating to the storage of electronic data on government databases. In *S. and Marper v the United Kingdom*[1108] the applicants' fingerprints, cellular and DNA samples were to be held indefinitely in a database, following criminal proceedings against them. The ECtHR held that Article 8 had been violated as the blanket and indiscriminate nature of the powers of retention of the fingerprints, cell

[1099] *Halford*, supra note 113.
[1100] *Liberty*, supra note 114.
[1101] *Copland v United Kingdom* (2007) 45 EHRR 858.
[1102] European Court of Human Rights, Factsheet-New Technologies (June 2015), <http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf>.
[1103] *Leander v Sweden* (1987) 9 EHRR 433.
[1104] *Amann v Switzerland* (2000) (App. No. 27798/95).
[1105] *Leander*, supra note 120, para 22.
[1106] *Amann*, supra note 121, para 69.
[1107] ibid, para. 70.
[1108] *S. and Marper v United Kingdom* (2009) 48 EHRR 1169.

samples and DNA profiles of persons suspected but not convicted of offences, failed to strike a fair balance between the competing private and public interests, as they were disproportionate to the aims achieved.[1109] A violation of Article 8 was also found in the case of *Shimovolos v Russia*,[1110] concerning the collection of information in the so-called 'surveillance database' of a human rights activist's movements by train or air within Russia. The Court observed that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order, which had never been published or otherwise made accessible to the public. Therefore, the domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store information on individual's private lives in the database. Nor did it set out in a form accessible to the public any indication of the minimum safeguards against abuse.[1111] The Court continued to find violation of Article 8 in similar fashion in such cases as *M.K v France*[1112] and *Brunet v France*.[1113] In the former, the ECtHR held that the retention of the data in question had amounted to disproportionate interference with his right to privacy. In the latter judgment, the Court considered that the French state had overstepped its discretion, as the retention could be regarded as a disproportionate breach of the applicant's right to privacy and was not necessary in a democratic society. Likewise, an infringement of Article 8 was found in *Robathin v Austria*,[1114] where the applicant's documents and electronic data were searched by the police following a criminal investigation. The interference related to the fact that the search concerned all of his electronic data rather than that relating solely to case under investigation. As there were no substantiating reasons given for such an all encompassing search, the Court held that the seizure and examination of all the data had gone beyond what was necessary to achieve the legitimate aim.

The recent judgments in *Roman Zakharov v Russia*[1115] and *Szabo and Vissy v Hungary*,[1116] decided by the ECtHR Grand Chamber in 2015 and 2016 respectively, consolidated the Court's previous case law in relation to secret surveillance. The case relates solely to Russia's domestic legal framework aimed at the state's nationals and in that sense

[1109] European Court of Human Rights, Factsheet-New Technologies, supra note 119, p. 1.
[1110] *Shimovolos v Russia* (App. No. 30194/09) 21 June 2011.
[1111] European Court of Human Rights, Factsheet-New Technologies, supra note 119, p. 2.
[1112] *M.K v France* (2013) (App. No 19522/09)
[1113] *Brunet v France* (2014) (App. No. 21010/10).
[1114] *Robathin v Austria* (2012) (App. No. 30457/06).
[1115] *Roman Zakharov v Russia* (2015) (App. No. 47143/06).
[1116] *Szabo and Vissy v Hungary* (2016) (App. No. 37138).

does not address extraterritorial surveillance, nor transborder searches of protected data. Nevertheless, it is now the leading authority on the approach the ECtHR takes when assessing such measures and therefore may be indicative of a stance that the Court may adopt to cases concerning blanket extraterritorial surveillance and searches. *Zakharov* concerned a system of secret interception of all mobile telephone communications in the interest of crime prevention and national security in Russia. The applicant complained that Russian network operators were required by law (Order No. 70) to install equipment enabling law enforcement agencies to carry out operational search activities, without prior judicial authorization.[1117] This permitted blanket interception and was unsuccessfully challenged by the complainant, Mr Zakharov at national level. He therefore brought the case before the ECtHR arguing three grounds, namely that these methods of surveillance infringed his Article 8 rights, that parts of the Russian laws were not accessible to the public[1118] and that there were not sufficient remedies available to him[1119] (Article 13 ECHR). The Ground Chamber of the ECtHR unanimously found that there was a violation of Article 8 ECHR. This was based on a number of systematic faults with the Russian laws, including the fact that the interception was exceedingly broad in scope, accessible to both the secret services and the police, whilst its enabling laws did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. The case is of importance for a number of reasons.

First, the Grand Chamber considered the question of admissibility of Mr Zakharov's case. This preliminary stage requires from the applicant to show that he/she was personally and directly a victim of violation (Article 34)[1120] of the Convention rights and that he/she has suffered a 'significant disadvantage' (Article 35).[1121] If the applicant fails to satisfy this criteria,

---

[1117] supra note 132.

[1118] ibid, paragraph 180, p. 43.

[1119] ibid, paragraph 216, p. 53. Zakharov argued that 'the questions of notification of surveillance measures and of the effectiveness of remedies before the courts were inextricably linked, since there was in principle little scope for recourse to the courts by the individual concerned unless the latter was advised of the measure taken without his or her knowledge and was thus able to challenge their legality retrospectively'.

[1120] ECHR, supra note 3, art 34:

> [t]he Court may receive applications from any person, nongovernmental organization or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.

[1121] ECHR, supra note 3, art 35(3):

the ECtHR will not normally review a member state's relevant law and practice in the abstract. However, the Court has shown a degree of flexibility in this regard in the past. In *Klass v Germany,*[1122] it was found that the mere existence of laws and practices, which permitted and established a system of secret surveillance entailed a threat of surveillance for all those to whom the legislation might be applied. It was therefore held that an applicant could be a 'victim' in a situation where a violation is a result of the mere existence of secret measure or legislation permitting such measure, without having to show that it has in fact been applied to him/her. [1123] In *Kennedy v United Kingdom*[1124] the ECtHR stated that in order to assess whether an individual could claim an interference as a result of the mere existence of legislation permitting secret surveillance, the Court had to have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to the person concerned.[1125] Where there is no possibility to challenge the secret surveillance measure at domestic level, widespread suspicion and concern among the general public that such powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low there is a greater need for scrutiny by the ECtHR.[1126] In *Zakharov* the Court adopted the *Klass* and the *Kennedy* approaches[1127] and formulated a uniform and foreseeable approach to the circumstances as to when an applicant can claim a victim status. Thus, it stipulated that the applicant 'could claim to be a victim of violation of Article 8 occasioned by the mere existence of legislation, which allowed a system of secret interception of communications, without having to demonstrate that such measures were in fact applied to him',[1128] under certain conditions. First, he/she must show that he/she either belongs to a group of persons targeted by the secret surveillance measure, or that it directly affects all users of

---

> [t]he Court shall declare inadmissible any individual application submitted under Article 34 if it considers that:
> […]
> (b) the applicant has not suffered a significant disadvantage, unless respect for human rights as de ned in the Convention and the Protocols thereto requires an examination of the application on the merits and provided that no case may be rejected on this ground which has not been duly considered by a domestic tribunal.

[1122] supra note 111.
[1123] ibid, paragraph 36.
[1124] *Kennedy v United Kingdom* (2010) (Application No. 26839/05).
[1125] ibid, paragraph 124.
[1126] ibid.
[1127] *Zakharov*, supra note 132, p. 41.
[1128] ibid, paragraph 171, p. 41.

communications services. Secondly, the Court will take into account the available remedies at national level and adjust the degree of its scrutiny depending on the effectiveness of the remedies. [1129] Undoubtedly, the judgment has clarified the position with respect of who is permitted to bring a claim before the ECtHR, [1130] as the Court resolved the seemingly conflicting approaches and decided that the mere existence of laws and practices, which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied.[1131] Thus, the mere threat[1132] of secret surveillance measures is now sufficient to allow standing. It could be said that the Grand Chamber adopted a broad and liberal approach to this issue, because it examined the relevant legislation authorizing these measures not from the point of specific surveillance of Mr Zakhorov as the victim, but in the abstract. The ECtHR noted that the Russian legal framework provided for a system, under which any person using mobile phone services could have their communications intercepted, without ever being notified of the surveillance and as such, the legislation affected all users.[1133] In addition, Russian law did not provide for effective remedies for a person who suspected that they may be subject to surveillance.[1134] As a result of these findings, Mr Zakharov did not have to demonstrate that,

---

[1129] The Court at paragraph 171 specified these conditions in the following way:
(a) 'the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communications services by instituting a system where any person can have his or her communications intercepted'; and (b)'the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies'.

[1130] Before the *Zakharov* judgment, there were two lines of case law. The first, required the applicant to show a 'reasonable likelihood' that the security services had compiled and retained information concerning his/her private life (*Esbester v United Kingdom*, *Redgrave v United Kingdom*, *Christie v United Kingdom*, *Matthews v United Kingdom*. In these cases, the applicants alleged actual interception of their communications and in *Esbester*, *Redgrave*, *Mathews* and *Christie*, they also made general complaints about legislation and practice permitting secret surveillance measures.) The 'reasonable likelihood' requirement favoured the government's position. The second line of cases, including *Klass v Germany and Kennedy v UK*, suggested that the sole existence of laws and practices, which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied. Thus, the mere menace of secret surveillance measures was sufficient to allow standing and therefore this approach favoured the applicant.

[1131] *Zakharov*, supra note 132, para 168, p. 40.

[1132] ibid, para 171, p. 41.

[1133] ibid, para 175, p. 42.

[1134] ibid, para 176, p.42.

due to his personal situation, he was at risk of being subjected to secret surveillance.[1135] He was entitled to claim to be a victim of a violation of the Convention, despite not being able to demonstrate that he was subject to a concreate measure of surveillance-the mere existence of the legislation allowing this amounted to an interference with his rights under Article 8.[1136] This suggests that the ECtHR willingness to consider a case such as this *in abstracto* (that is without the applicant's need to show 'significant disadvantage' under Article 35), will make it easier (provided that all domestic avenues have been exhausted) to bring future challenges to state surveillance to the Strasbourg Court on condition that he/she can show the existence of legislation allowing for surveillance that affects all users of services in question and the lack of effective means to challenge the law at domestic level.[1137]

The second important aspect of this judgment is the enumeration of the criteria, according to which the Court will assess secret surveillance. These the Court enumerated as (a) the accessibility of the domestic law; (b) the scope and duration of the secret surveillance measures; (c) the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data; (d) the authorization procedures, the arrangements for supervising the implementation of secret surveillance measures; (e) any notification mechanisms and (f) the remedies provided for by national law.[1138] Having applied these to the Russian legal framework in *Zakharov,* [1139] the Court took issue with its many aspects. In particular, it criticized the fact that the legislation allowed interception of communications for broad 'national, military, economic, or ecological security purposes'.[1140] Since the law enforcement authorities had direct access to all mobile telephone communications and related communications data, the Court observed that 'any system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorization to the communications service provider, or to any one else, is particularly prone to abuse',[1141] which calls for greater safeguards against arbitrariness and abuse. Other aspects of the interception regime were also considered,[1142] but importantly the ECtHR viewed the

[1135] ibid, para 177, p.42.
[1136] ibid, para 179, p. 42.
[1137] ibid, para 179, p. 42.
[1138] ibid, para 238, p. 60.
[1139] ibid.
[1140] ibid, para 248, p. 62.
[1141] ibid, para 270, p. 69.
[1142] These included '(a) the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity; (b) provisions on

remedies available to challenge the interception under the Russian legal system inadequate, in that they were available only to persons, who were able to submit proof of interception. Obtaining such evidence was impossible in the absence of any notification requirement therefore an ability to retrospectively challenge a surveillance measure was practically meaningless.[1143]

The third aspect of the *Zakharov* judgment worthy of note is the fact that it has updated and consolidated the Court's previous extensive jurisprudence on surveillance, stressing the requirements of 'necessity' and 'proportionality' in Article 8(2). It could be said therefore that this case is not a departure from the Court's previous decisions, but it reaffirms and highlights the dangers of bulk, untargeted surveillance conducted without proper independent oversights. Thus, the Court reiterated the need for the authorization warrants, which must be very specific and targeted at particular individuals or premises based on a reasonable and verifiable suspicion against the person concerned, stressing in particular the need for factual indictors for suspecting that a given individual is planning, committing or having committed a criminal act or one endangering national security.[1144] The requested interception must meet the requirements of 'necessity' and 'proportionality' in a democratic society, including whether it is proportionate to the aim pursued by verifying, for example whether it is possible to achieve that aim by less restrictive means (*Klass,*[1145] *Association for European Integration and Human Rights and Ekimdziehiev v Bulgarian*[1146]). In *Zakharov*, the Court acknowledged that the interception requests were reviewed before national courts. However, the authorizations were based on information pertaining to criminal offence or activities endangering national, economic or ecological security. There was no need under the domestic law for them to be supported by any

discontinuation of secret surveillance do not provide sufficient guarantees against arbitrary interference; (c) the domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of the trial; (d) the authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when 'necessary in a democratic sociality'; (e) the supervision of interception, as it is currently organized, does not comply with the requirement of independence, powers and competence which are sufficient to exercise an effective and continuous control, public security and effectiveness in practice; (f) the effectiveness of remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interception'. Paragraph 302.

[1143] *Zakharov*, supra note 132, para 300, p. 78.

[1144] ibid, paragraph 260-20, p. 65.

[1145] supra note 111.

[1146] *Association of European Integration and Human Rights and Ekmdzhiev v Bulgaria* (227) (App. No. 62540/00).

other evidence.[1147] The only criteria for rejection of the interception request was the lack of signature of a competent person. As Russian courts never had to verify whether there was a 'reasonable suspicion' relating to the person concerned, there was no need to apply the 'necessity' and 'proportionality' test.[1148] Therefore the legislation permitting the interception of communications for broad national security, or military purposes, without an indication of the particular circumstances, under which an individual's communications may be intercepted, simply did not justify the use of such measures, even if the legislation required prior judicial authorization.

The ECtHR took an equally robust stance regarding domestic surveillance measures in the Hungarian case of *Szabo and Vissy v Hungary*,[1149] which was decided shorty after *Zakharov*. The case concerned surveillance powers of the Hungarian intelligence agencies under the Police Act 1994 (s. 7/E(3)), including interception of electronic or computerized communications on anti-terrorist grounds, without the consent of the person concerned. These powers were subject to ministerial, rather than judicial authorization. They were not linked to a particular crime and required a general warrant, which had to relate only to premises, persons concerned or 'a range of persons', being therefore potentially executable against any person in Hungary. Given that the scope of the measures could include virtually everyone in that country, the ordering was entirely in the guise of the executive without an assessment of whether interception was strictly necessary. Since new technologies enabled the Hungarian government to intercept vast amounts of data concerning even persons outside the original range of operations and because there was an absence of any effective remedial measure, the ECtHR concluded that there has been a violation of Article 8 ECHR.

The *Zakharov* and *Szabo* decisions could be viewed as seriously undermining of bulk, untargeted surveillance regimes. In *Zakhorov* not only did the ECtHR list and refer to the recent cases of the Court of Justice of the European Union in *Schrems v Data Protection Commissioner*[1150] and *Digital Rights Ireland* [1151] (both discussed elsewhere in this chapter), but it also made several explicit references to the Snowden revelations in the judgment

[1147] *Zakharov*, supra note 132, p. 66.
[1148] ibid, para 263, p. 67.
[1149] *Szabo*, supra note 133.
[1150] Case C-362/14 *Maximillian Schrems v Data Protection* Commissioner [2015] ECJ.
[1151] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitilinger and Others* [2014] ECJ.

itself.[1152] These judgments are an indication of the ECtHR antagonism towards mass surveillance and signal that the Court may take an uncompromising approach to the surveillance practices of the UK GCHQ, domestic and extraterritorial alike, when reaching its decisions in three currently pending cyber surveillance cases of *Bureau of Investigative Journalism and Alice Ross v UK*,[1153] *Big Brother Watch and Others v UK*,[1154] and *10 Human Rights Organizations v UK*.[1155]

b. The Inter-American Human Rights System

The origins of this system lie in two distinct but related instruments:- (a) the OAS Charter system of human rights, which relies on the OAS Charter and the American Declaration on the Rights and Duties of Man 1948; and (b) the American Convention on Human Rights 1969, binding on those member states, which have voluntarily become parties to the Convention.[1156] The right to privacy is contained in Article 11.[1157] These two systems operate through inter-

[1152] *Zakharov*, supra note 132. Direct references were made to the text from the Director of the European Union Agency for Human Rights discussing Snowden and in the separate opinion issued by Judge Dedov.

[1153] *Bureau of Investigative Journalism and Alice Ross v UK* (App. No. 62322/14). The case concerns the applicants' allegations regarding breach of Article 8 and 10 rights through interception, storage and exploitation of internet and telephone communications by the UK government agencies, including GCHQ, as revealed by Edward Snowden.

[1154] *Big Brother Watch and Others v UK* (App. No. 58170/13). This case has been brought before the ECtHR by three NGOs and an academic, alleging breach of Article 8 right on the basis that they are likely to have been subjects of surveillance by the UK intelligence agencies, following the revelations of Edward Snowden.

[1155] *10 Human Rights Organizations v UK* (9 April 2015) (Index No.: IOR 60/1415/2015). Amnesty International states that 'the Applicants are 10 non-governmental human rights organizations based both within and outside the United Kingdom - the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International. Their complaints to ECHR are concerned with mass bulk interception, collection, inspection, distribution and retention of communications on a vast, unprecedented scale. The UK Government carries out such activity itself and also receives the product of such activity carried out by the US Government. The Applicants complain of violations of their rights both in relation to the content of their communications and the associated metadata.' Amnesty International <https://www.amnesty.org/en/documents/ior60/1415/2015/en/>.

[1156] Rehman, supra note 79, p. 272.

[1157] American Convention on Human Rights, supra note 5, art 11:

1. [e]veryone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

related organ, the Inter-American Commission on Human Rights (IACommHR) and the Inter-American Court on Human Rights (IACtHR). Both organs are mandated with deciding individual complaints concerning human rights violations and the Commission also engages in human rights monitoring and promotion activities.[1158] It is important to note that the US has signed but not ratified the ACHR, hence the IACtHR and IACommHR have no jurisdiction to hear cases against that country. Nevertheless, the protection of privacy in Article 11 ACHR applies to most Latin American states. In addition, the US has signed and ratified the Charter of the Organization of American States and therefore in the view of the IACommHR it is bound at international level by the American Declaration.[1159]

In a similar vein to the ICCPR, the ACHR in Article 11 prohibits 'arbitrary or abusive interference with [individual's] private life or correspondence'. The American Declaration also refers to the notion of private life in Article 5, which provides that 'every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life'. Moreover, Article 10 of the Declaration states that 'every person has the right to the inviolability of his correspondence'.[1160] Article 11 ACHR is also phrased in a similar way to Article 8 ECHR. In addition, the Inter-American Commission has been influenced in its approach by the decisions of the ECtHR in interpreting the ambit of Article 11. Although the jurisprudence of the IACtHR is not as well developed as that of the Strasbourg Court, it did consider the question of interference with the right to privacy in two cases relating to the lawfulness of telephone wiretapping. In *Donoso v Panama*[1161] the IACtHR concluded that telephone conversations, whether private or business related, fall within the ambit of Article 11. Therefore, the interception of telephone communications without the consent of the callers constituted an interference with the right to privacy. In *Escher v Columbia*,[1162] the Court

3. Everyone has the right to the protection of the law against such interference or attacks.

[1158] The Commission holds thematic hearings on specific issues, publishes studies and reports, requests the adoption of precautionary measures to protect individuals at risk and has established a number of thematic rapporteurships to closely monitor certain human rights themes. Individuals, groups of individuals and non-governmental organizations recognized in the OAS may submit complaints (petitions) concerning violations of the American Declaration of the Rights and Duties of Man 1948, American Convention on Human Rights and other regional human rights treaties.

[1159] *Roach v United States*, Case 9647, Inter-Am. Comm'n HR.

[1160] American Declaration of the Rights and Duties of Man, O.AS. Res. XXX, adopted by the Ninth International Conference of American States (1948), Article X.

[1161] *Donoso v Panama*, Judgement, IACtHR (Ser. C) No. 193 (27 January 2009), para 193,

[1162] *Escher v Columbia*, Judgement IACtHR (Ser. C) No. 200, para 114.

enumerated the protected aspects of telephone conversations, namely their content, as well as all related information, such as the caller, the recipient, time and duration of the call.

All the above human rights instruments have some unifying features, in that (a) they refer to the right to privacy of correspondence, which has been interpreted by at least two judicial organs (the HRC and the ECtHR) to cover electronic surveillance and interception of communications by state agencies; (b) they all use the term 'interference' to describe the prohibited action, except for the American Declaration, but none refer to what type of interference is prohibited; and (c) in all four documents the right to privacy is qualified, rather than absolute. At least some treaties, for example Article 8(2) ECHR, enumerate permissible limitations of this right, whilst others, such as ICCPR, do not.

C. Domestic Legal Bases Permitting Interception of Communications

All governments are under a duty to protect citizens within their borders from acts of terrorism and criminality. To that end, they may carry out surveillance both within and beyond their own territory on the basis of their domestic legal frameworks. However, these frameworks must comply with states' human rights obligations and meet the minimum standards, defined by the international human rights treaties and as interpreted by the relevant judicial organs.

Cyber surveillance is a new challenge to the right of privacy of communications set out by international law. The scale and scope of surveillance has been made possible because of an a-territorial nature of cyberspace as it mandates borderless routing and storage of information, allowing states to conduct interception of communications from within their own territories and then share it. This calls into question the extent to which an individual may rely on human rights protection. Historically, governments were restricted in their exercise of communications surveillance in another country. If such operations were conducted, this would inevitably breach the principles of state sovereignty and give affected persons protection under their domestic laws. The expeditious technical progress in digital communications, coupled with the post 11 September 2001 (9/11) shift in focus from surveillance of the foreign powers and states to the interception of communications of all individuals, means that the privacy rights of all concerned (foreign nationals, nationals and stateless persons alike) have been compromised to a significant degree. This is not only because of the scope and the breath of

surveillance methods through such programmes as Tempora and Boundless Informant,[1163] but also due to the highly integrated nature of communications networks. This integrated nature means that many of the agencies sweep up all data indiscriminately, justifying this on the basis of the technical difficulties between distinguishing foreign and domestic communications.[1164]

On inspection of the legislative interception powers of the Five Eyes partners, it becomes clear that there is a disparity in treatment of individuals based on their nationality and/or location. In most of the countries concerned greater procedural protection of privacy rights is given to the citizens as opposed to non-citizens, or non-nationals. The particular domestic statutes that expressly regulate intelligence agencies surveillance powers are: (a) the UK Regulation of Investigatory Powers Act 2000 (RIPA), 5;[1165] (b) the US 18 U.S.C § 2511(2), the so-called Wiretap Act;[1166] (c) South African Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 (RICA), ss. 2-11;[1167] (d) Australian Telecommunications (Interception and Access) Act 1979, s 6;[1168](e) Canadian Criminal Code of Canada (Invasion of Privacy) 1985 Part VI;[1169] and (f) New Zealand Government Communication Security Bureau Act 2003, s. 15.[1170] As a general rule, these laws make the interception of domestic communications by state agencies illegal, unless authorized

---

[1163] Glenn Greenwald and Ewan MacAskill 'Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data' (11 June 2013) *The Guardian* <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>. *The Guardian* exposed that Boundless Informant data contained in a top secrete NSA document showed that in March 2013 the NSA collected 97bn pieces of intelligence from computer networks worldwide. The largest amount of information was gathered from Iran, with more than 14bn reports in that period, followed by 13.5bn from Pakistan, 12.7bn from Jordan (one of the US closest Arab allies), 7.6bn form Egypt and 6.3bn from India. Boundless Informant details and maps by country the amount of information it collects from computer and telephone networks, mainly metadata.

[1164] supra note 180. According to *The Guardian*, a spokesman for the NSA said that 'current technology simply does not permit us to positively identify all of the persons or locations associated with a given communication (for example, it may be possible to say with certainty that a communication traversed a particular path within the internet. It is harder to know the ultimate source or destination, or more particularly the identity of the person represented by the TO:, FROM:, or CC:, field of an e-mail address or the abstraction of an IP address'.

[1165] Parliament of the United Kingdom, Regulation of Investigatory Powers Act, 2000 c. 23 (Royal Assent 28 July 2000), s. 5.

[1166] US 18 U.S.C § 2511(1).

[1167] Regulation of Interception of Communications and Provision of Communication Related Information Act 2002, Part 1.

[1168] Telecommunications (Interception and Access) Act 1979, s. 6.

[1169] Criminal Code (R.S.C. 1985), 164.

[1170] Government Communication Security Bureau Act 2003, s. 15.

by appropriate judicial, or executive authority on such grounds as serious criminal or terrorist activities.

a. Domestic Legal Frameworks Authorizing Foreign Surveillance and the Principle of Non-Discrimination

The two sets of domestic laws with regard to conducting cyber surveillance abroad discussed next are those of the US and UK.

In the US the applicable legislation that allows for acquisition of foreign intelligence information is the Foreign Intelligence Surveillance Act 1978 (FISA), (as amended by of the FISA Amendment Act 2008 (FAA)) and by the Executive Order 12333.[1171] Section 702 of FISA 'Procedures for Targeting Certain Persons Outside the United States Other than United States Persons' (50 USC Sec. §1881a) states that:

> [t]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

As an amendment to the 1978 FISA, section 702 (§1881a) introduced new power for the US government entities to gather foreign intelligence information for national security purposes and acquire data of non-US persons believed to be located abroad. As such, it is the foundational authority by which the NSA collects, retains, analyses and disseminates foreign intelligence information. [1172] The principle application of §1881a is the collection of communications by foreign persons that occur wholly outside the United States. [1173] This provision is used for making the so-called PRISM orders, which are directed at specific private companies to compel disclosure of content of communications, so long as it is targeted at a

[1171] Executive Order 12333, United States Intelligence Activities (As Amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), < https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf>.
[1172] Richard A. Clarke et al., *The NSA Report. Liberty and Security in a Changing World. The President's Review Group on Intelligence and Communications Technologies*. (Princeton University Press 2014).
[1173] ibid.

sufficient percentage (51%) of foreign people.[1174] It is also the basis for the 'Upstream' Collection Orders, allowing the NSA to work with telecommunication companies to copy, scan and filter internet and phone traffic through their physical infrastructure[1175] Section 702 specifically prohibits intentionally targeting of Americans, so when intercepting their communications, the government officials must operate under at least a modicum of judicial oversight (i.e. have a warrant showing a probable cause), lest they are guilty of a felony.[1176]

Likewise, UK RIPA makes a nationality distinction by differentiating between 'internal' and 'external' surveillance.[1177] Section 20 defines 'external communication' as 'means of communication sent or received outside the British Islands'.[1178] The section does not directly define 'internal communication', but it could be said that this means communication, which is neither sent, nor received outside the British Islands. In case of 'internal communication', section 8 RIPA specifies that an interception warrant must be issued to permit lawful interception, it must describe one person as the 'interception subject', or identify a 'single set of premises', for which the interception is to take place.[1179] Section 8(2) requires a warrant, which must set out 'the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted'.[1180] In case of 'external' communication, RIPA s. 8(1) and (2) does not apply, which means that there is no need to identify any particular person who is to be subject of the interception, or a particular address that will be targeted.

Similar distinctions between surveillance conducted on citizens and foreign nationals are made under the New Zealand section 15A of the Government Communications Security

---

[1174] Electronic Frontier Foundation, 'Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its Illegal and Unconstitutional Use', <https://www.eff.org/files/filenode/702_one_pager_final_adv.pdf>.
[1175] ibid.
[1176] ibid.
[1177] ibid.
[1178] RIPA, supra note 182, s. 20.
[1179] ibid, s. 8(1)(a) and (b):

> [a]n interception warrant must name or describe either—
> (a) one person as the interception subject; or
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

[1180] ibid, s. 8(2):

> [t]he provisions of an interception warrant describing communications the interception of which is authorized or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.

Bureau Act 2003 (amended in 2013),[1181] section 9 of the Australian Intelligence Services Act 2000[1182] and section 273 of the Canadian National Defense Act 2015.[1183]

The discriminatory nature of s 702 FAA 2008 and s 8 RIPA 2000 is clear, but it is just a part of a wider US and its Five Eyes partners' policy stance post 11 September 2001, which places emphasis on citizenship as a basis for fundamental rights.[1184] This therefore requires that the rights of non-citizens be clarified under international law. The fundamental recognition that all persons by virtue of their essential humanity are equal and should enjoy all human rights without discrimination is contained in Article 2(1) of the Universal Declaration of Human Rights;[1185] Articles 2[1186] and 26[1187] of the ICCPR; Articles 1[1188] and 2[1189] of the International Covenant of on Economic Social and Cultural Rights 1976 (ICESCR); and Article 14[1190] of the ECHR. In General Comment No. 15 in relation to the rights under the ICCPR, the Human Rights Committee explained that the rights in the Covenant apply to everyone, irrespective of their nationality and the general rule is that each one of these rights must be guaranteed without discrimination between citizens and aliens.[1191] The ICESCR likewise established that governments shall take progressive measures to the extent of available resources to protect the rights of everyone regardless of their citizenship.[1192] Thus, the fundamental principle dictates that human rights are presumptively owed to citizens and non-citizens alike, unless a particular treaty (or customary rule) allows for differential treatment. Both the ICCPR and the ICESCR permit states to draw distinctions between citizens and non-citizens, but only with respect to three categories of rights, namely political rights, freedom of

[1181] The Government Security Communications Bureau (GCSB) can apply for an interception warrant under s. 15A of the Government Communications Security Bureau Act 2003 (amended 2013).
[1182] Intelligence Services Act 2001, s. 8.
[1183] The National Defence Act 2015 give powers to the Communications Security Establishment Canada (CSEC), section 273.64(1).
[1184] Marko Milanovic, 'Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?' (25 November 2013) EJIL: Talk! <http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/>.
[1185] Universal Declaration of Human Rights, supra note 81, art 2(1).
[1186] ICCPR supra note 2, art 2(1).
[1187] ibid, art 26.
[1188] International Covenant on Economic Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) UNTS 993 (ICESCR), art 1.
[1189] ICESCR, ibid art 2.
[1190] ECHR, supra note 3, art 14.
[1191] UN HRC, 'General Comment No. 15. The Position of Aliens under the Covenant' (1986) UN Doc HRI/Gen/1/Rev.9/(Vol.1) para 1-2.
[1192] ICESCR, supra note 205, art 2.

movement and economic rights in developing countries. Thus, under Article 25 ICCPR, the right to participate in public affairs, to vote, to hold office and to have access to public services is guaranteed to citizens only.[1193] Similarly, Article 12(4) ICCPR provides that no one shall be arbitrarily deprived of the right to enter his own country, [1194] whilst the ICESCR Article 2(3) allows developing counties to 'determine to what extent they would guarantee the economic rights recognized in the present Covenant to non-nationals'.[1195] States therefore may not draw distinction between citizens and non-citizens as to social and cultural rights, with exception of the right to public participation and of movement. Having said that, international law, as well as state practice consistently sanctions discrimination and distinctions on the basis of nationality, which means that some discrimination on these grounds would be permissible.[1196] The HRC in its General Comment No. 18 clarified this by stating that:

> [n]ot every differentiation of treatment will constitute discrimination, if the criteria for such a differentiation are reasonable and objective and if the aim is to achieve a purpose, which is legitimate under the [International] Covenant [of Civil and Political Rights][1197]

and is proportional to the achievement of that objective.

The 'objective and reasonable justification' is also the criteria that the European Court of Human Rights requires a state to satisfy in order to show that the difference in treatment was not discriminatory. In *Burden v United Kingdom*[1198] the Strasbourg Court held that:

> [a] difference of treatment is discriminatory if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim and if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised. The Contracting State enjoys a margin of appreciation in assessing whether and to what extent

[1193] ICCPR, supra note 2, art 25.
[1194] ibid, art 12(4).
[1195] ICESCR, supra note 205, art 2(3).
[1196] General Comment No. 15, supra note 208, paras 23-30.
[1197] UN HRC, 'General Comment No. 18: Non-Discrimination' (1989) UN Doc HRI/GEN/1/Rev.1 para 13.
[1198] *Burden v United Kingdom* (2008) ECHR 357 [GC].

differences in otherwise similar situations justify a different treatment.[1199]

States are obliged to ensure that measures taken in the struggle against terrorism do not discriminate in purpose, or effect on grounds of nationality and the principle of non-discrimination must be observed in all matters, in particular in those concerning liberty, security and dignity of the person, equality before the courts and due process of law, as well as international cooperation in judicial and police matters.[1200] In guaranteeing certain rights to citizens only, the US and the UK laws breach the provisions of non-discrimination and equal treatment under the ICCPR and the ECHR, which as will be shown in the next part of this chapter, cannot be justified on objective and reasonable grounds. Indeed:

> [t]he unique position of the United States [and the United Kingdom] with regards to the physical infrastructure of the internet and the fact that the private companies based in the US collect and store huge amounts of data of persons residing anywhere in the world makes the exclusion of 'non-US [and UK] persons' from any legal protection against mass surveillance simply intolerable-it may well lead to the destruction of the internet as we know it.[1201]

This therefore calls for clarification as to whether and how human rights treaties apply to foreign cyber surveillance, that is their extraterritorial scope, as discussed next.

PART III: DO HUMAN RIGHTS TREATIES APPLY TO EXTRATERRITORIAL CYBER SURVEILLANCE AND THE TRANSBORDER ACCESS TO DATA?

Chapter 2 of this thesis made a number of observations in relation to the transnational nature of cyberspace. In particular, it noted that the early proponents of internet freedom, such as Johnson and Post,[1202] argued that states will never be able to exercise effective authority in that domain due to its a-territorial nature. This proved not to be the case, as governments do

[1199] ibid, para 60.
[1200] UNCHR, (Sub-Commission), 'Report by Special Rapporteur David Weissbrodt' (2003) UN Doc E/CN.4/Sub.2/2003/23, para 28.
[1201] 'Mass Surveillance', supra note 6.
[1202] David Johnson and David Post, 'Law and Borders-the Rise of Law in Cyberspace' (1996) 48 Stanford Law Review, p. 1367.

assert their rights to regulate online activities within their own borders through such methods as censorship. This chapter has shown that they also exercise powers of communications surveillance granted by their national laws (outlined above) with respect to foreigners, who are not located in their territories. Furthermore, the law enforcement agencies (LEAs), including those states, who are a party to the Cybercrime Convention 2001, are able to access information stored in other territories by- passing the requirements of the Mutual Assistance Treaties. The interoperability of the intelligence agencies of the Five Eyes (and their affiliates) and the law enforcement agencies at the technical and operational levels raise questions as to how and when states may be liable under international law for their cyber surveillance activities, which may have impact beyond their borders. Since the Snowden revelations, the issue of the application of human rights treaties to cyber surveillance has become particularly vexatious. It is also one of the most fundamental and problematic aspects of the future of internet governance that the international community must give serious consideration to.

In this context, two problems arise. First, can human rights treaties apply to extraterritorial cyber surveillance? Secondly, how can states' exercise of enforcement jurisdiction in order to gather evidence so as to prosecute certain crimes, be brought in line with their human rights obligations?

1. Extraterritorial Application of Human Rights Treaties

The jurisdictional scope of application of the ICCPR, the ECHR and the ACHR are set out in Article 2(1), [1203] Article 1 [1204] and Article 1 [1205] respectively. The jurisdictional

[1203] ICCPR, supra note 2, art 2(1):

> [e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political, or other opinion, national, or social origin, property, birth, or other status.

[1204] ECHR, supra note 3, art 1:

> [t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this Convention.

[1205] ACHR, supra note 5, art 1:

> 1. [t]he States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition.

competence of a state is primarily territorial.[1206] States may be liable for violations committed outside their territory, but the extent to which they will be accountable in respect of such acts or omissions is not entirely settled. Two opposing positions have been taken to the question of extraterritorial applicability of human rights treaties, namely a narrow and an expansive one. The former, held by the US executive branch has consistently rejected the view that the ICCPR places human rights obligations on that country outside its territory. The latter position, expressed by international courts and tribunals,[1207] firmly attests to the fact that in certain circumstances states do have human rights obligations outside their frontiers. Each view will be outlined below.

a. The Narrow View

The United States ratified the ICCPR in 1992. The first time that the US government articulated the stance that the Covenant cannot apply extraterritorially was in a 1995 statement it made to the Human Rights Committee.[1208] The US asserted that the wording of its Article 2 restricted its scope to persons who are simultaneously under the United States jurisdiction and within its territory. The subsequent administrations reiterated this view in the Consolidated Second and Third Periodic Report to the Human Rights Committee.[1209] The position taken by the US

---

2. For the purposes of this Convention, 'person' means every human being

[1206] *Bankovic and Others v Belgium* (2007) EHRR 57.

[1207] That is, the International Court of Justice, the United Nations Human Rights Committee and the European Court of Human Rights and the Inter-American Court of Human Rights and domestic courts of such countries as the United Kingdom.

[1208] UN HRC, Fifty -Third Session, Summary Record of the 1405th Meeting, CCPR/C/SR.1405 (24 April 1995). The US government's position was made clear in paragraph 20:

> Mr. Klein had asked whether the United States took the view that the Covenant did not apply to government actions outside the United States. The Covenant was not regarded as having extraterritorial application. In general, where the scope of application of a treaty was not specified, it was presumed to apply only within a party's territory. Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized 'to all individuals within its territory and subject to its jurisdiction'. That dual requirement restricted the scope of the Covenant to persons under United States jurisdiction and within United States territory. During the negotiating history, the words 'within its territory' had been debated and were added by vote, with the clear understanding that such wording would limit the obligations to within a Party's territory.

[1209] UN HRC, Consolidation of Reports Submitted by States Parties Under Article 40 of the Covenant, CCPR/C/USA/3 (28 November 2005). According to the Report:

> The Vienna Convention on the Law of Treaties states the basic rules for the

government is based on an an interpretation of Article 31(1) of the Vienna Convention on the Law of Treaties (VCLT),[1210] which requires that treaties should be read 'in accordance with the ordinary meaning […] of [their] terms'.[1211] Since, on this interpretation, an obligation arises only if both conditions in Article 1 ICCPR are satisfied, namely that an individual must be 'within its territory' and 'subject to its jurisdiction', extraterritorial application of ICCPR has been ruled out.

Both the Human Rights Committee in its General Comment 31 and case law, together with the International Court of Justice (ICJ) in the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* Advisory Opinion of 2004 (the Wall Advisory Opinion)[1212] and *Case Concerning Armed Activities on the Territory of the Congo* (DRC v Uganda)[1213] rejected this interpretation.[1214] In its 1995 Report the HRC stated that:

---

interpretation of treaties. In Article 31(1), it states that:

> [a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

> Resort to this fundamental rule of interpretation leads to the inescapable conclusion that the obligations assumed by a State Party to the International Covenant on Civil and Political Rights (Covenant) apply only within the territory of the State Party. Article 2(1) of the Covenant states that '[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind.' Hence, based on the plain and ordinary meaning of its text, this Article establishes that States Parties are required to ensure the rights in the Covenant only to individuals who are both within the territory of a State Party and subject to that State Party's sovereign authority.

[1210] Vienna Convention on the Law of the Treaties, 23 May 1969, 1155 U.N.T.S. 331.

[1211] ibid, article 31(1):

> [a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

[1212] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories*, Advisory Opinion, 2004 ICJ Reports 163 (9 July).

[1213] *Case Concerning Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda), Request for the Indication of Provisional Measures, Order of 1 July 2000, [2000] ICJ Reports 111.

[1214] Marco Milanovic, 'Foreign Surveillance and Human Rights, Part 2: Interpreting the ICCPR' (2015) EJILTalk!, p. 3. < http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-2-interpreting-the-iccpr/>.

> [it] does not share the view expressed by the Government [of the United States] that the Covenant lacks extraterritorial reach under all circumstances [because] such a view is contrary to the consistent interpretation of the Committee on this subject, that in special circumstances, persons may fall under the subject-matter jurisdiction of a [s]tate party even when outside that state's territory.[1215]

This criticism the Committee repeated in its 2006 and 2014 reports,[1216] observing that the US restrictive approach on the issue conflicted with international authorities and that the US holds this position 'despite the contrary opinions and established jurisprudence of the Committee and the International Court of Justice'.[1217] Although the US sustains the view that it is under no obligation to comply with Article 17 ICCPR outside its own geographical territory, the next part of this chapter will show that this position is very much in the minority.

[1215] Report of the UN Human Rights Committee, (1994) UN Doc 5/50/40, para 284.

[1216] Concluding Observations of the UN HRC on the US Repot Under the ICCPR, (2006) CCPR/C/USA/CO/3; Concluding Observations of the UNHRC on the US Report Under the ICCPR, (2014) CCPR/C/USA/4. Both Reports state in paragraph C. 4, *Applicability of the Covenant at National Level,* that:

> [t]he Committee regrets that the State party continues to maintain its position that the Covenant does not apply with respect to individuals under its jurisdiction but outside its territory, despite the contrary interpretation of article 2(1) supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and state practice. The Committee further notes that the State party has only limited avenues to ensure that state and local governments respect and implement the Covenant, and that its provisions have been declared to be non-self-executing at the time of ratification. Taken together, these elements considerably limit the legal reach and the practical relevance of the Covenant (art. 2).
>
> The State party should:
>
> (a) Interpret the Covenant in good faith, in accordance with the ordinary meaning to be given to its terms in their context, including subsequent practice, and in the light of its object and purpose and review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances, as outlined inter alia in the Committee's general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant;

[1217] UN HRC, 'Consideration of Reports Submitted by State Parties under Article 40 of the Covenant: Concluding Observations of the Human Rights Committee, United States of America', 87th Sess. 10-28 July 2006 (18 December 2006). UN Doc CCPR/C/USA/CO/3/Rev.1

b. The Expansive View

As already noted, the jurisdictional competence of a state is primarily territorial.[1218] However, the International Court of Justice (ICJ), together with all major human rights courts and bodies, such as the UN HRC, the Inter-American Commission on Human Rights (IACHR) and the European Court of Human Rights agree that in some circumstances human right obligations may apply extraterritorially. This means that a state is bound by international human rights law in relation to individuals, who may be not within its borders, but who are under its jurisdiction. To that end, a broadly similar approach, based on 'effective control', has been adopted to determine jurisdiction. Thus, the HRC held that:

> a [s]tate [p]arty must respect and ensure the rights laid down in the [International] Covenant [of Civil and Political Rights] to anyone within the power, or effective control of that State Party, even if not situated within the territory of the [s]tate [p]arty.[1219]

Similarly, the IACHR established that to determine whether a person is within a state's jurisdiction 'the inquiry turns not on the presumed victim's nationality, or presence within a particular geographical area, but on whether under specific circumstances, the State observed the rights of a person subject to its authority and control'.[1220] In conceptualizing when and how the international human rights obligations may arise outside a state's territory, two types of extraterritorial jurisdiction were distinguished, namely the spatial and the personal model. The spatial model sees jurisdiction as effective overall control over a geographical area, whereas the personal, as a physical control over an individual. The spatial model was articulated by the ECtHR in *Loizidou v Turkey*,[1221] where the Court held that state's responsibility was engaged when, as a consequence of lawful or unlawful military action, it exercised effective control of an area outside its national territory. Similar approach was adopted by the ICJ in the *Wall* Advisory Opinion [1222] and in *DRC v Uganda,* [1223] who found that the ICCPR applies

[1218] supra note 224.
[1219] UN HRC 'General Comment No. 31. The Nature of the General Obligations Imposed on State Parties to the Covenant' (2004) UN Doc CCPR/C/21/Rev.1/Add1326 May 2004, para 10.
[1220] *Alexandre v Cuba*, Case 11.589, (1999) IACHR Report No. 109/99, para 37.
[1221] *Loizidou v Turkey* (1995) 20 EHRR 99.
[1222] *Wall* Advisory Opinion, supra note 229.
[1223] *DRC v Uruguay*, supra note 230.

extraterritorially, where a state is occupying territory of another state. Whilst the spatial model has its merits, particularly in its clarity and setting some limits on states' obligations, it also has some drawbacks.[1224] As noted by Milanovic, 'a state is perfectly capable of violating the rights of individuals without controlling the actual area', for example by using drones for targeted killing thus disposing of the need to have troops on the ground.[1225]

The jurisprudence of the international human rights courts has additionally recognized that states have human rights obligations when exercising physical control over an individual. In *Lopez Burgos v Uruguay*[1226] the HRC held that state parties are liable for the actions of their agents on foreign territory, as it would be 'unconscionable to so interpret the responsibility under Article 2 of the [ICCPR] as to permit a [s]tate [p]arty to perpetrate violations of the Covenant on the territory of another [s]tate, which violations it could not perpetrate on its own territory'.[1227] In its General Comment No. 31 the Committee established that:

> a [s]tate [p]arty must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that [s]tate [p]arty, even if not situated within the territory of the [s]tate [p]arty…regardless of the circumstances in which such power or effective control was obtained.[1228]

However, by far the most varied jurisprudence regarding the personal model is that of the Strasbourg Court. In *Al-Skeini v UK*[1229] the ECtHR stressed the primary territorial nature of jurisdiction under the ECHR but recognized exceptions to that principle, namely where state agents exercise authority and control extra-territorially and when a state exercises effective control of an area outside national territory. State agent authority is particularly pertinent in military operations, where physical authority and control is exercised in formal detention centres, as was the case in the British controlled facilities in *Al-Skeini*. However, the exercise of authority was also held to have occurred outside of a formal detention centre in *Öcalan v Turkey*.[1230] The case concerned the handover in Kenya to Turkish authorities of an individual

---

[1224] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81, pp. 114-115.
[1225] ibid, p. 113.
[1226] UNHRC *Lopez Burgoz v Uruguay*, Communications No 52/1979 (17 July 1979) UN Doc CCPR/C/13/D/52/1979.
[1227] ibid, paras 12.2-12.3
[1228] supra note 236, para 10.
[1229] *Al-Skeini and Others v United Kingdom* [GC] (7 July 2011) ECHR 2011.
[1230] *Öcalan v Turkey* (2003) 41 EHRR 985.

suspected in Turkey of terrorist-related crimes. The ECtHR noted that he was effectively under Turkish authority and therefore within its jurisdiction, even though Turkish officials at the time of the arrest exercised their authority outside Turkey. In addition and most notably, the ECtHR has recognized that the extraterritorial jurisdiction on the basis of state agent authority, or control is not limited to situations of the physical custody over an individual, but may be engaged when state agents exercise authority and control over an individual's rights, as was the case in *Jaloud v the Netherlands*.[1231] That case concerned a fatal shooting of Azhar Sabah Jaloud, who at the time was passing through a checkpoint manned by personnel under the command and direct supervision of a Netherlands Royal Army officer in Iraq. The ECtHR found that the Netherlands exercised its jurisdiction on the basis that Dutch troops asserted 'authority and control over persons passing through the checkpoint' because they exercised authority and control over his right to life at that moment. This gave rise to extraterritorial jurisdiction, despite not having the physical control over Mr Jaloud. It could be said that the case marks the ECtHR moving away from an approach, whereby jurisdiction is found on the basis of pure factual authority, towards one based on the exercising of authority and control over an individual's rights.

c. Applicability of Human Rights Treaties to Extraterritorial Cyber Surveillance

It is submitted that if a state may be found to have human rights obligations, because it exercises authority and control over an individual's right to life as proposed in *Jaloud*, then by analogy the exercise of control over his/her right to privacy of communications should also give rise to state's extraterritorial obligations in cases of foreign cyber surveillance. Such an interpretation seems necessary, as the 'effective control' test is unsuitable, outdated and narrow in the context of state sponsored cyber surveillance operations. This is so because it has been articulated by the international human rights courts and bodies long before digital technologies began to play such a pervasive role in the lives of millions of individuals around the world. Furthermore, it is inadequate for the cyber and communications realm, as it places the emphasis on the exercise of physical control over persons, or territory, which is difficult to relate to cyberspace.[1232] The shortcomings of the effective control approach centre around the fact that some state intelligence services, particularly the NSA, exert effective remote, rather than

[1231] *Jaloud v the Netherlands* (2014) (App. No. 47708/08).
[1232] Peter Margulies, 'The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism' (2014) 82 Fordham Law Review 2137.

physical, control over much of the communications of foreign nationals abroad.[1233] This occurs through the eavesdropping on those communications, filtering, or altering their content and breaking many forms of encryption by installing 'back doors' engineered in many software systems.[1234] The NSA has also the capacity to gain control of computers not directly connected to the internet due to implantation of transmitting devices in computers manufactured in the US and elsewhere.[1235] In addition, the US has relationships with internet and telecommunication companies that facilitate surveillance and thereby the capacity to directly access the undersea cabled together with other carriers of internet and telephonic communications.[1236] The US virtual power is unprecedented[1237] and the narrowly defined standard requiring physical control means that states interfering with the right to privacy would continue to exploit this gap by circumventing their human rights obligations. There can be no doubt therefore that the 'effective control' test must be adapted to suit the realities of cyber surveillance operations.

A number of legal scholars made suggestions in this regard and their overall tenet seems to hinge on the control of communications, rather than the physical control over areas or individuals. Thus, Nyst argues that when data or communications are intercepted within a state's territory, the state should owe obligations to those individuals regardless of their location on the basis of 'interface-based jurisdiction,[1238] that is not to interfere with communications that pass through its territorial borders.[1239] This approach is broadly in line with that proposed by Milanovic, who distinguishes between the overarching positive obligation of states to secure or ensure human rights and extends even to preventing human rights violations by third parties and negative obligations of states to respect human rights that only requires states to refrain from interfering with the rights of individuals without sufficient justification.[1240] This model conceptualizes jurisdiction as a negative duty to refrain from interference and would apply to all potential violations of negative obligations, for example to

[1233] ibid, p. 2151.
[1234] ibid.
[1235] ibid.
[1236] ibid.
[1237] ibid.
[1238] Carly Nyst, 'Interface Based Jurisdiction Over Violations of the Right to Privacy' (21 November 2013) EJIL:Talk! <http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/>.
[1239] ibid.
[1240] supra note 241, p. 126.

refrain from interfering with privacy.[1241] In this sense, human rights treaties would apply to most, if not all foreign surveillance activities.[1242] Both these approaches have their merits, in as much as they recognize the weaknesses of the personal and spatial models and emphasise the negative duty of states not to interfere with the protected rights. However, the nature and scope of the Five Eyes surveillance seems to go beyond the interception, collection and storage of data. The partnership between the US and its allied services allows governments to easily engage in the so-called 'collusion for circumvention'.[1243] For example, GCHQ is allowed to spy on anyone but British nationals, whilst the NSA on anyone but Americans.[1244] Information sharing partnerships enable each agency to circumvent its respective national restrictions protecting their countries' citizens, since they are able to access the data collected by others.[1245] This reciprocity has important ramifications on the domestic level if it is strategically used to circumvent domestic legislation and limits on the governments' ability to tap its own citizens' communications.[1246] In this context, the negative duty not to interfere with privacy would only be discharged if the interference is also understood as the 'collusion for circumvention', encompassing such information sharing arrangements. This at present is not entirely clear and therefore calls for a model of jurisdiction, which is capable of meeting such challenges. A sound candidate may be the 'virtual control' test, proposed by Margulies.[1247] This test would make the ICCPR and other human rights treaties applicable when a state can assert 'virtual control' over an individual's communications, even though it lacks control over the territory, in which the individual is located, or over the 'physical person' of that individual.[1248] 'Virtual control' in this context means the ability to intercept, store, analyse and use communications. Although it could be argued that mere surveillance does not constitute physical control over an individual, it may constitute virtual control, in that it stifles not only his/her right to privacy, but also has a chilling effect on other human rights, such as free expression, freedom of conscience and religion, free assembly, association and health, to name but a few. It therefore does affect and control individuals' behaviour. Although the 'virtual control' approach has been criticised for being new and 'without support in patters of generally shared legal

[1241] ibid.
[1242] ibid, p. 129.
[1243] 'Mass Surveillance', supra note 6, paras 30-3.
[1244] ibid.
[1245] ibid.
[1246] ibid.
[1247] supra note 249, p. 2139.
[1248] ibid.

expectations about personal jurisdiction', [1249] it has a number of advantages. First, it corresponds to the notion of control developed and required by the human rights courts and bodies, [1250] outlined above. Secondly, it responds to the jurisdictional challenges of human rights obligations in surveillance cases, because the intelligence agencies under scrutiny are perfectly capable of controlling lives and private information with the press of the button. [1251] Thirdly, it is in line with the ECtHR reasoning in *Jaloud v the Netherlands*, where more expansive approach was taken and extraterritorial jurisdiction was established because of the state agents' exercise of authority and control over the individual's right to life, which made their physical proximity non critical. Fourthly, such an approach would ensure equal treatment of all individuals, irrespective of their nationality or physical location. This is because establishing 'virtual control' over someone's communications would not depend on where the interference takes place, but whether or not a state can assert control over an individual's communications, even though it lacks authority or control over the territory, or his physical person. Finally, it could also mean that governments' 'collusion for circumvention' arrangements may fall within their obligations not to interfere with the privacy rights, as they would have an obligation derived from the human rights treaties in relation to the effected rights of all individuals, whose communications fall within their control, inside and outside their territories.

Nevertheless, it still remains unclear how cyber surveillance may trigger the extraterritorial application of human rights law. A number of treaty bodies engaged with the issue of extraterritorial surveillance shortly after the 2013 Snowden disclosures. The Human Rights Committee for example suggested that extraterritorial surveillance does implicate the ICCPR, when addressing the NSA surveillance pursuant to s 702 of FISA conducted through PRISM and Upstream, stating that 'the Committee is concerned about the surveillance of communications in the interest of protecting national security conducted by the National Security Agency (NSA) conducted both within and outside the United States'. [1252] The United

[1249] Jordan J. Paust, 'Can You Hear Me Now? Private Communications, National Security and the Human Rights Disconnect' (2015) 15(2) Chicago Journal of International Law, p. 625.
[1250] Ilina Georgieva, 'The Right to Privacy Under Fire-Foreign Surveillance Under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31(80) Utrecht Journal of International and European Law p. 104.
[1251] ibid.
[1252] UN HRC, 'Concluding Observations on the Fourth Periodic Report of the United States of American' (April 2014) UN Doc CCPR/C/USA/CO/4, para 22.

Nations Office of the High Commissioner also addressed extraterritorial surveillance noting that:

> [d]igital surveillance […] may engage a State's human rights obligations if that surveillance involves the [s]tate's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example through direct tapping or penetration of that infrastructure. Equally, where the [s]tate exercises regulatory jurisdiction over a third party that physically controls the data, that [s]tate also would have obligations under the Covenant.[1253]

Similarly, Special Rapporteur Ben Emmerson QC observed that:

> [s]tate's jurisdiction is not only engaged where [s]tate agents place data interceptors on fibre-optic cables travelling through their jurisdictions, but also where a [s]tate exercises regulatory authority over the telecommunications or internet service providers that physically control the data.[1254]

These approaches seem to broadly correspond with the legal scholarship articulating jurisdiction being triggered on the basis of states' control over the individual's rights to privacy. However, they leave unanswered the question of what degree of control is necessary to establish that a state exercises 'power or effective control in relation to digital communications infrastructure'. In *Jaloud* the ECtHR indicated its approach to the issues of authority and control based on the actual exercise of such powers over an individual's rights. Whether or not it will apply this, or similar approach to the pending surveillance cases remains to be seen.

There can be no doubt that as currently defined, the 'effective control' test of extraterritorial jurisdiction is not well suited for application to cyber surveillance operations. Cyberspace is a transnational environment where information is deliberately routed through a number of jurisdictions to reach its destination. When interference is conducted remotely, physical control over an area, or an individual ceases to be relevant. At the very least, it leaves a gap that intelligence agencies can exploit to circumvent the obligations under the human

[1253] UN GA, 'Report of the Office of the United Nations High Commissioner for Human Rights the Right to Privacy in the Digital Age' (2014) UN Doc A/HRC/27/37, para 34.
[1254] UN HRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC' (2014) UN Doc A/69/397, para 41.

rights treaties through the use of intelligence sharing agreements. What becomes important in this context is the 'virtual control' over the individuals' right to privacy, notwithstanding where they are located, or their nationality. How these obligations may apply to cases of cyber surveillance remains unclear, especially bearing in mind the 'inevitable ripple effects on other scenarios such as extraterritorial use of lethal force through for example drone strikes'[1255] if a more permissive approach to this issue were to be adopted. This makes the task of the Human Rights Committee when drafting new general comment on Article 17, discussed in Chapter 5 of this thesis, particularly challenging.

Therefore, a strong case can be made for the extraterritorial application of human rights treaties to cyber surveillance. Arguably, similar analysis applies to transborder data searches by the LEAs. Since these activities may too trigger human rights obligations under the international human rights framework, the next part will consider whether access to data by the LEAs of the state parties to the Cybercrime Convention also breaches their human rights obligations.

2. Transborder Access to Data as a Violation of the Right to Privacy

The European Court of Human Rights case law in relation to breach of the right to privacy under Article 8 ECHR in the context of the law enforcement (LEAs) acting within the territory of their own states is well established and recently consolidated in *Zakharov v Russia* [1256] and *Szabo v Hungary*,[1257] discussed in the previous part of this chapter. This part of the chapter will show that in a situation, where LEAs of one state capture external communications of another, international obligations under the ICCPR, ECHR and Convention 108[1258] are also triggered and may amount to a violation.

The legality of transborder searches of protected digital data by the LEAs without recourse of MLAs has not yet been examined by the ECtHR. However, the Court will consider a similar issue relating to interception of external communications, including on the internet

[1255] Marko Milanovic 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR' (2016) EJIL: Talk! < https://www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/>.
[1256] supra note 132.
[1257] supra note 133.
[1258] supra note 4.

in *Bureau of Investigative Journalism and Alice Ross v UK.*[1259] The matter has already been addressed by the ECtHR in *Liberty v UK*[1260] in the context of telephone and electronic telecommunications conducted by the UK Ministry of Defence (MoD) between 1990-97 on the basis of the Interception of Communications Act 1985. The Act granted virtually unfettered discretion to the MoD to capture external communications and conferred a wide discretion on the extent, to which these communications could be listened to, or read. However, the statute did not indicate with sufficient clarity the scope, or manner of exercise of the discretion and was therefore not 'in accordance with the law' under Article 8(2). The Court emphasized that:

> 'in accordance with the law' requires that the impugned measure should not only have some basis in domestic law, but also that such basis should be compatible with the rule of law and accessible to the person concerned 'who must moreover, be able to foresee its consequences for him.[1261]

The Court held that the the Act did not indicate:

> with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the [s]tate to intercept and examine external communications [….] and in particular, it did not, as required by the Court's case law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.[1262]

As a result of this ruling, the mere existence of legislation providing for interception of communications, including outside state's territory, which allows for secret monitoring amounts in itself to an interference with Article 8 irrespective of any measures actually taken. Worthy of note is the fact that the Court applied the same conditions under Article 8 to this type of interceptions and did not consider that separate procedural rules from those articulated in *Weber* should apply to the interception of external communications.

[1259] *Alice Ross v UK*, supra note 170.
[1260] *Liberty v UK*, supra note 114.
[1261] ibid, para 59.
[1262] ibid, para 69.

It is submitted that these principles are applicable to transborder searches under Article 32(b) Cybercrime Convention and by way of court orders served on an ISPs, because the operational methods of data gathering by the LEAs resemble those conducted on the basis of the Interception of Communications Act 1985 in *Liberty v UK*. Therefore, they too are likely to amount to interference with the right to privacy of communications protected in Article 8 ECHR and 17 ICCPR. First, these types of interceptions fall within the scope of 'private life' and 'correspondence' (*General Comment 16, Estrella v Uruguay*, *Wieser v Austria*[1263]). In *Wieser,* the ECtHR made it clear that Article 8 applies to data stored by private companies. The issue of legal obligation on the part of an ISP to divulge to the police the personal details attached to an IP address without the consent of the subscriber is currently under consideration by the ECtHR in *Benedict v Slovenia*[1264] and *Ringler v Austria*.[1265] Secondly, the transmission of the obtained data to other authorities has been recognized as representing a further, separate interference with that rights in *Weber.*[1266] Both Article 8(2) and 17 ICCPR dictate that an interference, such as that exercised via Article 32(b), may be justified if it is 'in accordance with the law', necessary and proportionate[1267] Thus, in *Halford*[1268] a telephone interception was held not to be in accordance with the law because 'domestic law did not provide any regulation of the interception of calls'. In *MM v United Kingdom*,[1269] the Court found a violation of Article 8 ECHR because there existed no statutory system to regulate surveillance powers, whilst the guidelines applicable at the relevant time were neither legally binding nor directly publically accessible. These observations pertain Article 32(b) searches. Until the Snowden exposures in 2013, the scale of the intrusion of the LEAs into personal data under the control of data processor in other jurisdictions was not commonly known, let alone the legal frameworks authorizing this. In fact, they seem to be deployed in a domestic legal vacuum and

[1263] *Wieser v Austria* (2008) 46 EHRR. The Court considered that the search and seizure of electronic data constitute an interference with applicants' right to respect for their 'correspondence' within the meaning of Article 8. Having regard to […] the case law extending the notion of 'home' to a company's business premises, the Court sees no reason to distinguish between the first applicant, who is a natural person and the second applicant, which is a legal person, as regards the notion of 'correspondence'.
[1264] *Benedict v Slovenia* (App. No. 62357/14), Communicated to the Respondent Government in April 2015.
[1265] *Ringler v Austria* (App. No. 2309/10) Communicated to the Respondent Government in May 2013.
[1266] *Weber and Saravia v Germany* (2006) (App. No. 54934/00), para 79.
[1267] General Comment No.16; *Donoso; Escher; Malone; Liberty; Halford; MM v UK; Zakharov*.
[1268] *Halford v UK*, supra note 113, para 50-51.
[1269] *MM v United Kingdom* (2012) (App. No. 24029/07).

as such, do not fulfill the criteria of public availability, foreseeability and scope of operations, including the nature of offences and procedural safeguards. Equally, the searches are difficult to justify on the grounds of necessity and proportionality. The evidence from the Cybercrime Committee suggests that the transborder searches and 'data pulling' seem to be unrestricted, thus providing LEAs virtually unfettered discretion, as long as the transfers are pursuant to criminal investigations. Yet, in *Zakharov*,[1270] the ECtHR emphatically stated that blanket access to all information, without specifying particular reasons, the categories of persons and crimes, which also lack supporting evidence to be reviewed by an independent authority, do not fulfill the requirements of necessity and proportionality. Of particular note in this context is also the case of *Digital Rights Ireland*,[1271] where the Court of Justice of the European Union (CJEU) annulled Directive 2006/24/EC,[1272] which set out rules for the retention of metadata by private companies for the purposes of their later use by law enforcement agencies. The Luxemburg Court observed that the mere retention, even if the data were never used, interfered with the fundamental right to privacy under the European Charter of Human Rights (Article 7). It was accepted however that the retention for the purposes of their subsequent transmission to the competent national authority satisfied the objective of fighting crime and public security, but did not comply with the principle of proportionality.

In addition to the protection of the right to privacy of individuals under the ECHR, Council of Europe Convention 108 offers guarantees specifically with regard to automatic processing of personal data. The Convention entered into force in 1985 and has been signed and ratified by 45 out of 47 member states of the Council of Europe, as well as some non-members such as Uruguay. It is the first binding international instrument, which protects individuals against abuses that may accompany the collection and processing of personal data and seeks to regulate the transfrontier flow.[1273] The Convention's scope of application relates to all fields of automated personal data processing and therefore relates to data protection in the area of police and criminal justice.[1274] The purpose of the Convention is to 'secure in the

[1270] *Zakharov*, supra note 132.
[1271] *Digital Rights Ireland*, supra note 168.
[1272] Parliament and Council Directive 2006/24, 2006 O.J. (L105) 54 (EC).
[1273] Council of Europe, Details of Treaty 108, <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.
[1274] Explanatory Report, ETS 108, Automatic Processing of Personal Data Convention, para 33, art 3 – Scope:

> [a]ccording to paragraph 1 the convention applies to the public as well as the private sector. Although most international data traffic occurs in the private sector, the convention is nevertheless of great importance for the public sector and this for two

territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, in particular his right to privacy, with regard to automatic processing of personal data relating to him'.[1275] Restrictions on the rights under the Convention are possible only if higher interests are at stake, such as state's security and defense. In 2001 an Additional Protocol was adopted and introduced provisions on transborder data flows to non-parties.[1276] The Protocol describes transborder data flows as transfers of personal data to a recipient that is subject to the jurisdiction of a state, or organization that is not Party to the Convention,[1277] such as the US. It stipulates that transborder transfers of data may only take place if states ensure an adequate level of protection for the intended data transfer. The ECtHR has referred to Convention 108 on several occasions and highlighted the concordance between the extensive interpretation of 'private life' under Article 8 ECHR and that under Article 1 of Convention 108.[1278] The Court's case law interpreting Article 8 ECHR therefore complements Convention 108. This can be seen in Article 5 of Convention 108, which sets out the principle of the lawfulness of automatic processing of data, but without defining what constitutes unlawful processing, which must be read in the light of what constitutes the interference permitted by the ECHR.[1279]

It follows that, since what constitutes interference under Article 5 of Convention 108 must be read in conjunction with Article 8 ECHR as interpreted by the ECtHR jurisprudence, it could be concluded that it is likely that transborder searches of protected data by the law enforcement agencies without the recourse to the MLA breach Article 5 of Convention 108.

---

reasons. First, Article 3 imposes obligations on the member [s]tates to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country.'

[1275] Convention 108, supra note 4, art 1.

[1276] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, CETS No. 181, 2001.

[1277] ibid, art 2.

[1278] *Amann v Switzerland* supra note 121; *Rotaru v Romania* (2000) (App. No. 28341/95); *Haralambie v Romania* (2009) (Application No. 21737/03).

[1279] European Court of Human Rights, 'National Security and European Case-Law, Report of the Council of Europe Research Division' (2013) <https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20(final).pdf>.

PART IV: CYBER SURVEILLANCE AS AN INTERFERENCE WITH THE RIGHT TO PRIVACY OF COMMUNICATIONS

Reports on NSA and GCHQ activities exposed three substantial ways in which the US and UK governments (together with other partners from the Five Eyes) are possibly infringing the right to privacy under the ICCPR, ECHR and the ACHR. These are (1) the gathering, examining and storing of emails (PRISM); (2) tapping underwater fibre-optic cables, thus intercepting all internet traffic routed via the UK (Tempora); and (3) recording digital and telephone metadata (Fairview and Bondless Informant). There are no decided cases thus far from the HRC, the ECHR, or the IACtHR pronouncing on the issue of legality of these measures. Nevertheless, the 'post-Snowden' decisions by the European Court of Human Rights in *Zakharov* and *Szabo*, together with those of the Court of Justice of the European Union in *Digital Rights Ireland* [1280] and *Maximillian Schrems v Data Protection Commissioner* [1281] shed important light on the issue. Furthermore, UN General Assembly Resolution 68/167[1282] and a number of important Reports on international and regional levels have all unequivocally condemned mass surveillance and bulk collection of electronic communications.[1283] These developments will now be considered as a good indicator of the direction that the global policy pertaining the legality of cyber surveillance may be taking.

1. UN General Assembly Resolution 68/167

Following the Snowden disclosures in 2013, the General Assembly, being deeply concerned that electronic surveillance, interception and collection of personal data may negatively impact human rights, has adopted by consensus Resolution 68/167, *The Right to Privacy in the Digital Age*, strongly supporting the right to privacy and calling on all countries to take measures to end activities that violate this 'fundamental tenet of a democratic

[1280] *Digital Rights Ireland*, supra note 168.
[1281] *Schrems*, supra note 167.
[1282] UN GA Resolution, *Right to Privacy in Digital Age* (21 January 2014) UN Doc A/Res/68/167; see also UN GA, Resolution *Right to Privacy in Digital Age* (10 February 2015) UN Doc A/Res/69/166; UN GA, Resolution *Right to Privacy in Digital Age* (16 November 2016) UN Doc A/C.3/71/L.39/Rev.1.
[1283] OHCHR Report, supra note 270; Report of the Special Rapporteur Ben Emmerson QC, supra note 271; Parliamentary Assembly of the Council of Europe, 'Mass Surveillance', supra note 6.

society'. [1284] The Resolution emphasizes that 'unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy and to freedom of expression.' [1285] Deep concern was also expressed 'at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights'.[1286] The Resolution called upon all states 'to protect the right to privacy, including in the context of digital communications' [1287] and to that end, to 'ensure that relevant national legislation complies with their obligations under international human rights law'.[1288] Further, the Resolution requested the then United Nations High Commissioner for Human Rights, Dr. Navanethem Pillay, to submit views and recommendations to the General Assembly and the Human Rights Council on 'the right to privacy in the context of domestic and extraterritorial surveillance', including 'on mass scale',[1289] discussed next.

2. The Report of the UN High Commissioner for Human Rights

The Report, titled *The Right to Privacy in the Digital Age,*[1290] was published on 30 June 2014. The High Commissioner warned that globally, 'mass surveillance [is] emerging as a dangerous habit rather than an exceptional measure'.[1291] It also reaffirmed that government surveillance must respect the right to privacy and made a number of vital points on the issue, including that (a) mass surveillance constitutes an interference with privacy; (b) as does the collection and interception of metadata; as well as (c) their retention. Each of these points will be outlined in more detail below.

[1284] UNGA Resolution 68/167, supra note 299.
[1285] ibid, p. 2.
[1286] ibid.
[1287] ibid.
[1288] ibid.
[1289] ibid, p. 3.
[1290] OHCHR Report, supra note 270.
[1291] ibid.

a. *Mass Surveillance Necessarily Interferes with Privacy*

Having recalled the HRC General Comment 16, which requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*, the High Commissioner concluded that 'any capture of communications data is potentially an interference with privacy',[1292] 'the mere possibility' of communications being captured creates an interference with privacy and 'the very existence of a mass surveillance programmes thus creates an interference with privacy.'[1293] The High Commissioner based these observations on the ECtHR jurisprudence in such cases as *Malone*[1294] (interception was interpreted to include 'either targeted or mass surveillance of communications, the recording or bugging of an individual's telephone communications and interference with postal mail), *Liberty*[1295] (mass monitoring or recording of public telecommunications, including telephone, facsimile and email) and *Copland*[1296] (interception and storage of emails).

b. *The Interception or Collection of Metadata Interferes with the Right to Privacy*

The High Commissioner's Report rejected the claim that 'the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy'.[1297] The High Commissioner was explicit on this point, stating that 'the aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication'.[1298] Dr Pillay supported this point by referring to the recent landmark judgment of the CJEU in *Digital Rights Ireland*.[1299] The significance of this case stems from it being a successful challenge to the validity of the European Union (EU) 2006 Data Retention Directive. The Directive's main objective was to harmonize EU member states' provisions concerning the retention of certain

[1292] ibid, para 20.
[1293] ibid.
[1294] *Malone v UK*, supra note 112.
[1295] *Liberty v UK*, supra note 114.
[1296] *Copland v UK*, supra note 118.
[1297] OHCHR Report, supra note 270, para 19.
[1298] ibid.
[1299] ibid.

data, which are generated or processed by providers of publicly available electronic communications services or of public communications networks.[1300] It contained a mandatory data retention framework, whereby all Internet Service Provides (ISPs) and telecommunication service provides operating in Europe were compelled to collect and retain such information as a subscriber's incoming and outgoing telephone numbers; IP addresses; date, time and duration of communication; type; equipment used for the communication; location and other key data. These data were to be retained for period of between six months to two years. However, the content of communications was excluded from the ambit of the Directive. The information was to be gathered in order to assist the prevention, investigation, detection and prosecution of serious offences, such as organized crime and terrorism. The Directive not only lacked safeguards limiting governments' collection and access to individuals' data, but also omitted controls over what information can be used. The Irish High Court and the Austrian Constitutional Court asked the CJEU to examine the validity of the Directive, in particular in the light of the two rights under the Charter of the Fundamental Rights of the EU, namely the right to respect for private life and the protection of personal data (Article 7 and 8 respectively). In declaring the Directive invalid, the CJEU ruled that the bulk retention of 'all traffic data' relating to 'all means of electronic communication' from 'practically the entire European population, including those in respect of whom there was no suggestion that they had a connection, ever indirect, or remote, with serious crime',[1301] interfered in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.[1302] The fact that data were retained and subsequently used without the subscriber being informed, was likely to generate in the persons concerned a feeling that their lives were the subject of constant surveillance. The CJEU then examined whether such an interference with the fundamental rights was justified. The Court acknowledged that the retention of data for the purposes of their possible transmission to the competent national authority genuinely satisfied an objective of general interest, i.e. the fight against serious crime and ultimately public security.[1303] However, by adopting the Directive, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality.

[1300] Court of Justice of the European Union, Press Release, 'The Court of Justice Declares the Data Retention Directive to Be Invalid' (8 April 2014) <http://www.curia.eruopa.eu.>.
[1301] *Digital Rights Ireland*, supra note 168, paras. 56-58.
[1302] ECJ Press Release, supra note 317, p. 1.
[1303] ibid. p. 2.

c. *Retention of Data Amounts to Interference*

The OHCHR Report also rejected the view that the right to privacy is only interfered with, when a state accesses, consults, or uses the data that it collects. Accordingly, 'even the mere possibility of communications information being captured creates an interference with privacy'.[1304] This conclusion is in keeping with the Strasbourg Court case law. The Court has consistently held that not only the interception, but also storage of communication constitutes interference with the right to privacy.[1305] It did not matter that the database of the surveillance information did not contain any sensitive information about the applicant's private life.

3. UN Special Rapporteur

In September 2014 the UN Special Rapporteur Ben Emmerson QC presented his Report to the UN General Assembly.[1306] Building on the work of his predecessors, Martin Scheinin[1307] and Frank La Rue,[1308] his Report is categorical in finding that bulk access to communications, mass surveillance of content and metadata, its retention and the use of automated mining algorithms with no prior suspicion or any legal/executive authorization amounts to 'systematic interference with the right to respect of the privacy of communications and requires a correspondingly compelling justification'.[1309] Furthermore, the Report emphasized that 'the use of mass surveillance technology effectively does away with the right to privacy of communications on the internet altogether'.[1310] It also recalled that the UN General Assembly Resolution 69/167 confirmed the legal right to respect for the privacy of digital communications and therefore 'the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right'.[1311] Noting that the 'very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right

[1304] OHCHR Report supra note 270, para 20.
[1305] UN HRC General Comment No.16, supra note 85; *M.K. v France*, supra note 129; *Brunet v France*, supra note 130; *Shimovolos v Russia*, supra note 127.
[1306] Report of the Special Rapporteur Ben Emmerson QC, supra note 271.
[1307] UN HRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009) UN Doc A/HRC/13/137.
[1308] UN HRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) UN Doc A/HRC/23/40.
[1309] Report of the Special Rapporteur, Ben Emmerson QC, supra note 271, para 9.
[1310] ibid, paragraph 12.
[1311] ibid, paragraph 18.

to privacy', the Report concluded that 'it is incompatible with the existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to privacy of communications is that infringements must be exceptional and justified on a case-by-case basis'.[1312] The Report therefore put an onus 'on those states deploying bulk access surveillance technologies to explain promptly, precisely and publicly, why this wholesale intrusion into collective privacy is justified for the prevention of terrorism or other serious crime'.[1313]

4. The Council of Europe

In the already mentioned report of the Commissioner for Human Rights of the Council of Europe *The Rule of Law on the Internet and in the Wider Digital Age*,[1314] it was noted that European data protection law is founded on a set of basic principles and remedies that are 'special reflection of the general rule of law principles developed by the European Court of Human Rights'. [1315] The report observed that revelations of Edward Snowden made it 'increasingly clear that massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security'.[1316] It further considered that 'such interferences can only be accepted if they are strictly necessary and proportionate to a legitimate aim'.[1317]

In another report, that of the Committee on Legal Affairs and Human Right issued in 2015 and titled, *Mass Surveillance* serious concerns were likewise expressed about mass surveillance and large scale intrusion practices disclosed since June 2013 by Edward Snowden.[1318] In particular, the report noted the development in several countries (including the Five Eyes) of 'massive surveillance-industrial complex, which risks escaping democratic

---

[1312] ibid.
[1313] ibid, paragraph 19.
[1314]Council of Europe Commissioner for Human Rights, Nils Muižnieks, 'The Rule of Law on the Internet and in the Wider Digital World' (2014), p.18 <http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf>.
[1315] ibid, p. 16.
[1316] ibid.
[1317] ibid, p 17.
[1318] Committee on Legal Affairs and Human Rights, Pieter Omtzigt, 'Mass Surveillance' (18 March 2015) Doc 13734.

controls and accountability and threatens the free and open character of our societies'.[1319] The Committee was not only of a view that the surveillance practices endanger fundamental rights, including the right to privacy under Article 8 ECHR. It expressed deep concernes about the threats to internet security by the practices of certain intelligence agencies of seeking out systematically, using and even creating 'back doors' and other weaknesses in security standards and implementation, which could easily be exploited by terrorists, cyberterrorists and other criminals.[1320] Recognizing the need for transatlantic cooperation to fight terrorism and other organized crimes, the Committee stressed that this must be based on mutual trust and respect for human rights and the rule of law. This can only be achieved by rebuilding trust through putting into place a legal and technical framework at national and international level, which in particular protects the right to privacy.[1321] The Report made a number of proposals regarding the regulation of intelligence and law enforcement agencies activities on a regional level, which will be further discussed in Chapter 5.

5. The IACHR Special Rapporteur

On 27 June 2014 the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights released a report titled *Freedom of Expression on the Internet.*[1322] The Report's main concern was freedom of expression. It therefore identified four guiding principles that states should follow, when developing the digital environment, namely access, pluralism, non-discrimination and privacy. The last guiding principle of privacy is closely related to Article 11 ACHR and obliges states to both respect the privacy of individuals and to make sure that third parties do not act in ways that could arbitrarily affect that right.

6. The Court of Justice of the European Union

In 2015 the Court of Justice of the European Union declared in another of its landmark rulings, *Schrems v Data Protection Commissioner*[1323] that data transfers of EU citizens from Facebook

[1319] ibid, page 1.
[1320] ibid.
[1321] ibid.
[1322] Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, 'Report of the Special Rapporteur Freedom of Expression and the Internet' (31 December 2013) OEA/Ser.L/V/II.
[1323] *Schrems,* supra note 167.

European subsidiary, under the US Safe Harbour scheme are not safe and should be suspended on the ground that the US does not afford adequate level of protection of personal data. The case was referred to the CJEU by Maximilian Schrems, who complained that following the Snowden exposures in relation to the activities of the NSA, his Facebook data transferred from the Irish subsidiary to the US for processing is unsafe, as the US law does not offer sufficient protection against surveillance by the public authorities of data transferred to that country.[1324] Of particular note was the Court's finding that US national security, public interest and law enforcement requirements prevail over the safe harbour agreement, so that the US companies are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with these requirements.[1325] As such, the scheme enables interference by the US public authorities with the fundamental rights of the Europeans. The Court also held that the process of transfer of all EU citizens' data to the US was beyond what was necessary and proportionate to the protection of national security. The legislation authorizing the transfers was not limited to what was strictly necessary, as it authorized on a generalized basis storage of all of the personal data of all the persons without any differentiation, limitation or exception being made. Furthermore, the persons concerned had no administrative or judicial means of redress enabling in particular the data relating to them to be accessed, rectified, or erased. The Court therefore declared the safe harbour scheme invalid. It has since been replaced by another non-legally binding agreement, called the Privacy Shield, addressed in Chapter 5.

7. The Legal Contours of the Interference with the Right to Privacy of Digital Communications

Drawing from the above jurisprudence and soft law sources, some basic parameters can be set out regarding what constitutes interference with privacy of digital communications. This includes:

a) interception of data by public authorities of every form of communications, including electronic email (HRC General Comment 16, HRC Concluding Observations on Sweden, *Liberty*);
b) use, sharing and storage of data (*Leader*, *Weber*, *Amann*, *Marper*, *Estrella v Uruguay*,);

[1324] Court of Justice of the European Union, Press Release No. 117/15 (6 October 2015) <www.curia.europa.eu>.
[1325] ibid.

c) either targeted (*Malone*), or mass surveillance of communications, including email (*Liberty* and *Copland*);
d) bulk collection and retention of metadata by service provides in order for it to be passed on to government authorities (*Digital Rights Ireland*);
e) the mere existence of legislation allowing secret surveillance (*Klass, Kennedy, Weber, Zakharov*);
f) interception of personal information pertaining to the telephone and internet usage, including both content and metering (*Malone*, *Copland*, *Liberty*, *Klass, Escher v Columbia*);
g) all nature of correspondence- not only purely personal- business, or professional type may constitute part of an individual's private life (*Kopp, Donoso v Panama*);
h) systematic collection and storage of information by authorities on databases (HRC General Comment 16, *M.K v France* and *Brunet*) as well as on so called 'surveillance databases' (*Shimovolos*);
i) the 'pulling' of data based on Article 32(b) of the Cybercrime Convention by the law enforcement agencies from servers located in another country without formal mutual assistance arrangements, may be incompatible with Article 8 ECHR, Article 17 ICCPR and Article 1 Convention 108;
j) untargeted search of all electronic data (*Robathin*);
k) the transfer of personal data of all EU residents by social sites, such as Facebook, to US servers under the now invalidated Safe Harbour Agreement violates the right to privacy, as it does not provide sufficient level of protection of personal information (*Schrems v Data Protection Commissioner*);
l) the retention by service providers of all traffic and location data to make it available for the purposes of the investigation, detection and prosecution of serious crime by LEAs constitutes an interference with private life and the right to protection of personal data (*Digital Rights Ireland*);
m) domestic legal framework providing for secret interception of all mobile phone communications violates Article 8 (*Zakharov, Szabo).*

Assessed against these principles it can be concluded that it is highly likely that (a) the gathering, examination and storage of emails under the PRISM interception programme constitute interference with the right to privacy (HRC General Comment 16, HRC Concluding Observations on Sweden, *Liberty*, *Leader*, *Weber*, *Amann*, *Marper* and *Estrella v Uruguay*,);

(b) interception of all internet traffic (both internal and external) routed via the UK on the basis of the Tempora programme likewise interferes with the right to privacy (*Liberty* and *Copland);* (c) as does recording of digital and telephone metadata pursuant to Fareview and Bondless Informant (*Malone, Digital Rights Ireland)*. Support for these conclusions can also be found in the above-mentioned Reports from the Human Rights Commissioner, the UN Special Rapporteurs and the Report of the Council of Europe Committee on Legal Affairs and Human Rights, all relaying on the ICCPR and ECHR and their respective jurisprudence and concluding interference with the protected right. It is worth reiterating that the Reports robustly condemn electronic surveillance, in particular observing that capture, collection, retention and even the mere possibility of communication being captured creates an interference with privacy, with a potential chilling effect on other rights, including those of expression and association,[1326] not to mention the very existence of a mass surveillance programmes, which in itself creates interference. There has been no suggestion from the OHCHR, or the Special Rapporteurs however that the surveillance is inherently incapable of justification. Indeed, the onus would be on the state to demonstrate that such interference is neither arbitrary, nor unlawful[1327] and according to Ben Emmerson QC any justification would have to be compelling.[1328] This is subject of consideration in the next part of this chapter.

PART V: JUSTIFICATIONS

The right to privacy is subject to legitimate limitations, which means that if a state successfully shows that the restriction is within the prescribed limits, that restriction would be permissible and not amount to violation. Whether or not the interference with privacy of both domestic and foreign surveillance activities by the Five Eyes intelligence agencies may be justified must be assessed in accordance with the provisions of Article 17 ICCPR, Article 8 ECHR and Article 11 ACHR.

[1326] OHCHR Report, supra note 270, para 20; Special Rapporteur Ben Emmerson QC supra note 271; CoE Commissioner Report, supra note 6.
[1327] ibid.
[1328] Special Rapporteur, Ben Emmerson QC, supra note 271, para 9.

1. Limitations: Articles 17 ICCPR, 8 ECHR and 11 ACHR

According to Article 17 ICCPR an interference with an individual's right to privacy is only permissible under international human rights law if it is neither unlawful, nor arbitrary.
In contrast with other ICCPR provisions (for example Article 19), Article 17 does not spell out the elements for a test of permissible limitations. Nevertheless, such permissible limits have been considered to be similar to other enumerated limitations in the ICCPR.[1329] Moreover, the HRC set out some parameters with regard to states' ability to interfere with the right to privacy. First, any interference authorised by states can only take place on the basis envisaged by the law, which itself must comply with the provisions, aims and objectives of the Covenant.[1330] This means that the interference that is permissible under national law may still be unlawful if that law is in conflict with the provisions of the ICCPR.[1331] Secondly, the law which allows for interference must be precise and circumscribed, so as not to give decision makers too much discretion in authorising interference with privacy.[1332] Thirdly, the interference must be authorised only by the authority designed under the law and solely on a case –by-case basis.[1333] The term 'arbitrary interference' in Article 17 was interpreted by the HRC by introducing the concept of reasonableness. The Committee stated that arbitrary interference must not be unreasonable and explained that:

> [it] can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[1334]

[1329] Joseph and Castan, supra note 86, p. 538.
[1330] General Comment No. 16, supra note 85; para 3:
> [n]o interference can take place except in case envisaged by the law. Interference authorised by [s]tates can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.

[1331] OHCHR Report, supra note 270, para 21.
[1332] General Comment No. 16, supra note 85; para. 8:
> '[e]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated by the law and on a case-by-case basis'

[1333] ibid.
[1334] ibid. para 4.

The notion of reasonableness was also elaborated on in the case of *Toonen v Australia*,[1335] where the HRC stated that it 'interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.[1336] The requirement of proportionality has not been directly addressed though by the HRC in the context of Article 17. However, in its General Comment 27 the Committee commented on the nature of permissible restrictions and made the following observations in respect to the requirement of proportionality:

> […] restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected […] The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.[1337]

Thus, it could be said that a state may in principle interfere with the privacy of individuals, but only if (a) the interference takes place pursuant to detailed national legislation; (b) where it is authorised by a relevant authority on a case-by-case basis; (c) it is not arbitrary; (d) reasonable in particular circumstances and (e) proportional to the ends sought. The requirements of reasonableness and proportionality are closely related and in the context of the HRC's interpretation of Article 17, both seem to imply that a restriction may only be put in place in least intrusive manner and if absolutely necessary.

Unlike Article 17 ICCPR, Article 8(2) ECHR enumerates the grounds, which allow states to place limitations on privacy rights. The Article permits public authority to interfere with that right, provided such interference is 'in accordance with the law', 'necessary in a democratic society' and in pursuit of 'legitimate aims'. The 'legitimate aims' under Article 8(2) are- national security; public safety or the economic well being of the country; prevention of disorder or crime; protection of health and morals and the protection of the rights and freedoms of others.

[1335] *Toonen v Australia* (488/92)
[1336] ibid, para 8.3.
[1337] UN HRC, 'General Comment No. 27, Freedom of Movement (Art 12)' (2 November 1999) UN Doc CCPR/C/21/Rev.1/Add. 9, paras. 14 and 15.

In similar manner to Article 17 ICCPR, Article 11(2) of the American Convention on Human Rights also refers to 'arbitrary' or 'abusive' interference with private life. It does not contain an explicit clause justifying restrictions, nevertheless limitations are implied in the provisions of that Article and would be authorised by the Inter-American Commission.[1338] The Inter American Court of Human Rights interpreted the scope of Article 11(2) in a number of cases. In *Donoso v Panama*[1339] the IACtHR stated that in order to be non-abusive and non-arbitrary, any state restrictions on the right to privacy must 'serve a legitimate purpose and meet the requirements of suitability, necessity and proportionality which render [them] necessary in a democratic society'.[1340] In *Donoso*[1341] and *Escher v Columbia*[1342] judgments the Court has also confirmed that there is a legality requirement, which means that restrictions must be 'statutorily enacted'. Moreover, in the context of law authorising the interception of telephone communications, the IACtHR held that such law 'must be precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorised to request it, to order it and to carry it out and the procedures to be followed'.[1343] The Inter American Commission has been influenced in its approach by the decisions of the ECtHR.[1344] Both the Inter American Court and the Inter American Commission made it clear that any discretion given to the State has to be construed narrowly.[1345]

In summary, the approaches to limitations of privacy right outlined above share three common features, namely that (a) the interference must be in accordance with the law; (b) it must serve a legitimate aim and (c) be necessary in a democratic society. In addition, the Strasbourg Court and the HRC consider the issue of proportionality of the interference in securing the legitimate aim as central to the determination of legality. The question that will now be addressed is whether the interference with the right to privacy through the use of cyber surveillance programmes may be justified on these bases.

[1338] ibid.
[1339] D*onoso v Panama*, supra note 178.
[1340] ibid, paragraph 56.
[1341] ibid.
[1342] *Escher v Columbia*, supra note 179, para 130.
[1343] ibid, paragraph 114.
[1344] ibid.
[1345] *Steve Clark v Granada*, Case 10.325, Report No. 2/96, IACHR, OEA/Ser.L/V/II.91 Doc. 7 at 113 (1996).

a. ‘In Accordance with the Law’

The first requirement is that the restriction imposed on the right to privacy is ‘in accordance with the law’, which will only be met when three conditions are satisfied: (a) the impugned measure must have some basis in domestic law; (b) the quality of the law must be such as to be accessible to the person concerned and (c) must have foreseeable consequences

i. Legal Basis

The requirement that the interference with privacy can only occur if conducted pursuant to national laws have been confirmed by the three courts- the HRC, IACtHR and ECtHR.

The HRC in its General Comment 16 observed that ‘[t]the term ‘unlawful’ means that no interference can take place except in cases actually envisaged by the law. In addition, any interference authorised by [s]tates can only take place on the basis of law that itself must comply with the provisions, aims and objectives of the Covenant.’[1346]

The IACtHR in *Donoso* and *Escher* cases likewise stated that any restriction must be statutorily enacted. In *Donoso* the IACtHR observed that:

> [t]he right to privacy is not an absolute one and so, it may be restricted by the [s]tates provided that their interference is not abusive or arbitrary; accordingly, such restriction must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity and proportionality which render it necessary in a democratic society.[1347]

Applying these conditions to the facts in *Donoso,* the IACtHR held that the Panamanian State, due to the lack of adequate, accurate and clear legislation to regulate interference with telephone communications, failed to fulfil its obligation to adapt its domestic legislation to secure the right of Mr. Donoso not to be subjected to arbitrary interference with his private life.

[1346] General Comment No.16, supra note 85, para 3.
[1347] *Donoso v Panama,* supra note 178, para 56.

On the European level, the Strasbourg Court similarly concluded that any interference with privacy must be on the basis of domestic laws.[1348] For example in *Malone*, the UK government surveillance activities were performed under a broad set of administrative rules. The Court was not clear what legal standards applied and disapproved of the UK government's ability to change the parameters of its surveillance activities as it saw fit. The ECtHR stressed that the law must indicate the scope of any discretion with regard to the interception of communications and the manner of its exercise with sufficient clarity to give an individual protection against arbitrary interference.

Public admissions as to the existence of PRISM, Tempora, Upsteam and Boundless Informant are rarely made by government officials, not to mention the legal basis pursuant to which they operate.

The existence of PRISM and Upstream have been officially confirmed by the US government[1349] to be operated on the basis of the US FAA s 702 (US Code §1881(a) and the Executive Order 12333. The FAA adopts different rules for international communications depending on whether the target of the surveillance is a United States person or non-United States person.[1350] Thus, if the government targets a US person who may be both inside and outside of the US, the surveillance is permissible only if it is intended to acquire foreign intelligence information and if the Foreign Intelligence Court (FISC) issues a warrant based on a finding that there is a probable cause to believe that the US person is an agent of a foreign power.[1351] However, when the target of foreign intelligence surveillance is a non-US person who 'is reasonable believed to be located outside the United States', the government need not have probable cause to believe that the target is an agent of a foreign power and need not obtain an individual warrant from the FISC, even if the interception takes place inside the US.[1352] In fact, s 702 authorises the FISC to approve annual certifications submitted by the Attorney General and the Director of National Intelligence that identify certain categories of foreign intelligence targets whose communications may be collected, subject to FISC-approved targeting and minimisation procedures, that is procedures that must be 'reasonably designed

[1348] *Malone v UK*, supra note 112, paragraph 67; *Huvig v France* (1990) (App. No. 11105/87), para 28; *Krusin v France* (1990) (App. No. 11801/85), para 27; *Khan v the United Kingdom*, (2000) (App. No. 35394/97), para. 26.
[1349] The White House, Office of the Press Secretary, 'Remarks by the President of Review of Signals Intelligence' (17 January 2014) <https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.
[1350] The NSA Report, supra note 189, p. 86.
[1351] ibid.
[1352] ibid.

[…] to minimize the acquisition and retention and prohibit the dissemination of unpublicly available information concerning unconsenting Unites States persons'.[1353] The categories of who may be target of interception are broad and the certifications typically specify international terrorists and individuals involved in the proliferation of weapons of mass destruction.[1354] Reports as to how s 702 powers have been used in practice attest that this type of surveillance does lack legitimate legal basis. For example, according to the 2014 report on Privacy and Civil Liberties Oversight Board Hearing on Section 702 of the FISA Amendment Act:

> [t]he surveillance under FAA [is not] predicated on probable cause or an individualised suspicion. The targets need not be agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the [US] government to target any foreigner located outside of the US so long as the pragmatic purpose of the surveillance is to acquire 'foreign intelligence information'.[1355]

This gives the US government sweeping authority to monitor the communications of foreigners abroad. However the targeting and the minimization procedures indicate that the US authorities had implemented these powers in a manner that guarantees that the NSA will acquire and retain purely domestic communications as well on the basis of s 702.[1356] The former NSA director Keith Alexander publically acknowledged that the NSA uses s 702 data not only for the purposes of foreign information gathering, but also to access Americans' communications without a warrant through a 'back door search loophole' using 'US personal identifiers', for example email addresses associated with someone in the US.[1357] This means that the US is using a statute that was intended to permit broad access to American's international communications as a tool to engage in wide surveillance of American's purely domestic

[1353] 50 U.S.C §§ 1801 (h) (1), 1821 (4) (A).
[1354] ibid.
[1355] American Civil Liberties Union, 'Privacy and Civil Liberties Oversight Board Hearing on Section 702 of the FISA Amendment Act' (19 March 2014) <http://www.ohchr.org/Documents/Issues/Privacy/ACLU2.pdf >.
[1356] ibid.
[1357] Ron Wyden, Senator for Oregon, 'Wyden, Udall on Revelations that Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act Loophole' (1 April 2014) https://www.wyden.senate.gov/news/press-releases/wyden-udall-on-revelations-that-intelligence-agencies-have-exploited-foreign-intelligence-surveillance-act-loophole

communications.[1358] A similar sweeping access to communications of Europeans has been declared as not 'in accordance with the law' in *Digital Rights Ireland* case.[1359] There the CJEU held that although the aim of the Data Retention Directive might have been legitimate, its implementation was not proportionate to the intended objective. This is because the Directive failed to stipulate clear and precise rules on the extent of the interference with the protected rights, as it applied to all traffic data and all users of all modes of electronic communications for an unspecified length of time. It was also not sufficiently specific about the conditions of data storage and the obligations of the security agencies accessing the data. Likewise, the broad powers under s 702 that are used to intercept communications of US and non-US persons alike do not 'indicate the scope of any legal discretion conferred on the competent authority and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference'.[1360] Such use of s 702 is therefore highly likely not to fulfil the requirement of 'in accordance with the law'.

Even more oblique then the NSA use of s 702 is its surveillance on the basis of the Executive Order 12333 (EO), as amended. The original EO 12333 was signed by President Ronald Regan in 1981 and established broad new surveillance authorities for the intelligence community outside the scope of public law.[1361] It has been amended three times (by the EO 13284 in 2003, EO 13555 in 2004 and EO 13470 in 2008).[1362] The EO 12333 is said to serve often as an alternative basis of authority for surveillance activities, above and beyond s 702 FAA.[1363] Indeed, little is known even to the US state officials how the NSA uses the EO 12333 to conducts its surveillance operations abroad. For example, Senator Dianne Feinstein, the Chair of the US Senate State Intelligence Committee commented in 2013 that '[the Intelligence Committee] does not receive the same number of official reports on other NSA surveillance activities directed abroad pursuant to legal authorities outside of FISA (specifically Executive Order 12333), but I intend to add to the [C]ommittee's focus on those activities'.[1364] The extent

[1358] American Civil Liberties Union, supra note 372.
[1359] *Digital Rights Ireland*, supra note 168.
[1360] *Malone*, supra note 112, para 67.
[1361] Electronic Privacy Information Centre, 'Executive Order 12333' <https://epic.org/privacy/surveillance/12333/>.
[1362] supra note 188.
[1363] supra note 378.
[1364] United States Senator for California, Diane Feinstein, 'Feinstein on NSA Compliance' (16 August 2013) < https://www.feinstein.senate.gov/public/index.cfm/2013/8/feinstein-statement-on-nsa-compliance>.

of the collection and storage of communications of both Americans and foreigners pursuant to the EO 12333 is simply not known.[1365]

Tempora is authorised by certificates issued under s 8(4) of RIPA, granted to GCHQ, which relates to 'external communications', i.e. communications that are either sent or received outside the British Islands. GCHQ has confirmed that Tempora has 10 'basic' certificates, which creates a 'broad, overall legal authority, which has to be renewed at intervals'.[1366] These include a global certificate, which gives GCHQ authority to intercept any transatlantic cable data, as long as the purpose of the intercept falls within one of a number of very broad categories, such as terrorism, organized crime and the economic well-being of the UK.[1367] This is the basis of a legal challenge of GCHQ cyber surveillance in the case currently pending before the ECtHR of *Big Brother Watch v UK*.[1368] The applicants argue that the UK surveillance measures are not in accordance with the law, because the law permits blanket monitoring of external communications provided that one party is outside the British Isles.[1369] In addition, the certificates are often framed only in very broad terms (usually referencing national security grounds), with no reference to the scope, or duration of the interception. As such, the 'generic interception of external communications by GCHQ merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables is an inherently disproportionate interference with the private lives of thousands, perhaps millions of people'.[1370]

Based on the available information and official admissions from governments, it could be said that at least some of the programmes of the Five Eyes (such as PRISM, Upstream and Tempora) have been and continue to be run pursuant to the domestic legal frameworks, which have been published. Their purpose is so broadly defined, that they fail to provide the precise basis for the interception and no grounds whatsoever for the receipt, analysis, use and storage of data received from foreign intelligence agencies. However, there is also a whole host of

---

[1365] see for example John Napier Tye,'Meet the Executive Order 12333: The Reagan Rule that Lets the NSA Spy on Americans' (18 July 2014) < https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.e2177132821a >. Tye, a former Obama State Department Official, called for greater scrutiny of the EO 12333.

[1366] Ewan MacAskill, Julian Borger, Nick Hopkins, Nick Davis and James Ball, 'The Legal Loophole that Allow GCHQ to Spy on the World' (21 June 2013) *The Guardian*.

[1367] *Big Brother Watch v UK*, supra note 171, p. 14.

[1368] ibid.

[1369] ibid.

[1370] ibid, at Complaints.

other surveillance systems in existence, including MUSCULAR, OPTIC NERVE, MYSTIC, OPERATION SOCIALIST, GEMALTO HACKING and THREE SMURFS (Dreamy, Nosey and Tracker), whose legal bases are obscure and rarely acknowledged by state authorities.

ii. Accessibility

The criteria of 'legal basis' is not just limited to the requirement that the law must be published on national level, but that it meets the standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur.[1371] The Human Rights Committee stressed in its General Comment 16 that legislation authorising interference with private communications 'must specify in detail the precise circumstances in which such interference may be permitted.'[1372]

This approach is also reflected in the case law of the ECtHR, according to which for domestic law to be accessible, it must give an individual an indication of the applicable legal rules,[1373] that have to be sufficiently precise, detailed and foreseeable.[1374] Thus, in *Silver v United Kingdom*,[1375] specific orders and instructions given to by the British Home Secretary to prison governors did not meet the accessibility test because they were not published and therefore not available to the prisoners, nor was their content explained. In *Malone*, the ECtHR stated that national laws must indicate the scope of the discretion conferred on the competent public authority and the 'manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference'.[1376] Similarly, in *Huvig v France* the ECtHR observed that national laws must indicate 'with reasonable clarity the scope and manner of exercise of the relevant discretion of public authorities in exercising an intrusive power'.[1377] Furthermore, the Court mindful of the role that surveillance may play in undermining privacy, has developed a robust set of principles relating to how national legislation has to ensure lawful surveillance. These principles were set out in the core of the Court's case law concerned with interception of communications and wiretapping (albeit prior to introduction of mass cyber surveillance programmes), including

[1371] Report of the Special Rapporteur Ben Emmerson QC, supra note 271, para 36.
[1372] General Comment No. 16, supra note 85, para 8.
[1373] *Sunday Times v the United Kingdom* (1979) (App. No. 6538/74), para 47.
[1374] *Vogt v Germany* (1996) (App. No. 17851/91).
[1375] *Silver and Others v United Kingdom* 1983) (App. No. 5947/ 72), paras 87-93.
[1376] *Malone,* supra note 112, para 68.
[1377] *Huvig,* supra note 365, para 35.

the already referred to cases of *Huvig*, *Malone*, *Klass*, *Kopp*, *Khan*, *Copland*, and recently reaffirmed in *Zakharov*. In essence, the national laws under which interferences, including surveillance of communications, may be legitimate shall define: (a) the categories of people liable to have their communications monitored; (b) the nature of the offences which may give rise to an interception order; (c) limits on the duration of such monitoring; (d) the procedures to be followed for examining, using and storing the data obtained; (e) precautions to be taken when communicating the data to other parties; and (f) circumstances in which data obtained may or must be erased or the tapes destroyed.[1378]

Viewed in the light of these detailed rules, mass surveillance programmes significantly challenge the accessibility requirements of Articles 17 ICCPR, 8 ECHR and 11 ACHR. These criteria have not been met, as the domestic laws (such as FAA and RIPA) fail to set out the scope of the discretionary powers of the NSA and GCHQ, nor is the manner of their activities outlined in any detail. In the UK, there is no legislation (or other legal provisions) that can be said to give 'citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort' to the measures.[1379] Further, the legislation seemingly authorising bulk interception programmes, (PRISM, Tempora) neither sets limits to the categories of persons who may be subject to surveillance, nor the duration of the interception. To that end, Ben Emmerson QC observed that the detailed legal and administrative frameworks for mass surveillance often remain classified and little is still publicly known about the ways, in which captured data are operationalized.[1380] Moreover, the programmes often operate under outdated domestic laws, which were designed to deal with more rudimentary forms of

---

[1378] *Huvig*, ibid; *Kruslin v France* (1990) (App. No. 1180/85/), para 35. The ECtHR stated at para. 34 in *Huvig v France* that:

> [a]bove all, the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court. The information provided by the Government on these various points shows at best the existence of a practice, but a practice lacking the necessary regulatory control in the absence of legislation or case-law.

[1379] *Big Brother Watch*, supra note 171, p. 48.

[1380] Report of the Special Repporteur Ben Emmerson QC, supra note 271, para. 37.

surveillance and have not been modified to date to reflect the increased technical capabilities.[1381] In some cases, states have 'intentionally sought to apply older and weaker safeguards regimes to ever more sensitive information'.[1382] In this regard, the UN High Commissioner for Human Rights commented that 'secret rules and secret interpretations-even secret judicial interpretations-of law do not have the necessary qualities of law'[1383] and cannot serve as the basis for the legality of surveillance programmes. Above all, none of the national legislation expressly mentions and therefore authorises cyber surveillance programmes- it is simply admitted (or has not been robustly denied) by the national authorities that they operate pursuant to these statutes.

A recent 2015 UK case, *Liberty v GCHQ*,[1384] heard by the Investigatory Powers Tribunal (IPT) confirmed that the country's national legal framework authorising cyber surveillance breaches the requirement of accessibility. The issue before the IPT was the legality of intelligence sharing operations between the UK and the US of electronic communications intercepted in bulk. The challenge was brought by Liberty, Privacy International and other civil liberties groups, who claimed that GCHQ's receipt of private communications intercepted by the NSA through mass surveillance programmes, PRISM and Upstream, was illegal. The IPT declared that 'the regime governing the soliciting, receiving, storing and transmitting by the UK authorities of private communications of individuals located in the UK, which have been obtained by the US authorities pursuant to PRISM and/or Upstream contravened Articles 8 or 10 [of the ECHR]'.[1385] The IPT stated that the government's regulations were illegal because the public were unaware of safeguards that were in place and that the details of those safeguards were only revealed during the legal challenge at the IPT. However, the ruling appears to suggest that the illegality related to those operations which were conducted between 2007-2014 and that GCHQ's access to NSA intelligence was lawful from that time onwards because secret policies governing the UK-US relationship were made public. Liberty disagrees that the limited safeguards revealed during the IPT proceedings are sufficient to make GCHQ's mass surveillance and intelligence sharing lawful and has challenged the Tribunal's decision at the ECtHR, which is now pending decision.

[1381] ibid.
[1382] ibid.
[1383] OHCHR, Report supra note 270, para 29.
[1384] *Liberty and Others v the Security Services* (6 February 2015) IPT/13/77/H.
[1385] Investigatory Powers Tribunal, List of Judgments, <http://www.ipt-uk.com/section.aspx?pageid=8>.

iii. Foreseeability

Foreseeability requires that national law must be 'sufficiently clear in terms of providing citizens with adequate indication of the circumstances and conditions in which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence'.[1386] In *Doegra v the Netherlands*[1387] the ECtHR stated that a rule is foreseeable 'if it is formulated with sufficient precision to enable the person concerned-if need be with appropriate advice- to regulate his conduct'.[1388]

When applying these principles to the relevant provisions of the RIPA and FAA Acts, it appears that this condition, in similar vein to the accessibility criteria, has been disregarded too, both in relation to domestic and foreign surveillance.

In the UK, section 8(4) RIPA provides that interception warrants do not have to specify a person or premises, if they refer to the interception of communications outside the UK and if an authorising certificate has been issued by a Secretary of State. This seems to be the basis upon which the UK Government authorises GCHQ to run Tempora. This inevitably introduces an element of unforseeability, for the interception is both indiscriminate and deliberately unpredictable. The statutory regime that applies to the external communications warrants breaches this criteria because the restrictions and safeguards that apply to internal authorisations are not applicable to external warrants and are not approved by a judge or an independent authority, whether before or after they have been issued.[1389] Furthermore, the safeguards in RIPA that relate to external warrants are deficient. For example, the 'national security' basis upon which the warrants are granted do not define with any precision the nature of the offences that may give rise to an interception or examination of communications, or the categories of people liable to have their communications intercepted. There is no effective limit on the interception and the law does not set out the procedures to be followed for examining the communications or the precautions to be taken when supplying them to third parties, such as the NSA.[1390] The circumstances, in which the communications must be destroyed, whilst specified, are so broad as to effectively permit the retention of enormous amounts of intercepted information, which means that they do not meet the criteria relating to interception

[1386] *Malone*, supra note 112, para 67.
[1387] *Doerga v the Netherlands* (2004) (App. No. 50210/99).
[1388] ibid, para. 50.
[1389] *Big Brother Watch*, supra note 171, p. 49
[1390] ibid, p. 54.

of external communications as set out in *Liberty* v *UK* and therefore are incompatible with Article 8.

However, the blanket surveillance of foreign communications under s 8(4) RIPA is only part of the problem relating to the UK laws giving surveillance powers. Whilst the critical piece of legislation authorising interception is RIPA, there are other parallel statutory frameworks in place, which authorise interception and acquisition of communications data within the UK, without the same degree of attention, analysis and oversight as RIPA.[1391] Among them, the Wireless Telegraphy Act 2006 (WTA), which by sections 48 and 49 grants the Secretary of State and the Commissioners of Revenue and Customs very broad powers to authorise the interception of wireless and other communications.[1392] In principle both RIPA and WTA may be used to intercept the same communications.[1393] Other non-RIPA powers of public authorities and law enforcement agencies stem from some 65 different statutory mechanisms authorising 46 different public bodies to have access to, or require production of communications data,[1394] for example the Telecommunications Act 1984 s. 94.[1395] As regards these powers, David Anderson QC observed that there is little, or nothing in the public domain that explains how frequently they are used and that at least some or perhaps many agencies and departments exercise these powers without any published codes of practice in place. When recommending consolidation and reform to the UK government, Anderson stated that 'obscure laws-and there are few more impenetrable than RIPA and its satellites-corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean'.[1396] Similar conclusion was reached by the recent Independent Surveillance Review, commissioned in March 2014 by the then Coalition Government to assess the legality, effectiveness and privacy implications of UK surveillance programmes by the Royal United Services Institute (RUSI). The Report, titled *A Democratic Licence to Operate*, published in July 2015 highlighted the inadequacies in law and oversight

---

[1391] David Anderson QC, 'A Question of Trust. Report of the Investigatory Powers Review', (June 2015), para. 6.9 p. 97 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf>.

[1392] ibid.

[1393] ibid.

[1394] ibid.

[1395] Telecommunications Act 1984, s. 94 grants the Secretary of State a power to give 'directions of a general character' to an individual to the extent that they are 'necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom'.

[1396] David Anderson QC, supra note 408, para 13.31, p. 252.

and urgently called for new legislation to provide an up to date democratic mandate for digital intelligence. It concluded that the present arrangements are too complex to be understood by the citizen and have contributed to the public credibility gap that must be addressed.[1397] The Review set out ten tests that any legislation must pass before it can be regarded as giving the police and the intelligence services a democratic licence to operate, namely the rule of law, necessity, proportionality, restraint, effective oversight, recognition of necessary secrecy, minimal secrecy, transparency, legislative clarity and multilateral cooperation.[1398]

[1397] Royal United Services Institute for Defence and Security Studies, 'A Democratic Licence to Operate. Report of the Independent Surveillance Review' (2-15 July 2015) ISSN 1750-9432.

[1398] ibid. p.104. The ten tests for the intrusion of privacy that any new legislation or regulation must be seen to pass before the UK Parliament are:

1. rule of law: all intrusion into privacy must be in accordance with law through processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.
2. necessity: all intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.
3. proportionality: intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgment that the degree of intrusion is matched by the seriousness of the harm to be prevented.
4. restraint: it should never become routine for the state to intrude into the lives of its citizens. It must be reluctant to do so, restrained in the powers it chooses to use, and properly authorized when it deems it necessary to intrude.
5. effective oversight: an effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials and ministers to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.
6. recognition of necessary secrecy: the 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.
7. minimal secrecy: the 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of their employees) and all other aspects of their work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters.
8. transparency: how the law applies to the citizen must be evident if the rule of law is to be upheld. Anything that does not need to be secret should be transparent to the public; not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands.
9. legislative clarity: relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date

There also seems to be a disregard for foreseeability in the framework of the US FAA, s 702 relating to gathering information on a suspected overseas targets.[1399] Any foreign national outside the US can be a target of surveillance under s 702 FISA as long as the government's purpose is to obtain foreign intelligence.[1400] The Act fails to provide any criteria whatsoever or clarification of the grounds for the interception. It therefore seems that a reasonable belief by the intelligence/security agencies that a person is abroad may trigger a one-year spying authorisation.[1401]

b. Legitimate Aim- National Security

The general principle under the provisions of ECHR is that once a court is satisfied that any restriction has legal basis, i.e. meets the requirement of 'in accordance with the law', it will go on to consider whether the restriction is for one of the specified aims. Similar position is taken under the ICCPR and ACHR, although unlike the second paragraph of Article 8, Articles 17 and 11 do not enumerate specific grounds for limitations.

In justifying cyber surveillance programmes the governments of the Five Eyes often rely on the national security grounds, particularly fighting or preventing the terrorism threat. As already mentioned, the interests of national security have been expressly recognized in Article 8(2) ECHR and in the ECtHR case law. Thus, in *Klass*, the Strasbourg Court accepted that secret surveillance measures fall within the national security exception, since democratic societies find themselves threatened by highly sophisticated forms of espionage and terrorism and need to undertake secret surveillance to counter such threats.[1402] However, in *Weber* the Court emphasised that employing secret surveillance in the fight against terrorism and espionage for the sake of national security may undermine, or even destroy democracy therefore it requires adequate safeguards against abuse. The Special Rapporteur Ben Emmerson QC, whilst agreeing that preventing terrorism is clearly a legitimate aim, emphasised that the

---

and are accessible to citizens, the private sector, foreign governments and practitioners alike.

10. multilateral collaboration: government policy on intrusion should be capable of being harmonized with that of like-minded open and democratic governments.

[1399] Anitai Etzioni, 'NSA-National Security v Individual Rights' (2015) 30 Intelligence and National Security), pp. 101-136.
[1400] Georgieva, supra note 267, p.120
[1401] ibid.
[1402] ibid, p. 316.

activities of intelligence and law enforcement agencies must still comply with international human rights law.[1403] It is difficult to disagree with Emmerson's view that 'merely to assert-without particularization-that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human right law justification for its use. The fact that something is technically feasible and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful'.[1404] The question that arises in this context is therefore how effective are mass surveillance programmes in preventing and fighting serious crime and terrorism, addressed next.

i. The Effectiveness of Cyber Surveillance Programmes in Fighting Terrorism

Shortly after the flood of revelations regarding surveillance activities of the NSA came to the fore, President Obama's administration hastened to defend them as legal and essential to US national security and counterterrorism. During his 2013 Berlin visit the President himself declared that at least 50 terrorist threats have been averted and lives have been saved.[1405] In addition, General Keith Alexander, the then director of the NSA, testified at the hearing of the US House Intelligence Committee that:

> [t]he programmes are immensely valuable for protecting our nation and securing the security of our allies. In recent years the information gathered from these programmes provided the US government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world. FAA 702 contributed in over 90 percent of these cases. At least 10 of these events included homeland-based threats. In the vast majority, business records, FISA reporting, contributed as well.[1406]

Also the Representative Michael Rogers, in the same hearing before the Congress stated that

---

[1403] Special Rapporteur Ben Emmerson QC, supra note 271, para. 11.
[1404] ibid.
[1405] *Huffington Post*, 'Obama Says NSA Programs Saved Lives' (19 June 2013) <http://www.huffingtonpost.com/2013/06/19/obama-nsa-programs_n_3464425.html>.
[1406] Office of the Director of National Intelligence, 'Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries' (18 June 2013) <http://icontherecord.tumblr.com/post/57812486681/hearing-of-the-house-permanent-select-committee-on>.

'54 times [the NSA programmes] stopped and thwarted terrorist attacks both here in Europe-saving real lives'.[1407] Other supporters of electronic mass surveillance programmes claim that they significantly contributed to tracking Bin Laden[1408] and led to significant decline in Al Qaeda's electronic communications.[1409]

Notwithstanding these assurances, the 'terrorism' justification has been soundly rejected as devoid of evidence. In 2013 in *Klayman v Obama*[1410] a federal judge found that the US government was unable to 'cite a single case in which analysis of the NSA's bulk metadata collection actually stopped an imminent terrorist attack'.[1411] President Obama's own Review Group on Intelligence and Communications Technologies admitted that mass surveillance was not essential to preventing terrorist attacks and information used to detect plots could readily have been obtained in a timely manner using conventional court orders.[1412] Furthermore, at least one study, conducted by the New American Foundation in 2014, challenged the claims regarding the effectiveness of mass surveillance and asserted that they are exaggerated, or even misleading. The Study scrutinized the records of 225 individuals recruited by Al-Qaeda and other like-minded groups, such as Al-Shabab, charged with acts of terrorism since 9/11. It demonstrated that traditional investigative methods, such as the use of informants, tips from local communities and targeted intelligence provided the initial impetus for investigations in

---

[1407] ibid.

[1408] Etzioni, supra note 416, p. 110.

[1409] ibid.

[1410] *Klayman v Obama*, 957 F. Supp. 2d. 1 (2013).

[1411] Lawrence Hurley, 'US Court Hands Win to NSA over Metadata Collection' (28 August 2015), *Reuters* < http://www.reuters.com/article/us-usa-court-surveillance-idUSKCN0QX1QM20150828>. The decision that the NSA mass collection of phone metadata was unconstitutional was reversed however by the US Court of Appeals for the District of Columbia on in August 2015.

[1412] Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies, 'Liberty and Security in a Changing World' (12 December 2013), p. 104< https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>. The Report found *inter alia* that: 'NSA believes that on at least a few occasions, information derived from the section 215 bulk telephony meta-data program has contributed to its efforts to prevent possible terrorist attacks, either in the United States or somewhere else in the world. More often, negative results from section 215 queries have helped to alleviate concern that particular terrorist suspects are in contact with co-conspirators in the United States. Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders'.

the majority of cases, while the contribution of the NSA bulk surveillance programmes to these cases was minimal.[1413] In particular, the study found that the surveillance of non-US persons outside the US under s. 702 of the FISA Amendment Act played a role in 4.4% of terrorism cases, whilst surveillance under an unidentified authority played a role in 1.3% of the examined cases.[1414] The Report concluded that the main problem with the approach that officials take to US counterterrorism is not that they need even greater amounts of information from the bulk surveillance programmes, but that 'they do not sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques'.[1415] According to the Report, had the information that the intelligence agencies already had been utilized correctly, in cases of such attacks as the 9/11 and the Mumbai bombings, these and other crimes could have been prevented. Admittedly, the findings of this Report are uncorroborated by other evidence. However, the inescapable conclusion is that even if they were to be dismissed for this reason, mass surveillance and bulk data collection (operational at an unprecedented scale since at least 2007) is disproportionate in the light of the number of attacks and terrorist plots that the US authorities to date admitted they prevented, namely 54.

c. Necessity

Article 8(2) ECHR provides that in addition to being lawful and serving a legitimate purpose, the restriction must be necessary in a democratic society. This requires from a state to show that the action, which it has been taking is in response to a pressing social need and that the interference with the protected rights is not greater than necessary to address that pressing social need. This is also known as test of proportionality. In applying this test, the Strasbourg Court will balance the severity of the restriction placed on the individual against the legitimate aim to be protected.

A similar approach has been adopted by the Human Rights Committee, which in *Canepa v Canada* stated that 'arbitrariness within the meaning of Article 17 is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's

[1413] Peter Bergen, David Sterman, Emily Schneider, Baily Cahall, 'Do NSA's Bulk Surveillance Programs Stop Terrorists?' (13 January 2014), New American Foundation <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf>.
[1414] ibid, p. 2.
[1415] ibid. p. 4.

rights under Article 17 and its compatibility with the purposes, aims and objectives of the Covenant'.[1416]

i. Proportionality

When assessing necessity of having laws granting domestic authorities the powers to act in national security interests, a balance must be struck between the seriousness of the interference and the right to privacy (*Leander v Sweden*[1417]). In other words, the measure in question must by proportionate to the aims achieved. In striking this balance the Strasbourg Court has allowed states a broad margin of appreciation and elaborated on how proportionality should be assessed through a number of cases. In *Leaden,* for example the Court accepted that states should enjoy wide discretion, both in assessing the existence of a pressing social need and in choosing the means of achieving the legitimate aim of protecting national security.[1418] Similarly, in *Klass,* the ECtHR agreed with the fact that the sophistication of modern terrorism mandated some secret surveillance over post and telecommunications necessary in exceptional circumstances. Therefore, it permitted a degree of discretion to the national legislature with respect to organizing and controlling such systems. This however does not mean that states are allowed an unlimited license of interception. Rather, they must satisfy the Court that adequate and effective safeguards are in place. In *Peck v U.K.* the Strasbourg Court stipulated that the margin of appreciation enjoyed by national authorities in the exercise of surveillance powers depends on the nature and seriousness of the interest at stake and the gravity of the interference.[1419]

According to the sources leaked by Snowden, NSA and GCHQ have the technical ability and capacity to access, store and analyze huge volumes of communications between entirely innocent people, as well as targeted suspects derived from, among other methods, the tapping of fibre-optic cables. Britain's technical capacity to access world's communications has allegedly made GCHQ an intelligence superpower, which by 2010 was able to boast the biggest internet access of any member of the Five Eyes alliance.[1420] Tempora alone is said to

---

[1416] *Giouse Canepa v Canada*, Communication No. 558/1993, UN Doc CCPR/C/59/D/558/1993 (1997), para. 11.4.
[1417] *Leander v Sweden*, supra note 120.
[1418] ibid, paragraph 59.
[1419] *Peck v the United Kingdom* (2003) (App. No. 44647/98), para. 77.
[1420] Ewan MacAskill, Julian Gorger, Nick Hopkins, Nick Davis and James Ball, 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications' (21 June 2013) *The Guardian*.

give access to 2 billion internet users globally each day and additional technical work is ongoing to expand its capacity to ingest data from new super cables carrying data at 100 gigabites a second.[1421] GCHQ's justification for collecting this information all the time is to combat sophisticated forms of terrorism, as well as against child exploitation networks and in the field of cyber defence.[1422] In particular, GCHQ officials claim that it has directly contributed to the arrest and imprisonment of a terrorist cell in the Midlands, who were planning coordinated attacks, the arrest of five Luton based individuals plotting acts of terror, as well as the arrest of three London based would- be attackers targeting the Olympics.[1423] At first blush, assessed in the light of the *Klass* judgment, these successful preventative measures seem to give reasons for the government to resort to 'secrete surveillance of subversive elements'.[1424] Bearing in mind that the internet has been increasingly used by terrorist organizations for communication, propaganda, research, planning, publicity, fundraising and recruiting purposes,[1425] GCHQ, the NSA and their partner agencies, may well be acting within the broad margin of appreciation that the courts allow. After all, they need to keep in line and abreast of the nefarious activities of terrorist and criminal groups, which have increasingly been taking place on-line. It is also true to say that the body of jurisprudence from the ECtHR has on occasions deemed surveillance legislation both compatible and proportionate with the human rights obligations. For example in *Weber*, the Strasbourg Court found that the German statute in question (the 'G 10') did not violate Article 8 because a series of conditions were satisfied including the factual indications relating to suspecting a person of planning, committing or having committed certain serious criminal offences.[1426] The Court emphasized however, that the so-called 'exploratory' or general surveillance is not permitted.[1427] In *Weber* only a small percent of communications were intercepted and the surveillance was limited to a precise number of specified countries.[1428] This was reiterated in *Zakharov*-mass surveillance is not allowed, being disproportionate and unnecessary. State authorities must have 'reasonable and verifiable suspicion about the person concerned', including factual indicators before an interception warrant is granted. Even if it were accepted that PRISAM and Tempora operate

[1421] ibid.
[1422] ibid.
[1423] ibid.
[1424] *Klass v Germany*, supra note 111, para. 48.
[1425] Ian Brown and Douwe Dorff, 'Terrorism and the Proportionality of Internet Surveillance' (2009) 6(2) European Journal of Criminology, p. 119.
[1426] *Weber v Germany*, supra note 283, para. 110.
[1427] ibid.
[1428] ibid.

for the legitimate purpose of national security and fall within the wide margin of discretion needed due to the increased terrorist attacks committed in Europe in the past few years, the surveillance under these programmes does not seem to be restricted to particular individuals, groups, or even countries. As they lack any specified targets, they do not meet the *Zakharov* criteria of reasonable and verifiable suspicion, process vast amounts of data and run for unspecified duration. For these reasons the operation of Tempora by GCHQ has been challenged on the grounds of being disproportionate and (as discussed above for lacking legitimate basis) in *Big Brother Watch*. The application, currently before the ECtHR, states that:

> [i]ntercept[s] of communications simply because of the means by which [they have] been transmitted [are] excessively broad and insufficiently linked with the ostensible purposes for which such intercept[s] occur[s]. For example, communications sent by persons and from locations not under suspicion are intercepted and then subjected to the search machinery, rendering their communications liable to be further analyzed, reported upon and subject to further action.[1429]

Official justifications regarding proportionality of bulk collections are very rare. One of such statements is from the UK Intelligence and Security Committee of Parliament (a body responsible for holding all UK security intelligence agencies to account) to the Independent Surveillance Review, according to which:

> GCHQ bulk interception capability is used primarily to find patters in, or characteristics of, online communications, which indicate involvement in threats to national security. The people involved in those communications are sometimes already known, in which case valuable extra intelligence may be obtained […] In other cases, it exposes previous unknown individuals or plots that threaten our security which would not otherwise be detected.[1430]

However, this statement viewed from the perspective of the parameters laid down in General Comment 31, *Canepa v Canada, Leanden, Weber, Klass and Zakharov* (to name but a few

[1429] *Big Brother Watch*, supra note 171, p. 61.
[1430] The RUSI Report, supra note 414, p.19.

legal authorities), indicates that GCHQ's bulk interception described above bears all the hallmarks of exploratory surveillance, rather then targeted surveillance- the exact opposite of what the ECtHR and other human rights courts and bodies deems as proportionate.

ii. Existing Legal Safeguards

The assessment of necessity for foreign surveillance measures would not be complete without taking into account existing legal safeguards against abuse, since the judicial bodies, such as ECtHR takes a holistic approach to reaching the decisions when considering the legality of state surveillance. In *Klass,* the ECtHR stated that it:

> [m]ust be satisfied that, whatever system of surveillance is adopted, there exists adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise them and the kind of remedy provided by the national law.'[1431]

In *Telegraph Media Nederland Landelijke Media BV v the Netherlands,* the ECtHR stated that 'in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole it is in principle desirable to entrust supervisory control to a judge'.[1432] Two aspects of the domestic powers granting surveillance are of particular note in the light of these observations. First, there appears to be no substantive limitation to restrict the scope of the intelligence agencies' operations. For example, under s 702 of the US FAA there is no restriction on surveillance with regard to non-US persons located aboard. In theory, these could derive from at least two sources- US constitutional protection against unreasonable searches and seizures in the Fourth Amendment[1433] and international law

[1431] *Klass v Germany,* supra note 111, para. 50.
[1432] *Telegraph Media Nederland Landelijke Media BV v the Netherlands* (2012) (Application No. 39315/06), para. 98.
[1433] The right to protection from unreasonable searches and seizures is contained in the Bill of Rights in the Fourth Amendment of the US Constitution, adopted in 1791, which states that:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be

obligations stemming from Articles 17 ICCPR and 11 ACHR. The first category does not offer much hope for non-US persons residing abroad, as the the Fourth Amendment can only be invoked by the US citizens and foreigners, who have developed such ties with the United States that they form part of the national community. This is because the Fourth Amendment was not 'intended to apply to activities of the United States directed against aliens in foreign territory or in international waters'.[1434] Consequently, foreigners subject to the US surveillance abroad, who have no other connections with the United States are, in principle, not entitled to the protection of the Fourth Amendment and will not be able to bring a legal challenge to the unlawful searches and seizures in the US courts.[1435] The second limitation on the scope of s 702 powers is the right to respect the right to privacy in Article 17 ICCPR. This too continues to be robustly rejected the the US administration. First, US specifically declared that Articles 1-27 ICCPR are not self-executing, which means that they do not have any effect in domestic law unless legislation is passed to give them such effect. Secondly, the US denies the Covenant's extraterritorial application, as discussed in the previous part of this chapter. The end result is that non-US persons residing abroad may not rely on the ICCPR in US courts to challenge s 702 powers.

Similar approach has been recently adopted by the UK Investigatory Powers Tribunal (IPT), which overseas the working methods of the intelligence agencies in *Human Rights Watch v the Secretary of State for the Foreign and Commonwealth Office (HRW v Secretary of State).*[1436] The case related to the interception, storage and use of information and communications by GCHQ of two groups of applicants-those resident in the UK and those who were not. Regarding the latter, the IPT ruled that the UK 'owes no obligation under Article 8 ECHR to persons [who] are situated outside its territory in respect of electronic communications between them, which pass through that state'.[1437]

Additionally, a series of criticisms have been directed at the quality of the independent supervision when granting surveillance orders by both the British Investigatory Powers Tribunal (IPT) and the American Foreign Intelligence Surveillance Court (FISC). The FISC

---

seized.

[1434] *United States v Verdugo-Urquidez*, 494, US 259, 269 (1990).

[1435] William Banks, 'Pragmatic Surveillance and FISA: Of Needles in Haystacks' (2010) 88 Texas Law Review, pp. 1656-1657.

[1436] *Human Rights Watch Inc. and Others v The Secretary of State for the Foreign and Commonwealth Office and Others* [2016] ALL ER (D) 105 (May).

[1437] ibid, para 60.

was created in 1987 and its purpose was to hear applications for and grant orders approving electronic surveillance anywhere within the Unites States.[1438] The original intention of the US Congress was the setting up of a system of approving individualized warrants for foreign surveillance of specified individuals in the context of national security. With the passage of s 702 of FAA, these powers have been exponentially extended, resulting in FISA Court approval of mass surveillance. The Court's sphere of competence includes granting of surveillance orders under s 702 (§188a), but there is no requirement for a separate judicial approval of the FISC order for each individual exercise of §1881a. The American defenders of mass surveillance point out that Americans are given special protection, because of the requirement for a FISA court order for a targeted surveillance. Consequently, the procedural safeguards for non-US persons located abroad are considerably weaker then before s 702 FAA was introduced, as there is no need for the authorities to show in each individual case that the target of the acquisition was a foreign power or it's official.[1439] The position was summarized by the former US national intelligence director, James Clapper in these terms:

> Section 702, authorizes surveillance directed at non-US persons located overseas who are of foreign intelligence importance. At the same time, it provides a comprehensive regime of oversight by all three branches of Government to protect the privacy and civil liberties of US persons. Under section 702, the Attorney General and the Director of National Intelligence may authorize annually, with the approval of the Foreign

[1438] Foreign Intelligence Surveillance Act 1978, s. 103(a):

> [t]he Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have juris- diction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this sub- section shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

[1439] James R. Clapper and Eric H. Holder, 'Letter to (US Congress) John Boemer, Harry Reid, Nancy Pelosi and Mitch McConnell About the Re-authorisation of Title VII of the Foreign Intelligence Surveillance Act (FISA) Enacted by the FISA Amendment Act of 2008 (FAA)', (8 February 2012) <https://www.justice.gov/sites/default/files/ola/legacy/2012/11/08/02-08-12-fisa-reauthorization.pdf>.

> Intelligence Surveillance Court (FISC), intelligence collection targeting categories of non-US persons abroad, without the need for a court order for each individual target.[1440]

In other words, the FISA court places no limitations whatsoever in relation to intelligence gathering of non-US nationals abroad (i.e. most of the world's population). It is also not a forum, which will hear complaints about bulk collection. That being the case, both Special Rapporteur Ben Emmerson QC[1441] and the UN High Commissioner for Human Rights[1442] emphasized that states are bound by the ICCPR obligations in the situation, where they penetrate the infrastructure located outside their territorial jurisdictions. In addition, as already noted in this chapter, Article 26 of the ICCPR prohibits discrimination on grounds of, inter alia, nationality and citizenship. As discriminating on the grounds of nationality and/or location does not seem to be justified, states must afford the same privacy protections for nationals, non-national and all those within and outside their jurisdictions. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant.

The UK Investigatory Powers Tribunal (IPT) established under RIPA, is the only judicial body independent of the UK government authorized to hear complaints about surveillance conducted by the intelligence agencies, including GCHQ. It too does not provide an adequate remedy for those, who are neither British citizens, nor residents, as clearly shown by its rejection to hear an interception complaint in *HRW v Secretary of State*.[1443] However, an individual within the UK may file a complaint, which may only concern search operations, or targeted surveillance activities, therefore generalized surveillance programmes, such as Tempora do not qualify to by subject of IPT review.

The conclusion that can be drawn from this analysis is that the legality of the NSA/GCHQ surveillance practices is highly doubtful under international human rights law. There are a number of indicators outlined above, which show that both foreign and domestic cyber surveillance programmes are not 'in accordance with the law', are arbitrary and disproportionate to the aims achieved. In addition, individuals affected by the interference have no meaningful and effective remedies in the domestic courts. Therefore, on the basis of the available information relating to these programmes, successful justification of the interference with the right to privacy of correspondence seems unlikely. It can therefore be concluded that

[1440] ibid.
[1441] Special Rapporteur Ben Emmerson QC Report, supra note 269.
[1442] OHCHR Report, supra note 268.
[1443] supra note 453.

mass bulk collection and interception programmes operated both domestically and abroad interfere with the right to privacy under Article 17 ICCPR, Article 11 ACHR and Article 8 ECHR.

CONCLUSION

Cyberspace has created a means for intelligence and law enforcement agencies to have an unrestricted access to vast amounts of digital information. This chapter focused on two such methods, namely transborder data searches and cyber surveillance techniques. With respect to transborder data searches by law enforcement agencies (LEAs), the chapter noted that many LEAs engage in unrestricted, blanket data cross-border transfers. The Cyber Crime Convention Article 32 has been designed to facilitate this process to a certain extent, but recent evidence shows that it is deficient for a number of reasons. First, the Convention does not specify that the 'lawful consent' must be granted by an appropriate state organ. This leads to unilateral transfers, occasioned by consent of private companies (ISPs). Secondly, it has been shown that the current practice of states tends to ignore official channels of authorisation when exercising enforcement jurisdiction abroad, which breaches the principle of territorial sovereignty and the right to privacy under the ICCPR, the ECHR and Convention 108. However, not all transborder searches breach the territoriality principle and privacy laws. Open source data searches, as provided for in Article 32(a) Budapest Convention are lawful and recognized as part of customary international law. This calls for Article 32(b) Cyber Crime Convention to be reformed and this work is now underway. However, no consensus has yet been reached as to how this provision is to be amended. The chapter also discussed cyber surveillance activities of intelligence services and assessed them in the light of Articles 17 ICCPR, 8 ECHR and 11 ACHR. It argued that mass surveillance programmes interfere with the interests protected under these legal frameworks and therefore pose serious threat to individuals' right to privacy, including of all those individuals who are not within the Five Eyes territories, especially on American, or British soil. The chapter discussed when states may be liable under international law for their surveillance activities, the effect of which may be felt beyond their borders. It illustrated that the narrowly defined territorial limitations on human rights protection based on nationality (e.g. s 702 FISA), or geographical distinctions (s. 8(4) RIPA) are meaningless when applied to highly integrated global communications networks. Although international human rights jurisprudence recognizes that there are certain circumstances when extraterritorial human rights obligations will be engaged based on the 'effective control' test, the chapter has

highlighted its limitations in the cyber domain and proposed a 'virtual control' test, understood as a remote control over an individual's right to privacy. The chapter then considered restrictions on the right to privacy as international and regional human rights treaties recognize that governments have a legitimate interest in limiting this right, especially on the grounds of national security. However, by examining the justifications put forward by some governments (especially the US and the UK) it became apparent that measures they employ lack legal bases and are disproportionate, whilst the claimed contribution to fighting, or preventing terrorism and crime is highly dubious. These findings led to the conclusion that the Five Eyes cyber surveillance practices breach the right to privacy under the ICCPR, ACHR and ECHR. Although the gravity of the problem has been recognized at international and regional levels, with the UN General Assembly passing a number of resolutions on the right to privacy in the digital age, both cyber surveillance and transborder data searches persist. An increasing number of terrorist attacks in recent years propel governments to enact more powers of surveillance on a domestic level to show that they are discharging their duties as far as national security protection is concerned. This does not align well with the pro-privacy views taken by international human rights organizations, NGOs and other groups and calls for solutions to mass surveillance and greater protection of human rights online, which will be discussed in the next chapter.

Chapter 5: 'International Legal Solutions to State Mass Cyber Surveillance'

INTRODUCTION

One of the starkest lessons that can be learned from the 2013 Snowden disclosures is the need for a global legal solution regarding surveillance. Chapter 4 of this thesis unequivocally demonstrated that cyber surveillance breaches international human rights law and that so far the key states engaged have not made a convincing case to justify the continued operation of their mass surveillance programmes. Despite numerous calls from the UN international organizations and human rights courts and bodies condemning these practices, there is no consensus to date on how to bring them in line with human rights law. This is partly due to the continued lack of agreement as to the future of internet governance and the focus on cyber security, which does not prioritize human rights protection. In addition, in recent years the emerging state practice shows decisive tendencies towards greater securitization as a response to the malignant terrorist attacks. This creates a clear gap between the international institutions calling on states to take decisive action to comply with their human rights obligations on the one hand and many governments clearly in favour of continuing mass surveillance, on the other hand. The aim of this chapter is to bridge this gap.

There are a number of technical and legal safeguards that can be implemented. The former, known as privacy-enhancing technologies are at the forefront of technological measures reducing privacy risks and consists of policy, encryption, filtering and anonymity tools to improve users' privacy control and remove unnecessary personal identifiers from sent data.[1444] These technical methods are beyond the scope of this chapter, which will focus on five legal options, namely (a) the adoption of new hard law instruments on an international and (b) regional levels; (c) updating and supplementing the existing privacy norms under Article 17 ICCPR and Article 8 ECHR; (d) harmonizing data protection laws; (e) continued use of soft

[1444] Rolf H. Weber and Dominic N. Staiger, 'Privacy versus Security. Identifying the Challenges in a Global Information Society', in Joanna Kulesza and Roy Balleste (eds.), *Cybersecurity and Human Rights in the Age of Surveillance* (Rowman and Littlefield 2016), p. 78.

law instruments and confidence building measures. The chapter is divided into two parts. Part one analyses a governance model based on a multilateral, international cyber security treaty regulating state-to- behaviour in cyberspace in relation to all forms of harmful cyber operations falling below the use of force threshold under Article 2(4) Charter of the United Nations. This option reflects the governance structures proposed in Chapter 3 of this study based on the UN Law of the Seas Convention 1982 (UNCLOS), in particular the application of the principle of the Common Heritage of Mankind (CHM) to the internet and considers how international human rights framework may fit into this discourse. This part also puts forward another hard law instrument, regional in scope, which aims to specifically regulate economic and political cyber espionage. Such a multilateral 'no-spy' treaty, called the Intelligence Codex, was proposed by the Council of Europe in 2015 to regulate intelligence gathering activities among European states and to date remains the only tangible response from an international organization that attempts to address mass surveillance.[1445] This part of the chapter evaluates the feasibility of these two hard law solutions coming to fruition. It also discusses Universal Periodic Review Mechanism and the need for updating privacy norms under the existing international law instruments, focusing on Article 17 ICCPR and Article 8 ECHR. In addition, it emphasises the need for greater harmonization of data protection rules and identifies the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[1446] (Convention 108) as the best candidate to set a global benchmark in this regard. Part two focuses on a complementary approach to address the problem of surveillance and data transfers through soft law instruments. It identifies the advantages of non-legally binding guidelines and agreements on the UN and regional levels, such as the new Privacy Shield. It also discusses the use of diplomatic means to curtail untargeted mass surveillance though confidence building measure for cyberspace.

The picture that emerges is of a legal landscape that is highly fragmented, comprising outdated privacy laws and peppered with international and regional non-legally binding instruments of varying importance and utility. The lack of international regulation of signals intelligence gathering, the continued disagreements among the international community regarding the future stewardship of the internet and the trends towards the adoption of more surveillance

[1445] Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, Resolution 2045 (21 April 2015).

[1446] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, in force 1 October 1985 ETS 108.

powers on a domestic level all point to the conclusion that there are no 'quick fixes' to the problem of mass surveillance. Having evaluated the various options, the chapter concludes that the most realistic solution must be through a combination of updating the existing international and domestic privacy laws, continued 'globalization' of Convention 108 and the use of diplomacy to encourage a negotiated agreement. This may in future lead to the development of an international hard law instrument to regulate state behaviour in cyberspace (including mass untargeted surveillance) and/or to the eventual emergence of customary law norms in this area.

PART I: REGULATION OF STATES' ACTIVITIES IN CYBERSPACE THROUGH A HARD LAW INSTRUMENT

A. International Level

a. Solution 1- An International Legally Binding Treaty for Cyberspace Based on the UN Law of the Sea Convention 1982 and the Common Common Heritage of Mankind

Treaties, defined in Article 2(2) of the Vienna Convention on the Law of Treaties 1969 as '[a]n international agreement between [s]tates in written form and governed by international law'[1447] are, beside customary international law, the main sources of obligations. They are express agreements among states, whereby the participating parties bind themselves legally and are expected to fulfil their commitments, in line with the principle of *pacta sunt servanda*.[1448]

The efforts to construct a global coordination and policy making framework for the internet begun in the mid- 1990s and to date remain unsuccessful.[1449] There is no single state, or international body formally in overall charge of ensuring compliance with the law in respect

[1447] Vienna Convention on the Law of Treaties, 23 May 1969, United Nations Treaty Series, vol. 1155, p. 331, art 2(2).
[1448] Vaughan Lowe, *International Law* (Oxford University Press, 2011), pp. 64-65.
[1449] Milton Mueller, et al., 'The Internet and Global Governance: Principles and Norms of a New Regime' (2007) 13 Global Governance 237.

of the way the internet works.[1450] Nor is there an overall treaty applicable to the internet, although as already mentioned in Chapter 2 there are international and regional treaties together with national laws that are applicable to the activities on the internet.[1451] Some states, including France[1452] and Russia[1453] made a number of attempts to introduce a cyber security treaty in the 1990s. The Shanghai Cooperation Organization (SCO) proposed such an instrument twice- in 2011 and 2015. The treaty, known as the *Draft Code of Conduct for Information Security*, [1454] was to set out the rules of the road in respect to such issues as cyber crime, cyber espionage, hostile activities or acts of aggression, proliferation of information weapons and related technologies.[1455] However, as discussed in Chapter 2, a global agreement to this treaty is unlikely.

There is no doubt that the Snowden disclosures of government sponsored mass surveillance added a further layer of distrust among the international community, which makes reaching an agreement on how to reduce mass surveillance problematic. One conceptual solution, which advocates protecting the internet in the interest of the present and future generations, originally proposed in 1997,[1456] was recently reiterated in the UN by the Republic of Malta. This solution, discussed in Chapter 3 of this study, sees the stewardship of cyberspace based on the premise

---

[1450] Council of Europe Commissioner for Human Rights, 'The Rule of Law on the Internet and in the Wider Digital World' (2014) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806da51c > p.36

[1451] see Chapter 2 of this thesis, p. 61.

[1452] Kristen Eichensehr, 'The Cyber-Law of Nations', (2015) The Georgetown Law Journal, p. 355. In 1996 France proposed a 'Charter for International Cooperation on the Internet'.

[1453] ibid. In the late 1990s Russia circulated a draft 'arms control treaty for cyberspace' among UN Security Council members but the United States and its allies dismissed the draft treaty.

[1454] UNGA, 'Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the UN Addressed to the Secretary General' (2011) UN Doc A/66/359; UNGA, 'Letter Drafted 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the UN Addressed to the Secretary-General' (13 January 2015) UN Doc A/69/723.

[1455] ibid.

[1456] Statement by Dr Alex Sceberras Trigona Special Envoy of the Prime Minister of the Republic of Malta Permanent Mission of the Republic of Malta to the United Nations, World Summit on International Society Review Process, New York (15 December 2015) <https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf>. Applying the Common Heritage of Mankind to the internet's critical infrastructure was first proposed by the Republic of Malta in 1997 in Kuala Lumpur, Malaysia at the World Internet Forum.

of the Common Heritage of Mankind. [1457] The idea was put forward in December 2015 by Dr Trigona, Special Envoy of Malta's Prime Minister, who addressed the United Nations General Assembly in New York at the High Level Meeting reviewing developments after 10 years since the World Summit on the Information Society (WSIS+10). He reiterated that the legal concept of the Common Heritage of Mankind should be applicable to the internet by analogy with Article 136 United Nations Law of the Sea Convention 1982 (UNCLOS 1982).[1458] Noting that it is becoming increasingly apparent that the internet governance problems cannot be solved on a national basis alone, but must be dealt with globally, a reliable legal framework such as that of the Common Heritage of Mankind is needed. He also emphasised that the internet has moved a long way from the paradigm based on Barlow's *Declaration of Independence* and therefore it cannot be treated as *res nullius*, a no-man's land where everyone could be independent.[1459] Instead, cyberspace (particularly the internet), must be seen as *res comunis omnium*, that is a common good with common rules, especially for the next billion users. Designating the internet as the Common Heritage of Mankind is also dictated by privacy concerns and in that sense the Common Heritage of Mankind is the best framework for all stakeholders.[1460] The Maltese proposal, called 'Protection of the Internet as Part of the Common Heritage of Mankind' seems to be gaining some traction already. During a Cyber Warfare Conference in Estonia in May 2015 the NSA Director Admiral Michael Rogers cited the Maltese 1967 initiative proclaiming the sea-bed and its subsoil beyond national jurisdictions as Common Heritage of Mankind in Article 136 UNCLOS 1982 as a hopeful equivalent for an analogous Law of the Internet.[1461]

i. The Feasibility of an International Treaty for Cyberspace

The specifics of applying the Common Heritage of Mankind (CHM) to the internet were discussed in Chapter 3 of this thesis and the normative regime applicable to the seabed in the UNCLOS 1982 were applied by analogy. The outcome of that analysis was that the Common Heritage of Mankind, as a legal concept fits well to the internet. This is because in line with the main tenets of the CHM, the internet is a global resource that should not be appropriated

[1457] ibid.
[1458] ibid.
[1459] ibid.
[1460] ibid.
[1461] ibid.

by any single state, should be subject to a common management system, be managed for the benefit of all mankind and be used for peaceful purposes only. In addition, Common Heritage of Mankind as a legal concept has been in operation for decades and has a proven track record in relation to preserving not only the maritime resources of the seabed but it has also been extended to other areas and resources. It can be found in the Outer Space Treaty 1967, the Moon Treaty 1979, the Antarctic Treaty 1959 and the UNESCO 's Treaty on the Human Genome 1997. Thus, a new legal regime for cyberspace could in theory be devised by analogy to at least this aspect of the UNCLOS 1982. It is difficult to predict that such a global regime be successfully realised at this point in time, bearing in mind the distrust generated by the revelations of mass surveillance. Past examples of devising new regimes to govern the existing environments, such as the UNCLOS 1982, attest that it is in principle possible. However, creating new international legal framework is slow. Furthermore, the process is bound to be protracted for a number of reasons, namely (a) the continued lack of agreement among the international community; (b) the uncertainty as to which international organization should be in charge of the process of treaty making, monitoring and enforcement; (c) the time it takes to reach an international agreement and; (d) the uncertainty as to how exactly human rights obligations are to apply through such a treaty, as evidenced by the international politics of internet governance and cyber security. Each of these obstacles will be discussed in turn below.

- Continued Lack of Agreement Among the International Community

Despite the failed attempts at introducing an internationally binding treaty in the form of the *Draft International Code of Conduct for Information Security* by the Shanghai Cooperation Organization, the political process regarding internet governance, which has been underway since the ITU-hosted Wold Summits on the Information Society 2003 and 2005, continues. Nevertheless, the disagreements as to who should be in charge of the internet and how to govern it remain unsettled.

This inability to reach consensus as to how the cyberspace is to be governed is largely due to the two competing ideologies envisioned for the running of the internet, discussed in Chapter 2 of this thesis. The idea of 'internet freedom' reflected in the multistakeholder approach, continues to be championed by the US and most European countries. This model is rooted in the free flow of information and freedom of expression. It favours the involvement

of a variety of actors, including private companies, such as (ICANN) and (IANA), academics, as well as governmental and non-governmental organizations. Conversely, 'internet sovereignty' supported by, among others, Russia and China, sees greater involvement of states and seeks to subject cyberspace to the traditional understanding of international order, with particular emphasis on such international law principles as sovereignty and non-intervention. This approach also envisages a greater role for the United Nations organizations, such as the International Telecommunications Union (ITU), which seems to have been side-lined again by the US government's 2016 decision to give up its control over the domain name system to ICANN, discussed below in more detail. In addition to these long standing differences of opinion, the political fallout from the Snowden disclosures in 2013 has seriously undermined the chances of an agreement regarding an international cyber treaty. To begin with, the revelations that the NSA spied on even its closest allies have affected state-to-state relationships with the Brazilian, German and Indian authorities expressing their outrage in the immediate aftermath. [1462] The trend for more 'technological sovereignty' and 'data nationalization' has also intensified, with Brazil and the European Union announcing plans to lay a $185 million fibre-optic cables between them and thereby thwart US surveillance.[1463] Furthermore, the enactment by the People's Republic of China's government of the new Cyber Security Law in November 2016, which will come into force on 1 June 2017, illustrates the entrenched positon this country takes on the issue of cyberspace governance. By introducing the Cyber Security Law, China made a decisive move towards more stringent regulations for network security. This new legislation reflects a long standing Chinese policy, which reinforces that country's aims at protecting 'internet sovereignty', with the focus on the critical information infrastructure. Critical information infrastructure, being left undefined in the Cyber Security Law, may include any services needed for public communication and information, power, transportation, finance, public service, as well as any infrastructure that could endanger national security, welfare, 'popular livelihood', or public interest if destroyed

[1462] *The Guardian,* 'Brazilian President: US Surveillance a Breach of International Law' (24 September 2013) < https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>; *Spiegel Online,* 'The NSA's Secret Spy Hub in Berlin' (27 October 2013)< http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>; *The Hindu,* 'India Among Top Targets of Spying by NSA' (23 September 2013) <http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece>.

[1463] supra note 2, para 108.

or hacked.[1464] The new law provides the Chinese government with sweeping authority to regulate and monitor internet services.[1465] It is said to be the first fundamental legislation exclusively focusing on network security protection in that country.[1466] It has three main aspects (1) co-operation with authorities- network operators must cooperate with and provide technical support and assistance to the public and state security authorities for reasons of national security and criminal investigation; (2) data localisation- operators of critical information infrastructure must store personal and other important business data within China; data are not allowed to be transferred out of the Chinese territory unless it is 'truly necessary' and specified security assessments have been conducted and satisfied; and (3) restrictions on key network products- this aims at encouraging the use of Chinese manufactured software and hardware instead of their foreign equivalent, as a result of foreign hacking and spying incidents of recent years.[1467] The Cybersecurity Law mainly serves to increase Chinese government's ability to control domestic internet activity and means that the multi-national businesses and internet companies operating in that country will be subjected to broad and poorly defined array of regulations and potential punishments. For example, businesses could face confiscation of between one and ten times their 'illegal gains' due to the restrictions placed on the amount of personal identifiable information that can be collected.[1468] The law could be seen as an indication of the direction that China has been pursuing for some time now towards the heavily regulated Chinese internet and technology sector. The enactment of the this legislation also reflects and reinforces that country's policy stance regarding censoring of the internet content, discussed in chapter 2 of this thesis, as it extends the monitoring to the infrastructure, which will have implications for technical standards and network interoperability.[1469] This indicates that China's cyberspace could become increasingly isolated and detached from the global internet in the coming years.[1470] It also evidences the lack of interest by the Chinese authorities

[1464] Chris Mirasola, 'Understanding China's Cybersecurity Law' (8 November 2016), *Lawfare*
< https://www.lawfareblog.com/understanding-chinas-cybersecurity-law>.
[1465] ibid.
[1466] *Lexology*, 'China's Cyber Security Law-More Stringent Regulations for Network Security' (8 November 2016) < http://www.lexology.com/library/detail.aspx?g=5ed61c4f-6dbc-450b-b812-1b1d94edb1da>
[1467] ibid.
[1468] ibid.
[1469] Hogan Lovells, 'China Passes Controversial Cyber Security Law' (11 November 2016) < https://www.hoganlovells.com/en/publications/china-passes-controversial-cyber-security-law>.
[1470] ibid.

in engaging in a dialogue with the Western powers regarding negotiations of a cyber treaty, who insist on free and open internet.

- What International Organization?

It remains unclear which organization could take a leading role as a standard setting body. In this regard, it is doubtful that either of the two principal organizations, that is the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union (ITU) could form the foundation for a universal regulatory regime. The ITU has been the international body of choice for some states, such as Russia and China, who wish to assert greater UN role in cyberspace. However, the ITU has not only been criticized for being unable to adjust to the rapid changes in the cyberspace environment, but also for being ill equipped to regulate other, non-technical aspects of cyberspace such as international and criminal law.[1471] Furthermore, the idea for an enhanced role of the ITU to play a part in regulating critical aspects of the internet was firmly rejected by the US at the 2012 World Conference on International Communications in Dubai (outlined in Chapter 3 of this thesis). However, on 1st October 2016 the US government made a concession by officially relinquishing its power over the internet address system to ICANN. [1472] Until that date, the US Department of Commerce had the ultimate authority over how the Domain Name System, one of the internet's most important components, is controlled. The US government oversaw all domain names for websites and individual IP addresses for internet users, which included assigning the operations of high level domain names such as '.com' and '.uk'.[1473] This arguably "gave Washington the power to make entire countries 'go dark' on the internet by removing them from the central naming system".[1474] The handover of this authority to ICANN was supported by the Obama administration, who viewed the change as the only way to prevent the

[1471] Jutta Brunnee and Tamar Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (2015) 58 German Yearbook of International Law, p. 158.
[1472] Richard Waters, 'US Gives up Its Remaining Control Over the Internet' (1 October 2016) *Financial Times <https://www.ft.com/content/66291afc-87f8-11e6-8cb7-e7ada1d123b1>*
[1473] Bryan Lynn, "Did the US Just 'Give Away' Control of the Internet?' (3rd October 2016) <http://learningenglish.voanews.com/a/did-the-us-government-just-give-away-control-of-the-internet-to-icann/3535200.html>
[1474] supra note 29.

tendencies by some governments to separate their own networks and thereby eventually Balkanizing the global system. The handing over of control to ICANN will make little difference to the end user, as that organization has been involved with the running of the internet since the facility was created in 1998.[1475] ICANN will remain to be domiciled in Los Angeles, California, but it will be accountable to multiple stakeholders, including countries, businesses and groups offering technical expertise, who wish to have a greater say over the internet. The transformation is a big change, as it marks a transition from an internet governed by one nation to a mulitstakeholder governed internet and as such is a vital act of international diplomacy.[1476] However, it is also a move on the part of the US to resist the Russian and the Chinese calls for the domain name system to be controlled by the International Telecommunications Union, thus shifting the control to ICANN and not the UN.[1477]

- The Time Factor

A treaty centred around the protection of cyberspace designated as a 'common good' or a 'common resource' in line with the Maltese proposal is in principle sound, but such a conceptual framework is highly likely to take a long time to develop. The obstacles that would have to be overcome, apart from the state security interests, include the general reluctance of states to engage in the treaty making process, as well as the entrenched reticence of some states (particularly the US) to subject cyberspace to an international legal regime, as exemplified by that country's reluctance regarding the involvement of the International Telecommunications Union, outlined in the previous paragraph. In addition, since cyber technologies develop and change rapidly, any international treaty may already be outdated before it comes into force.

- Human Rights Obligations and Cyber Treaty

Finally, there is the problem of how exactly are the human rights obligations to apply to states through such a treaty. The protection of human rights online has been at the peripheries of the

[1475] Dave Lee, "US Ready to 'Hand Over' the Internet's Naming System" (18 August 2016) *BBC News* < http://www.bbc.co.uk/news/technology-37114313>.
[1476] ibid.
[1477] ibid.

internet governance[1478] discourse since the World Summit for Information Society 2003 and 2005 (WSIS I and II).[1479] Not until 2013 Snowden revelations, did the protection of privacy and other fundamental rights come to the forefront of the global internet governance discussions. Consequently, calls for setting of international norms in relation to interception of communications and data, have intensified. In 2013 the former President of the Republic of Brazil, Rousseff made a compelling case in her speech at the opening of the 68th session of the United Nations General Assembly for the creation of 'multilateral mechanisms for the worldwide network that are capable of ensuing principles such as freedom of expression, privacy of individuals and respect for human rights.'[1480] In addition, a joint statement from Pakistan on behalf of a group of countries[1481] made at the 24th session of the UN Human Rights Council,[1482] highlighted the need to protect the right to privacy as an essential element of free speech citing the International Covenant on Civil and Political Rights 1966. The statement made explicit links between the allegations of mass surveillance and the need for reforming global internet governance, stating that 'the existing mechanism like the Internet Governance Forum established under paragraph 72 of the World Summit on Information Society-Tunis Agenda have not been able to deliver the desired results'.[1483] It also called for 'a transparent international system with adequate international framework of internet governance including appropriate safeguards'.[1484]

[1478] World Summit on Information Society, 'Tunis Agenda for Information Society' (2005) WSIS-05/Tunis/Doc/6(Rev. 1)-4, <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.
[1479] ibid. The Tunis Agenda called 'upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practice and self-regulatory and knowledge measures by business and users'.
[1480] Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil at the Opening of the General Debate of the 68th Session of the United Nations General Assembly (24 September 2013)
< https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf>.
[1481] UN Human Rights Council, Joint Statement on Right to Privacy, 24th Regular Session (September 2013)
< https://www.apc.org/en/system/files/HRC24_Pakistan_20130919.pdf >. Pakistan spoke on behalf of Cuba, Venezuela, Zimbabwe, Uganda, Ecuador, Russia, Indonesia, Bolivia, Iran and China.
[1482] UN Human Rights Council 24th Regular Session (September 2013)
<http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session24/Pages/24RegularSession.aspx>.
[1483] ibid
[1484] ibid

Human rights concerns have also featured to some extent as an area of consideration in the discourse relating to cyber security, for example in the Shanghai Cooperation Organization's (SCO) *Draft International Code of Conduct for Information Security* (the Draft Code)[1485] of 2011 and 2015. These instruments were chiefly concerned with security issues and human rights protection (in particular privacy) was not intended to be their main objective. The 2011 Draft Code paid scant attention to issues pertaining human rights, whilst its later 2015 version side-lined the these matters in favour of state sovereignty, territoriality, national security and regime stability in the digital space.[1486] Having said that, the 2015 Draft Code 'made a nod in the right direction' as it did encourage states to pledge respect for human rights and fundamental freedoms. To that end, it introduced a new section (section 2(7)) calling on states to recognize that 'the rights of individual in the offline environment must also be protected in the online environment'.[1487] It also made an express reference to the International Covenant of Civil and Political Rights 1966. However, it referenced only Article 19 (freedom of opinion and expression), with particular emphasis on restrictions available to states with regards to that right. This seems to underpin the Shanghai Cooperation Organization states' belief in their right to exercise control over any digital content within their territories and at their discretion.[1488] Conspicuous by its absence in the 2015 Draft Code is the reference to the right to privacy (Article 17 ICCPR). This is rather surprising, bearing in mind that privacy has been very prominent on the UN agenda since the 2013 Snowden disclosures and before the re-drafted Code was resubmitted to the UN General Assembly in 2015. It could be said that this evidences the unwillingness of the SCO countries to deal with state cyber surveillance. Moreover, it does not inspire much confidence that the international community will come to an agreement regarding a global treaty for cyberspace, as it reinforces the difference in priorities among the SCO countries on the one hand and the UN and human rights organizations on the other hand. Even if the lack of detailed reference to human rights protection was to be put aside, the fact remains that the revised 2015 Draft Code is unlikely to find a global support. The Code emphasises state sovereignty and territoriality in the digital sphere above all else and is replete with national security and regime stability rhetoric. For example, it makes a stronger reference to equal rights of states then its predecessor (the 2011 Code) by emphasising that

[1485] supra note 11.
[1486] ibid.
[1487] Draft Code 2015, supra note 11, section 2(7).
[1488] Sarah McKune 'An Analysis of the International Code of Conduct for Information Society' (29 September 2015) < https://citizenlab.org/2015/09/international-code-of-conduct/>.

'states must play the same role in and carry equal responsibility for, international governance of the [i]nternet, its security, continuity and stability of operations and its development'.[1489] This is underpinned by the call to 'prevent other States from exploiting their dominant position in information and communications technologies'.[1490] Although its long-term future as an international treaty is unpredictable it could be an instrument laying down rules of state behaviour at a regional level for the group of like-minded states.

On the intergovernmental level, an agreement that international human rights law applies to the online environment was reached long before the 2013 Snowden disclosures. The UN 2012 Human Rights Council Resolution titled *The Promotion, Protection and Enjoyment of Human Rights on the Internet,*[1491] put human rights framework for the internet on the agenda at the highest echelons of the UN human rights agencies.[1492] The Resolution, revised in June 2016,[1493] affirmed that the same rights people have offline must also be protected online and noted the Global Multistakeholder Meeting on the Future of Internet Governance held in Sao Paulo in April 2014, which acknowledged, *inter alia*, the need for human rights to underpin internet governance.[1494] The Resolution also recognized that for the internet to remain global, open and interoperable, it is imperative that states address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy.[1495] These Resolutions also stressed the importance of applying a comprehensive human rights based approach when providing and expanding access to the internet and for the internet to be open, accessible and nurtured by multi-stakeholder participation. Nevertheless these and other UN Resolutions, including on the *Right to Privacy in the Digital Age,*[1496] seem only to scratch the surface. They are couched in a general language and in the words of one commentator, are 'far removed from the techno-legal and

[1489] supra note 11, section 2(5).
[1490] Ibid.
[1491] UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (16 June 2012) UN Doc A/HRC/20/8.
[1492] Marrianne Franklin, '(Global) Internet Governance and Its Discontents', in Joanna Kulesza and Roy Balleste (eds.), *Cybersecurity and Human Rights in the Age of Cybersurveillance'* (Rowman and Littlefield 2016), p. 112.
[1493] UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UN Doc A/HRC/32/L.20.
[1494] ibid.
[1495] ibid.
[1496] UN General Assembly Resolution 68/167, 'The Right to Privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167; UN General Assembly Resolution 69/166, 'The Right to Privacy in the Digital Age' (18 December 2014) UN Doc A/RES/69/166.

political practicalities of bringing human rights law and norms to bear on the complex, dense policy domain that encompasses both formal and informal decision making about how the internet is run and how people interact and produce content'.[1497] More specifically, the issues of implementation (how exactly) is the human rights framework to fit into the internet governance agenda, who is going to be accountable and how for the human rights violations, what international court or forum is to hear the complaints of violations, would such decisions be legally binding or not, what would constitute legal remedies and how to access them- all remain unanswered.

A concluding observation that can be derived on the basis of the preceding discussion is that it is unlikely that the international community will in the foreseeable future reach an agreement regarding the adoption of a new, legally binding international treaty for cyberspace, which answers both the security and privacy needs. Therefore, the next section will consider other options, such as modernizing the existing privacy laws under Article 17 ICCPR, the the Universal Periodic Review mechanism, expanding the data protection regime through 'globalizing' of Convention 108 and regulating state intelligence gathering activities through a regional multilateral treaty.

b. Solution 2-Reliance on the Existing International Human Rights Treaties to Protect Online Privacy

Following the Snowden disclosures a coalition of states led by Germany proposed to enshrine digital privacy in an international human rights treaty by means of a new additional protocol for the 'digital sphere' to the Article 17 ICCPR.[1498] The idea was put forward at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw, Poland.[1499] A subsequent resolution to update Article 17 ICCPR and 'create globally applicable

---

[1497] supra note 49, p. 113.

[1498] Ryan Gallagher, 'After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty', (September 2013) <http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html> . The coalition comprised Austria, Hungary, Switzerland and Liechtenstein.

[1499] 35th International Conference of Data Protection and Privacy Commissioners, Resolution on Anchoring Data Protection and the Protection of Privacy in International Law, (23-26 September 2013, Warsaw, Poland) <https://icdppc.org/wp-

standards for data protection and the protection of privacy in accordance with the rule of law' was overwhelmingly supported by the privacy authorities at that conference.[1500] The only country that did not approve the resolution was the US. Nevertheless, the opening of the negotiations on the additional protocol to Article 17 ICCPR conducted by the Special Rapporteur on Privacy, Professor Cannataci has begun.[1501] The additional protocol is not envisaged, however, as 'one new global all-encompassing international convention covering all of privacy or Internet governance'.[1502] The Special Rapporteur recognized that there is no need to create an entirely new privacy regime, since one already exists under the ICCPR Article 17. He adopted a realistic approach, expecting that protection of privacy could be increased by incremental growth of international law through the clarification and eventually, the extension of existing legal instruments, which will be considered next.

i. Modernizing Article 17 ICCPR

One solution of how to bring state sponsored untargeted cyber surveillance within the rule of law is through the process of modernization of Article 17 ICCPR. This could be done by the UN Human Rights Committee (HRC) updating its the General Comment No. 16 to Article 17 ICCPR issued in 1988, which has not kept pace with the rapid developments in surveillance and information technologies.

The past practice of the Human Rights Committee set a precedent for revising or replacing general comments.[1503] The Committee has been motivated by the need to provide

---

content/uploads/2015/02/International-law-resolution.pdf>; 37th International Conference of Data Protection and Privacy Commissioners, Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy, (27 October 2015) <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf>.

[1500] ibid.

[1501] UN HRC, 'Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci', (8 March 2016) UN Doc A/HRC/31/64.

[1502] ibid.

[1503] American Civil Liberties Union, 'Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant of Civil and Political Rights' (2014) < https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf>. In 2011 General Comment No. 10 (written in 1983) was replaced with General Comment No. 34 on Article 19, protecting the right to freedom of expression, whilst in 2013 General Comment No. 8 issued in 1982 was replaced with General Comment No. 35 on Article 9, protecting liberty and security of the person.

greater detailed and authoritative guidance on a content of a particular article, as well as the need to ensure that general comments reflect the changing realities and incorporate developments in the law.[1504] General Comment No. 16 is no exception. Although it sets out the core concepts contained in Article 17, it has lagged behind the technological developments in modern communications and surveillance practices. Consequently, new general comment on Article 17 ICCPR must provide explicit articulation of what is the right to privacy of communications in the digital sphere and spell out the content of this right to ensure its effective protection and enforcement. Currently some of the General Comment No. 16 shortcomings relate to the lack of explicit recognition of such matters as banning untargeted, mass surveillance; [1505] bulk metadata collection and retention; [1506] protecting metadata; [1507] intelligence services/law enforcement access to communications data held by third party service providers and internet companies including in a 'cloud'; the relationship between private companies and governments;[1508] biometric data gathering (through for example finger printing, facial recognition software) and transborder access to non-publically available data circumventing the requirements of the Mutual Legal Assistance Treaties. In addition, some matters must be settled beyond doubt, such as extraterritorial application of human rights and equal treatment of citizens and foreigners (discussed in Chapter 4 of this thesis), as well as specifying the circumstances when the right to privacy may be restricted. This last point relates to the fact that the privacy protection under Article 17 is not absolute. However, at present neither Article 17, nor General Comment No. 16 provide a list of specific limitations to the right to privacy, unlike other provisions in the ICCPR, such as Article 19(3), which does. [1509]

[1504] ibid.

[1505] *Roman Zakharov* v *Russia* (App No 47143/06) 2015 ECHR 1065; *Szabo and Vissy* v *Hungary* (App No 37138/14) 2016.

[1506] Joint Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitilinger and Others* [2014] ECJ. The CJEU declared that the EU Data Retention Directive, which compelled all internet and telecommunication service provides operating in Europe to obtain and retain a subscriber's incoming and outgoing telephone and internet metadata for the period of six months to two years, invalid.

[1507] *Copland v the United Kingdom* (App No 62617/00) (2007) ECHR; *Malone* v *UK* (App No 8691/79) 1985 7 EHHR 14; UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (16 May 2011) UN Doc A/HRC/17/27.

[1508] C-362/14 *Maximilian Schrems v Data Protection Commissioner* (6 October 2015). The CJEU held that Facebook's data transfers for its Irish subsidiary to the US headquarters under the Safe Harbour agreement were unsafe, because US law does not offer sufficient protection against surveillance by that country's public authorities.

[1509] Other provisions of the ICCPR, which set out specific limitations are: Article 12(3)-on the right to liberty of movement and freedom to choose his residence; Article 18(3) on the

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue and Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin both agreed that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as set out in General Comment 27. [1510]

Modern technologies allow for a far reaching intrusion of privacy and international law must reflect this. The process of reforming General Comment No. 16 has been commenced, when the Special Rapporteur on the right to privacy has been mandated with this task in 2015. There are other solutions to curtail mass surveillance that may be undertaken contemporaneously with the process of reforming Article 17 ICCPR, namely the process of the Universal Periodic Review, a regional non-spy legally binding agreement and the expansion of data protections laws, each discussed next.

---

right to freedom of thought, conscience and religion; Article 21 on the right to peaceful assembly and Article 22(2) on the right to freedom of association.

[1510] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Frank La Rue' (16 May 2011) UN Doc A/HRC/17/27, para 29; UNHRC 'Report by Special Rapporteur Martin Scheinin on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (17 May 2010) UN Doc A/HRC/14/46. The Special Rapporteurs suggested that the limitations to the right to privacy are subject to the test of permissible limitations set forth by the HRC in its General Comment No. 27 to Article 12 (freedom of movement), namely:

a) any restrictions must be provided by the law;
b) the essence of a human right is not subject to restrictions;
c) restrictions must be necessary in a democratic society;
d) any discretion exercised when implementing the restrictions must not be unfettered;
e) for a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim;
f) restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected
g) any restrictions must be consistent with the other rights guaranteed in the Covenant.

ii. Universal Periodic Review

The Universal Periodic Review (UPR) is a process that involves a periodic review of the human rights records of all 193 UN member states.[1511] The UPR was established on 15 March 2006- at the time when the Human Rights Council was created by the UN General Assembly in resolution 60/251.[1512] The resolution mandated the Council to 'undertake a universal periodic review, based on objective and reliable information, of the fulfilment by each [s]tate of its human rights obligations and commitments in a manner which ensures universality of coverage and equal treatment with respect to all [s]tates'.[1513] The main goal of the review, which is based on equal treatment for all countries, is the improvement of the human rights situation in every country with significant consequences for people around the globe.[1514] The process is designed to prompt, support and expand the promotion and protection of human rights. In order to achieve this, the UPR involves assessing states' human rights records and addressing their violations wherever they occur.[1515] In addition, the review 'aims to provide technical assistance to states and enhance their capacity to deal effectively with human rights challenges and to share best practice in the field of human rights among [s]tates and other stakeholders'.[1516] The reviews are conducted by the UPR Working Group, consisting of the 47 members of the Human Rights Council and each review is assisted by groups of three states known as 'troikas', who serve as rapporteurs.[1517] The troikas for each state are selected through a drawing of lots following elections for the Council membership in the General Assembly.[1518] The review is based on (a) information provided by the state undergoing the review, which may be in a form of a 'national report'; (b) information contained in the reports of independent human rights experts and groups, known as Special Procedures, human rights treaty bodies and other UN entities; (c) information from other stakeholders including national human rights institutions and non-governmental organizations.[1519] The reviews are conducted through an interactive discussion between the state undergoing the process and other UN member states, which take

[1511] UN HR Office of the High Commissioner, 'Basic Facts about the UPR' <http://www.ohchr.org/EN/HRBodies/UPR/Pages/BasicFacts.aspx>.
[1512] UN GA, Resolution 60/251. Human Rights Council UN Doc A/Res/251 (3 April 2006).
[1513] ibid.
[1514] supra note 68.
[1515] ibid.
[1516] ibid.
[1517] ibid.
[1518] ibid.
[1519] ibid.

place during a meeting of the UPR Working Group.[1520] The range of human rights obligations that are addressed relate to the extent to which states respect their human rights obligations set out in (a) the UN Charter; (b) the Universal Declaration of Human Rights; (c) human rights instruments to which the state is party (human rights treaties ratified by the state concerned); (d) voluntary pledges and commitments made by the state (for example national human rights policies and/or implemented programmes) and (f) applicable international humanitarian law.[1521] As a result of the review by the Working Group, the troika (with the involvement of the state undergoing the process and the assistance of the Office of the High Commissioner for Human Rights), prepares the 'outcome report'.[1522] The report is a summary of the discussion and consists of questions, comments and recommendations made by states to the country under review, together with that country's responses. Following the process whereby the reviewed state can either accept or note recommendations made to it, the report is then adopted at the plenary session of the Human Rights Council.[1523] During the session, the state under review may reply to questions and issues that were not sufficiently addressed during the Working Group and respond to any recommendations that were raised by states during the review.[1524] Following the final outcome, the state must implement any recommendations made and during the second review is expected to provide information on the steps taken in order to implement the recommendations made at the first review.[1525] The international community will assist in implementing the recommendations and conclusions regarding capacity-building and technical assistance in consultation with the country concerned.[1526] If a state is not cooperating with the UPR, the Human Rights Council will decide on the measures it would need to take in case of persistent non-cooperation.[1527]

Since its first meeting in 2008, all 193 UN member states have been reviewed twice within the first and second UPR cycles. The third cycle included the review of the human rights record of the United Kingdom and was held on 1 May 2017.[1528] Among the issues raised were

[1520] ibid.
[1521] ibid.
[1522] ibid.
[1523] ibid.
[1524] ibid.
[1525] ibid.
[1526] ibid.
[1527] ibid.
[1528] UN HR Office of the High Commissioner, 'United Kingdom's Human Rights Record to be Reviewed by the Universal Periodic Review' (1 May 2017) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21569&LangID=E >.

the proposal to replace the Human Rights Act 1998 with a new British bill of rights; the impact of existing counter-terrorism measures; procedures to authorize surveillance, including mass surveillance; data retention and upholding the right to privacy.[1529] The troika for the review of the UK were Albania, Ethiopia and Mongolia.[1530] Following the UPR, the UK received 227 recommendations, which it neither accepted nor rejected out of hand.[1531] Instead, the UK decided to reserve its position on all 227 recommendations until the September 2017 Human Rights Council session, where it will announce which recommendations it is accepting and which it is rejecting.[1532] The Human Rights Council will then present its recommendations and the UK will have to formally respond. This would be however only the beginning of the UK obligations, as the country would have to work to implement the recommendations it has accepted.[1533] As the UPR is a peer-review process central to the UN's human rights system, failure to accept the recommendations made during the review and to demonstrate sufficient progress to its peers could be damaging to the UK's reputation as a leader in human rights and international affairs.[1534] It could also erode the perception of the UPR process itself-the only mechanism by which the human rights record of all UN member states are regularly reviewed.

The United States had undergone the process of UPR in 2010 and 2105.[1535] In its 2010 review the US accepted 171 out of 240 recommendations. Among them were the recommendation to 'legislate appropriate regulations to prevent the violations of individual's privacy as well as eavesdropping of communications by its intelligence and security organizations' and to 'guarantee the right to privacy and stop spying on its citizens without authorization'.[1536] Notwithstanding these acknowledgements, the US government continued its

[1529] ibid. Other issues raised included, the realisation of rights enjoyed through EU instruments post-'Brexit'; ensuring the rights to freedom of expression and association; addressing discrimination against minority ethnic communities and preventing social profiling; measures to safeguard gender equality; combating trafficking in women and girls; domestic violence and violence against women; the impact of austerity measures including on the right to adequate housing; the impact of Immigration Act 2016.
[1530] ibid.
[1531] UNA-UK, 'UK's Universal Periodic Review Shines a Light on Human Rights Concerns' (2 May 2017) < https://www.una.org.uk/news/uk's-universal-periodic-review-shines-light-human-rights-concerns >.
[1532] ibid.
[1533] ibid.
[1534] ibid.
[1535] UNHRC, 'Draft Report of the Working Group on the Universal Periodic Review. United States of America' (21 May 2015) UN Doc A/HRC/W.6/22/L.20.
[1536] UNHRC, 'Report of the Working Group on the Universal Periodic Review. United States of America' (4 January 2011) UN Doc A/HRC/16/11.

surveillance practices, domestic and extraterritorial, which also became the subject of the 2015 UPR. Among the recommendations submitted to the US as the result of that review were those made by Brazil, Germany, Hungary, Liechtenstein and Switzerland, relating to data privacy and surveillance, including extraterritorial surveillance.[1537] The strongest and most specific recommendations are worth citing and called on the US to:

> [r]espect international human right obligations regarding the right to privacy when intercepting digital communications of individuals, collecting personal data or requiring disclosure of personal data from third countries. (Germany)
>
> Ensure that all surveillance policies and measures comply with the international human rights law, particularly the right to privacy, regardless of the nationality or location of those affected, including through the development of effective safeguards against abuse (Brazil).
>
> Strengthen the independent federal-level judicial and legislative oversight of surveillance activities of all digital communications with the aim of ensuring that the right of privacy is fully upheld, especially with regard to individuals outside the territorial borders of the United States (Hungary).
>
> Review their national laws and policies in order to ensure that all surveillance of digital communications is consistent with its international human rights obligations and is conducted on the basis of a legal framework which is publically accessible, clear, precise, comprehensive and non-discriminatory (Liechtenstein).
>
> Take all necessary measures to ensure an independent and effective oversight by all Government branches of the overseas surveillance operations of the National Security Agency, especially those carried out under the Executive Order 12333 and guarantee access to effective judicial and other remedies for people whose right to privacy would have been violated by the surveillance activities of the United States (Switzerland).[1538]

[1537] supra note 92.
[1538] ibid, paras 5.295-312.

These are no doubt positive developments. Through the UPR mechanism, concerns relating to surveillance laws and practice can be raised by states in many other countries in the world and the recommendations made are a sign that the right to privacy is receiving a deserved attention within the UPR processes. In this sense, this mechanism complements other developments within the UN, such as the establishment of the mandate of the Special Rapporteur on the right to privacy, to monitor and assess all states' compliance with thier obligations relating to the right to privacy.

B. Regional Level

a. Solution 3- Regulation of Mass Surveillance Through a Regional Legally Binding Treaty

Current state practice suggests lack of universal support for international surveillance norms aimed at regulating states' gathering of signals intelligence in cyberspace. However, that does not necessarily mean that achieving reduced surveillance, foreign and domestic, is always going to be impossible. At this stage, in the absence of international treaty and clear customary norms, a regional legally binding treaty could be an operationally viable way forward for a group of like-minded states. Indeed, in 2015 the Parliamentary Assembly of the Council of Europe (PACE) in its Resolution 2045 among other solutions to stop violations of human rights, urged its member and observer states to adopt an 'intelligence codex' (the Codex)- a binding multilateral European treaty to regulate the activities of intelligence agencies for the purposes of the fight against terrorism and organized crime. [1539] The need for a legal framework on the national and international level was made quite clear by the Council of Europe (CoE). Not only is it important to rebuild trust among transatlantic partners, member states of the CoE, as well as between citizens and their governments, [1540] but it was also recognized that surveillance practices endanger other human rights, which are the cornerstone of democracy (Article 10-freedom of information and expression; Article 6-right to fair trial; Article 9-freedom of religion). In addition, the PACE explanatory memorandum stated that:

[1539] Parliamentary Assembly of the Council of Europe, Resolution 2045, supra note 3.
[1540] ibid, para 13, p. 8.

> [t]he political problems caused by 'spying on friends' and the possible collusion between intelligence services for the circumvention of national restrictions show the need for states to come up with a generally accepted 'codex' for intelligence agencies that would put and end to unfettered mass surveillance and confine surveillance practices to what is strictly needed for legitimate security purposes.[1541]

Most importantly it was proposed that:

> [s]uch a codex would lay down precisely what is allowed and what is prohibited between allies and partners; it would clarify what intelligence agencies can do, how they can co-operate and how allies should refrain from spying on each other [...] it would be a signal that governments are willing to provide some degree of transparency in the conduct of their surveillance programmes and guarantee citizens' rights to privacy to the extent possible.[1542]

Four simple rules were suggested for governing co-operation among the intelligence agencies, which should form the cornerstone of the Codex. First, any form of mutual political, economic espionage must be prohibited without exception.[1543] Secondly, any intelligence activity on the territory of another member state would only be carried out with that state's approval and within a statutory framework, that is for a specific reason of preventing crime/terrorism.[1544] Thirdly, the tracking, analysing and storing of mass data is strictly prohibited if that data is from non-suspected individual from a friendly state. Only information pertaining to legitimately targeted individuals may be collected on an exceptional basis for specific purposes, whilst any data that is stored but not needed for these purposes must be immediately destroyed. [1545] Finally, the intelligence agencies would be banned from forcing telecommunication and internet companies to grant them unfettered access to their massive databases of personal data without a court order.[1546] Resolution 2045 adopted by the Council of Europe specified that 'the codex should include a mutual engagement to apply the same

[1541] Parliamentary Assembly of the Council of Europe Explanatory Memorandum, 'Mass Surveillance. Who is Watching the Watchers?' (21 April 2015), para 115, p. 50
[1542] ibid.
[1543] ibid, para 116.
[1544] Ibid.
[1545] ibid.
[1546] ibid.

rules to the surveillance of their own nationals and residents and to share data obtained through lawful surveillance measures solely for the purposes, for which they were collected.'[1547] It was also proposed that the 'Intelligence Codex' would adapt the safeguards devised by the European Court of Human Rights for surveillance.[1548] The question that arises in this context is therefore what would be the advantage of the Codex over and above the existing ECHR norms and how should these norms relate to mass surveillance? These points are discussed below.

i. The Intelligence Codex and the European Convention on Human Rights

The primary argument for adopting a multilateral treaty to regulate the operations of state intelligence agencies, such the Intelligence Codex, is the fact that the existing privacy framework in Article 8 ECHR in relation to surveillance consists of only the minimum standards.[1549] The PACE report recognizes that the jurisprudence developed by the European Court of Human Rights (ECtHR) must be supplemented by more specific rules reflecting the realities of the technical capabilities of modern surveillance, as the existing rules are merely a point of departure for European states.[1550] In this sense the Codex would provide more extensive guarantees. A number of points, where the ECtHR falls short of precise rules applicable to cyber surveillance illustrate the need for a separate, more detailed legally binding treaty. These include, but are not limited to: (a) defining 'communications surveillance'; (b) adopting and adapting standards set out by the ECtHR in relation to legality standards ('in accordance with the law') to foreign surveillance measures; (c) adopting more stringent standards as to what constitutes a 'legitimate aim' in relation to mass surveillance; (d) providing for mandatory judicial authorisation of surveillance; (e) providing that the complaints mechanism should include an obligatory user notification. Each of these will be considered in turn.

[1547] ibid.
[1548] ibid, para 97, p. 80.
[1549] ibid, p. 57.
[1550] Ibid.

- Defining 'Communications Surveillance'

In the aftermath of the Snowden disclosures, some governments sought to defend their activities by distinguishing between the automated collection and scanning of private communications on the one hand and those communications being scrutinized by human beings, on the other hand.[1551] The argument put forward was that automated collection or monitoring is not surveillance at all and as the collected data was not scrutinized by humans, no privacy invasion occurred.[1552] In *S and Marper v UK*[1553] the Grand Chamber of the ECtHR held that 'the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data'.[1554] The ECtHR has not specifically yet considered what is the definition of 'communications surveillance' in the digital context. The Intelligence Codex could build on the Court's ruling in *S and Marper* to avoid any future ambiguity. A definition put forward by privacy organizations and security experts at the UN Human Rights Council in Geneva in September 2013, which is contained in the International Principles on the Application of Human Rights to Communications Surveillance (The Necessary and Proportionate Principles),[1555] may also prove useful. Accordingly:

> [c]ommunications surveillance includes not only the actual reading of private communications by another human being, but also the full range of monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, or arises from a person's communications in the past, present, or future.[1556]

[1551] Necessary and Proportionate Coalition, 'Necessary and Proportionate Global Legal Analysis' (2014) < https://necessaryandproportionate.org/global-legal-analysis>, p. 12.
[1552] ibid.
[1553] *S and Marper v United Kingdom* (2009) 48 EHRR 50.
[1554] ibid, para 121.
[1555] supra note 108. *The Necessary and Proportionate Principles* were written by over 40 human rights organizations and security experts, including: Access, Article 19, Electronic Frontier Foundation, Open Rights Group, Privacy International, Bits of Freedom, Association for Progressive Communications. *The Principles* were endorsed by the UK's Liberal Democratic Conference, as well as European, Canadian and German Parliaments. They were cited, among others, by the US President Review Group on Intelligence and Communications Technologies Report and the Inter-American Commission on Human Rights.
[1556] ibid, p. 12.

- Legality

As discussed in Chapter 4 of this study, in a number of cases including *Klass,*[1557] *Malone,*[1558] *Weber,*[1559] *Liberty,*[1560] *Rotaru,*[1561] *Zakharov*[1562] and *Szabo,*[1563] the Strasbourg Court has developed minimum standards, which domestic law must meet in order to be compatible with Article 8 ECHR.[1564] Among them is the requirement to specify the categories of people liable to have their communication intercepted. In collecting information, state authorities often build a human network around an individual of interest to them by gathering telephone and/or internet metadata related to other persons with whom that individual may be in contact and who are usually one or two stops ('hops') away from him/her. This is known as 'contact chaining'. National legislation would usually set out these powers in terms of 'relevance' for the investigation of terrorism or crime.[1565] The Strasbourg Court has not yet addressed this issue in the context of interception of internet metadata,[1566] but in this case the 'relevance'

[1557] *Klass and Others v Germany* (App No 5029/71) (1978).
[1558] *Malone,* supra note 64.
[1559] *Weber and Saravia v Germany* (App No 54934/00) (2006).
[1560] *Liberty and Others v UK* (App No 58243/00) (2009) 48 EHRR.
[1561] *Rotaru v Romania* (App No 28341/95) (2000) ECHR 2000-V.
[1562] supra note 62.
[1563] ibid.
[1564] *Weber v Germany,* supra note 116. These include:

(1) the nature of the offences which may give rise to an interception order;
(2) definition of the categories of people liable to have their telephones tapped and a limit on the duration of telephone tapping;
(3) the procedures to be followed for examining, using and storing of data obtained; the precautions to be taken when communicating the data to other parties; and
(4) the circumstances in which recordings may or must be erased or the tapes destroyed.

[1565] European Commission for Democracy Through Law (the Venice Commission), 'The Democratic Oversight of Signals Intelligence Agencies' Study No. 719/2013 (15 December 2015)
< http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e>. In some jurisdictions, for example in the US, the access to stored telephony metadata will be granted on the basis of 'reasonable articulable suspicion' individually approved by the Foreign Intelligence Surveillance Court under s 215 Foreign Intelligence Surveillance Act.
[1566] ibid, para 98, 81. The Venice Commission explained contact chaining in the following terms:

> [t]he bulk metadata are analysed to identify communications patterns. This usually

criterion gives potential for expanding the net of surveillance greatly to cover huge numbers of people without any connection whatsoever to crime or terrorism.[1567] There is therefore a need for contact chaining to be regulated by placing strict limits on the power to query collected bulk metadata.

- Legitimate Aim

The *Zakharov* and *Szabo* cases illustrate the Court's acknowledgement that the legal threshold of 'national security' is dangerously broad especially in the context of mobile/electronic communications, which contrasts with its earlier more permissive approach in *Weber* and *Kennedy*. The ECtHR now favours a stringent test based on reasonable suspicion and this criterion should be adopted in the Intelligence Codex, as a legal requirement for all domestic surveillance powers. As for allowing the collection of signals intelligence for 'economic well being of the nation', it has been feared that this ground has been used as an excuse to justify state's conducting economically motivated cyber espionage.[1568] The problem is that there seems to be no limits set out by the ECtHR jurisprudence regarding when data may be collected pursuant to this ground. One view was that to avoid nations acting for nefarious purposes cloaked in 'economic well being of a nation', this criterion must be supplemented by clear prohibition of economic espionage, buttressed by effective oversight and prohibitions on letting government departments, or administrative agencies concerned with promoting trade, task the signals intelligence agencies.[1569]

- Judicial Authorisation

In order to comply with the ECHR a secret surveillance programme must be subject to independent supervision, which may be either judicial or non-judicial.[1570] In the past cases, the ECtHR held that judicial authorisation is 'in principle' desirable and 'offer[s] the best

takes the form of checking whether previously identified suspect telephone numbers (X) are in contact with other numbers (Y) and then whether Y is in contact with other numbers (Z).

[1567] ibid, para 10, p. 57.
[1568] ibid.
[1569] ibid para 73, p. 73.
[1570] *Weber* supra note 116; *Klass* supra note 114; *Zakharov* supra note 62; *Szabo and Vissy v Hungary* (App No 37138/14) (2016).

guarantee of independence, impartiality and a proper procedures',[1571] but stopped short of requiring this in all circumstances. In *Klass* the ECtHR found that oversight by a non-judicial body was allowed, where that body is sufficiently 'independent of the authorities carrying out the surveillance'.[1572] Yet, the issue of impartiality in cases where authorisation has been in the guise of a non-judicial bodies, such as an official of the Post Office, gave the Court reasons for concern. [1573] An opportunity to require that all states must provide that only judicial authorisation would suffice arose lately in *Zakharov*, but the Court held that 'control by an independent body, normally a judge with special expertise, *should* be the rule and substitute solution, the exception warranting close scrutiny'.[1574] *Szabo* was yet another confirmation that judicial control of secret surveillance is preferable, but not obligatory.[1575] In the sphere of mass surveillance, the key defect therefore of the current authorisation regime is the Court's repeated reticence to make the requirement of judicial authorisation mandatory across jurisdictions.

- Complaints Mechanism

Under Article 13 ECHR individuals have a right to an effective remedy in their national courts in cases where a public authority has infringed their rights under the 1950 European Convention on Human Rights .[1576] Part of this entitlement is the right of citizens to be informed of their data being collected and/or that they have been subject of surveillance, known as user notification.[1577] The issue of whether and when an individual may expect to be informed is far

[1571] *Klass*, supra note 85, para 87.
[1572] ibid para 56.
[1573] *Kopp v Switzerland* (App No 23224/94) (1999) 27 EHRR 91, para 74:

> [i]t is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge […].

[1574] *Zakharov*, supra note 62, para 77.
[1575] *Szabo*, supra note 127, para 75. The ECtHR opined that judicial authorisation offers the best guarantees of independence, impartiality and a proper procedure, since the supervision of a member of the executive (the Minister of Justice) did not provide the necessary guarantees against abuse.
[1576] The European Convention for the Protection of Human Rights and Fundamental Freedoms, 213 UNTS 222, art 13:

> [e]veryone, whose rights and freedoms as set forth in this Convention are violated, shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

[1577] Necessary and Proportionate, 'Global Legal Analysis. Background and Supporting International Legal Analysis for the International Principles on the Application of Human

from settled. In *Klass*, the ECtHR found that states are not required to disclose that they have ordered or conducted surveillance in a particular case, nor must they notify a person after the surveillance has ceased.[1578] The ECtHR considered that is was not feasible in practice to require subsequent (post interception) notification in all cases.[1579] However, in the more recent cases the ECtHR showed a clear tendency towards the establishment of this as a right. [1580] For example, in *Ekimdzhiev* v *Bulgaria*[1581] the ECtHR held that the missing notification of the individual after surveillance violated both Article 8 and Article 13 ECHR. However, the Court fell short of finding that notification was a necessary requirement of domestic surveillance laws in general, stating that authorities *should* issue a notification to an individual who had been secretly monitored.[1582]

There are a number of important matters either not addressed or left unclear by the ECtHR regarding secret surveillance rules, supporting the case for detailed norms applicable to foreign and domestic practice of surveillance powers, which ought to to be set out in a separate legally binding document. The argument in favour of a hard law regional instrument such as the Intelligence Codex from the protection of human rights perspective is compelling, as it could not only incorporate the rules of the ECHR as interpreted in the ECtHR jurisprudence as a minimum standard, but also 'fill in the gaps' where more detailed technical standards are necessary. Above all the Codex could introduce identical procedural standards as set out in *Weber* and reiterated in *Zakharov* for all cyber surveillance (domestic and extraterritorial alike) thus putting a stop to an unjustifiable distinction between these types of operations presently applied by many states to SIGINT collection. In this sense, it could both harmonize and govern state surveillance in accordance with the rule of law. This kind of solution was supported by the Commissioner for Human Rights of the CoE, Nils Muižnieks in 2014 when he stated that: '[m]ember [s]tates should bring the activities of national security and intelligence agencies within the overarching legal framework'.[1583] He stressed that '[u]nless

---

Rights to Communications Surveillance' (2014) <https://necessaryandproportionate.org/global-legal-analysis>, p. 24.

[1578] *Klass*, supra note 114, para 85.

[1579] ibid, para 58.

[1580] *Weber*, supra note 116; *Association for European Integration and Human Rights and Ekimdzhiev and Bulgaria* (App No 62540/00) (2007); *Kennedy v UK* (App No 26839/05) (2010); *Uzun v Germany (*App No 36623/05) (2010); *Zakharov*, supra note 62.

[1581] ibid.

[1582] ibid.

[1583] Council of Europe, Commissioner for Human Rights, supra note 7.

there is increased transparency on the rules under which these services operate democratically, extraterritorially and in cooperation with each other- their activities cannot be assumed to be in accordance with the rule of law'.[1584] Needles to say, such a solution will only be meaningful so long as the states, which are the most active in the surveillance sphere, particularly the US, are willing participants. Bearing in mind that the US would have to become a party to the ECHR and be subject to the jurisdiction of the ECtHR, this seems unlikely. Still, a European treaty setting out detailed technical and legal standard setting out 'the rules of the road' for security and law enforcement organizations, including intelligence sharing arrangements, in conformity with Article 8 ECHR could be a promising start.

ii. The Intelligence Codex and Political Realism

The 2015 proposal from the Council of Europe to regulate the activities of intelligence agencies in an interconnected global environment of cyberspace is the first, concrete proposal of this kind. Viewed from a realistic perspective of international relations, the success of the Intelligence Codex coming to fruition will no doubt be plagued with difficulties. Nevertheless, there are many advantages of this type of solution, not least of which is its originating from and being negotiated in the Council of Europe. This is because the CoE has a successful track record regarding the negotiation of international treaties, as demonstrated by the Convention on Cybercrime 2001 (the Budapest Convention) and Convention 108, both of which deal with activities conducted in the cyber environment. These two Conventions began life as regional, European instruments, but in time became international, albeit not universal, since both allow for accession by non-European countries. Thus, the Budapest Convention has been ratified by 49 parties, among them four non-Council of Europe states who signed it (the US, Canada, Japan and South Africa) and five, including the US which also ratified it.[1585] Similarly, the membership of Convention 108 is not purely confined to the Council of Europe members states. The process of 'globalization' of that treaty beyond its European origins has been

[1584] ibid.
[1585] Council of Europe Chart of Signatures and Ratifications of Treaty 185, Convention on Cybercrime, Status as of 31/07/2016. The other states are Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama and Sri Lanka.

underway since the start of this decade, when Uruguay accessed it in 2013.[1586] In this sense, the Intelligence Codex could not only be a regional treaty, but also be opened to other non-European states to accede to and thus potentially have wider than Europe reach.

It is still unclear however how the Codex has been received by states. To date, there is little reaction to it, although the Dutch government has already expressed its reservations. These mainly relate to the proposed prohibition on the exercise of mutual political, economic espionage, as being unrealistic.[1587]

Admittedly, as discussed in Chapter 1 of this thesis, states have shown no real appetite to regulate espionage, as there is no specific treaty regarding traditional forms of peacetime espionage, or cyber espionage. Historically, international law has been rather ambivalent regarding regulation of electronic surveillance, which falls within the broader concept of peacetime espionage, for a number of reasons.[1588] First, espionage is a tool widely deployed by states to protect their own core national security interests, regarding such fundamental aspects as gathering evidence of hostile intent or a planned terrorist attack originating abroad.[1589] Secondly, states are very secretive about their espionage capabilities. Therefore discussing ways and means to limit espionage conducted on other states without revealing certain information about their own capabilities means not only publically admitting in their engagement, but also losing an advantage over other states.[1590] Thirdly, a group of states with superior surveillance capabilities, such as the US, the UK, France Russia, China and Israel have

---

[1586] Graham Greenleaf, 'Balancing Globalization's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe' (23 June 2016) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2801054>.

[1587] Matthijs Koot, 'Dutch Government Rejects Idea of No-Spy Agreements Between European Countries' (13 March 2015) < https://blog.cyberwar.nl/2015/03/dutch-minister-of-the-interior-rejects-eu-pace-proposal-omtzigt-of-anti-spy-treaty-between-european-countries/>.

[1588] For example, the US FISA defines electronic surveillance to include 'the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the United States […]' 50 U.S.C. § 1801(f)(2). The 'contents' of a communication is defined to include 'any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication,' 50 U.S.C. § 1801(n), thus suggesting that the surveillance covered by FISA includes more than simply intercepting the verbal contents of some communications. Cf. 18 U.S.C. § 2510(8) (defining contents under Title III as including 'any information concerning the substance, purport, or meaning of that communication').

[1589] Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55 Virginia Journal of International Law pp. 292-367.

[1590] ibid.

to date resisted (and will in all probability continue to do so) excessive regulation of surveillance called for by the countries, who are not as technically advanced. These former nations also tend to have significant political and economic power on the international stage and therefore are in a strong position to control the direction of actions in the United Nations and elsewhere.[1591] Fourthly, the recent state practice from some Western democracies points to a divergent policy stance from that of the UN and major human rights organizations, leaning towards adopting more surveillance powers at the expense of privacy. A number of countries have recently passed new pro-surveillance laws as a legislative response to the stream of terrorist attacks in Europe and elsewhere. A case in point are the new statutes in the UK, France and the US. The UK Investigatory Powers Act 2016 presents a serious potential for breach of human rights on the basis of, *inter alia*, its powers for bulk communication data retention, compromising encryption by the government insisting on 'backdoors'/preventing end-to-end encryption, bulk thematic warrants and providing for insufficient safeguards in relation to intelligence sharing.[1592] The Act legislates for some of the most sweeping surveillance powers in Europe and has therefore prompted criticism from the Special Rapporteur Cannataci, who observed that the Act '*prima facie* fails the benchmark set by the [CJEU] in *Schrems* and ECtHR in *Zakharov*'.[1593] France has also enacted new digital surveillance law in the aftermath of the Charlie Hebdo attacks, the '*Loi Renseignement'* (Surveillance Act), described as the 'French Patriot Act',[1594] whilst in the US the Senate overwhelmingly passed the Cybersecurity Information Sharing Act (CISA)[1595] in October 2015. This state practice seems to pay little attention to the repeated calls from the UN General Assembly to:

> [t]ake measures to put an end to violations of [the right to privacy, including in the context of digital communications] and to create the conditions to prevent such

[1591] ibid, p. 23.
[1592] Liberty, 'Draft Investigatory Powers Bill: Liberty Calls for Full Redraft as Committee Report Highlights Major Concerns' (11 February 2016) < https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/draft-investigatory-powers-bill-liberty-calls-full-redraft>.
[1593] Report of the Special Rapporteur Cannataci, supra note 58, para 39, p. 14.
[1594] Ben McPortland, 'What Has France Actually Done to Fight Terrorism' (19 July 2016) *The Local*, < http://www.thelocal.fr/20160719/what-has-france-done-to-fight-terrorism>.
[1595] Sam Thielman, 'Senate Passes Controversial Cybersecurity Bill CISA 74 to 25' (27 October 2015), *The Guardian*, < https://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote>.

violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law.[1596]

In many respects therefore, the UN policy efforts and those of some Western governments seem to form 'parallel universes'. However, one aspect that appears to be in favour of at least some states agreeing to a regional, legally binding 'non-spy' agreement is the marked shift in focus in relation to who is the subject of surveillance. Historically signals intelligence efforts abroad were concentrated on gathering data about decision-making by foreign governments.[1597] Collecting was amounts of information on private individuals was not wide-spread and costly. Consequently, public pressure to curtail espionage was minimal, as it was not seen to effect average citizens abroad.[1598] This is no longer the case and may well contribute to some degree of interest in the proposed Intelligence Codex.

Thus far, the Codex has met with only one response (the Netherlands) out of the 47 CoE member states. In the absence of more responses from all the member states it is difficult to speculate what the future of the Codex may be. The Codex is contained in Resolution 2045(2015) and Recommendation 2067(2015) proposing that the Committee of Ministers, (the CoE decision making body composed of foreign ministers of the contracting parties) initiates it. However, PACE resolutions and recommendations are non-legally binding. [1599] Recommendations contain proposals addressed to the Committee of Ministers and their implementation is within the competence of the foreign ministers of all member states comprising the Committee. They may either support the Codex and begin the process of negations, or reject it, as was the case with the Dutch authorities. If the Codex is rejected, the attempt to exert influence by the PACE on Council of Europe member states to ban mass surveillance will undoubtedly be undermined. However, in view of the deep concerns and condemnation of these practices by the PACE, opting out could lead to triggering Article 52 ECHR procedures.[1600] Pursuant to this provision the Secretary General, a senior official of the

[1596] supra note 53.
[1597] supra note 146.
[1598] ibid.
[1599] Council of Europe Parliamentary Assembly, In Brief 'The Democratic Conscience of Greater Europe' <http://website-pace.net/en_GB/web/apce/in-brief>.
[1600] ECHR, supra note 133, art 52:

> [o]n receipt of a request from the Secretary General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of this Convention.

CoE, may require all 47 CoE member states to report on how their mass surveillance practices comply with the European Convention on Human Rights and make their replies public. This could lead to more political pressure being put on governments to carefully consider the stance they may take regarding the proposed Codex. This is particularly pertinent in the case of all those counties, where draconian counter terrorism measures have been recently enacted, or are in the process of being adopted, such as the UK. [1601] An example of the effectiveness of Article 52 ECHR initiative is the inquiry into secret detentions and illegal transfers of detainees involving Council of Europe Member States in 2005. [1602] The PACE Reports uncovered evidence of human rights violations and helped to put pressure on governments, leading to high profile international and national enquiries, which sought to bring those responsible to justice and led to developments of international law. [1603] The PACE has already requested that the Committee of Ministers draft its suggested Intelligence Codex and draw up guidelines for the 47 European governments the Council represents. [1604] Furthermore, the author of the *Mass Surveillance* report, Rapporteur Omitzigt recommended that Article 52 inquiry be launched in the wake of the 'BND/NSA scandal' in 2015. [1605] The allegations that the foreign intelligence agency of Germany (the BND) conducted surveillance on its European allies for the NSA caused Rapporteur Omtzigt to reiterate that 'the Intelligence Codex laying down the rules of fair play applicable to the secret services of like-minded countries is urgently needed' and urged national parliaments to start serious negotiations on the issue. [1606] Omtzigt's concerns that the surveillance powers will grow further, whilst political oversights keep diminishing,

---

[1601] Council of Europe, 'Nils Muižnieks: Human Rights in Europe Should Not Buckle under Mass Surveillance' (12 February 2016)
< https://www.coe.int/en/web/media-freedom/news/-/asset_publisher/RuR4jZRX8nrl/content/nils-muiznieks-human-rights-in-europe-should-not-buckle-under-mass-surveillance?>. This includes countries such as France, The Netherlands, Austria, Finland, the UK and Poland.
[1602] Council of Europe Parliamentary Assembly, 'Timeline: The Council of Europe Investigation into CIA Secret Prisons in Europe'
<http://assembly.coe.int/nw/xml/News/News-View-en.asp?newsid=5722&lang=2>.
[1603] ibid.
[1604] Natasha Lomas, 'European Rights Body Again Rejects Mass Surveillance' (22 April 2015)
< https://techcrunch.com/2015/04/22/european-rights-body-again-rejects-mass-surveillance/ >
[1605] Council of Europe Parliamentary Assembly, 'Rapporteur on Mass Surveillance Reacts to Revelations of Collusion Between NSA and BND' (4 May 2015)
<http://www.assembly.coe.int/nw/xml/News/News-VieEN.asp?newsid=5592&lang=2&cat=.>
[1606] ibid.

resulting in a 'runaway surveillance machine',[1607] is a warning that all European states must heed.

The Codex is a positive development. It urges that any form of political, economic and diplomatic espionage as well as mass surveillance be prohibited. Its main weakness is the fact that it is regional in scope and even if favourably received by the Council of Europe member states, it is unlikely that it will be of interest to the US.

b. Solution 4- Creating an International Legal Framework for Data Protection

The globalization of data processing due to the trans-border nature of the internet and the Snowden revelations contributed to an increased interest in and growing calls for creating an international legal framework for data protection.[1608]

Data protection law is focused mainly on the management of personal information[1609] and specifically regulates all, or most stages in the processing of certain kinds of data.[1610] It addresses the ways in which data is gathered, registered, stored, exploited and disseminated.[1611] It primarily aims to safeguard certain interests and rights of individuals (as against corporations or other legal/juristic persons) in their role as data subjects-that is when data about them is processed by others.[1612] The main rules of data protection law embody a set of procedural principles, such as that personal data should be collected by fair and lawful means, that the amount collected should be limited to what is necessary to achieve the specified purpose and that that purpose must be legitimate and not used in ways that are incompatible with purpose limitation.[1613]

[1607] *The Guardian*, 'Mass Surveillance is Fundamental Threat to Human Rights, Says European Report' (26 January 2015) < https://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe>.
[1608] Christopher Kuner, 'The European Union and the Search for an International Data Protection Framework' (2014) Gronigen Journal of International Law, pp. 55-71.
[1609] ibid.
[1610] Lee A. Bygrave, *Data Privacy. An International Perspective* (Oxford University Press 2014), p. 1.
[1611] ibid.
[1612] ibid.
[1613] ibid.

There are a variety of data protection legally binding and non-legally binding instruments (the latter dealt with elsewhere in this chapter) that have been enacted at international and regional levels. These present a fragmented legal landscape and add to the challenges for realising an international framework for data protection.

On the international level, Article 17 of the International Covenant of Civil and Political Rights 1966 protects the processing of personal data and makes some reference 'to gathering and holding of personal information on computers and data banks'. [1614] However, Article 17 ICCPR does not deal or even mention data protection and is now in a need of modernization, as previously discussed. On the regional level, the three data protection regimes that will be subject of focus in this section, are (a) the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); [1615] (b) the European data protection legal framework; and (c) the African Union Convention of Cyber Security and Personal Data Protection (AU Convention). [1616]

i. The 'Globalization' of Convention 108

The Council of Europe was one of the first international bodies to begin developing normative responses to the threats posed by computer technology to privacy related interests. [1617] It has established a framework of specific principles setting standards for personal data protection and to date remains the only international organization to have drafted a multilateral treaty dealing directly with data privacy, namely Convention 108. The Convention was adopted in order to reconcile the right to privacy with the right to information and to ensure the same level of protection of these rights beyond national borders. [1618] It remains the only legally binding international instrument in this field, with a worldwide scope of application as it is open for accession by any country, including countries that are not members of the Council of Europe, that have data protection legislation compliant with the Convention. [1619] The treaty has 48

[1614] UNHRC, 'General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence and the Protection of Honour and Reputation' (8 April 1988), para 10.
[1615] Convention 108, supra note 3.
[1616] African Union Convention of Cyber Security and Personal Data Protection, 27 June 2014, EXCL/846(XXV).
[1617] supra note 167, p. 31.
[1618] ibid.
[1619] supra note 3, art 23(1).

signatories[1620] and its international scope has been expanding in recent years with non-European countries, such as Uruguay, Cape Verde, Morocco, Senegal and Tunisia either having already acceded to it, or in various stages of the process since 2013, which illustrates its potential for becoming a global standard.

Convention 108 complements and reinforces the right to respect for private life enshrined in Article 8 European Convention on Human Rights. It covers all operations carried out on the internet, such as collection, storage, alteration, erasure, retrieval and dissemination of personal data.[1621] It also provides for the lawful and fair obtaining and processing by public and private sector.[1622] It seeks to regulate transfrontier data flow to third countries, prohibiting such transfers to states and organizations that do not provide adequate levels of protection.[1623] With new data protection challenges, it became clear that Convention 108 should be modernized and this process has been undertaken by the Consultative Committee of the Convention (T-DP) since 2011. The recent rulings in *Schrems*,[1624] *Zakharov* and *Szabo* brought into a sharp focus the fact that its modernization and global promotion is more than ever of great necessity. Consequently, the Draft Modernized Convention 108 (the Draft Convention) was published in September 2016[1625] and once adopted will provide for additional obligations on state parties. Some of the innovations of the modernized Convention include the explicit requirement that data processing shall be proportionate,[1626] provision of an obligation on data controllers to declare data breaches[1627] and transparency of data processing.[1628] The additional individuals' safeguards include the right not to be subject to a decision based solely on automatic processing without having their views taken into consideration, the right to know the reasons underlying the processing[1629] and the right to object to it.[1630] The Draft Convention

[1620] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 108. Status as of 17/12/2016'.
[1621] supra note 3, Chapter II.
[1622] ibid, art 5(a)-(b).
[1623] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and trasborder data flows, (8 October 2001) ETS No 181.
[1624] supra note 67.
[1625] Council of Europe, Draft Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, (Modernized Convention) (September 2016).
[1626] ibid, art 5.
[1627] ibid, art 7.
[1628] ibid, art 7bis.
[1629] Draft Explanatory Report to Draft Modernized Convention 108 (24 August 2016), para 76.
[1630] supra note 182, art 8(1)(d).

also improves the competences of the T-PD to allow a stronger follow up and evaluation of the implementation of the Convention. [1631] Finally, the future mutual assistance as regulated in Chapter IV of the Draft Convention will be the sole task of national supervisory authorities, enabling their greater cooperation.[1632]

The steady global expansion of national data privacy laws in the last 45 years and the work carried out to modernize Convention 108 makes it perhaps the only prospect for a universal standard in the field of data privacy.[1633] The main factor in favour must be the lack of other candidates, making the Convention the only realistic prospect.[1634] Other regimes have been developed, most notably in the European Union. These count for some of the most ambitious, comprehensive and complex in the field. [1635] Data protection is a binding fundamental right under Article 8 of the Charter of Fundamental Rights[1636] and Article 16 of the Treaty of the European Union. [1637] The central instrument, Data Protection Directive (DPD)[1638] was created to regulate the progression of personal data within the EU and provides the rules for data protection in the public and private sphere based on the principles of purpose limitation, data minimization and the rights of data subjects. The DPD will be replaced in 2018 by the General Data Protection Regulation[1639] as part of the EU data protection reforms. This regime introduces some of the most stringent data laws in the world, impacting the way every entity uses and holds Europeans' personal data inside and outside Europe. For example, it adds a number of new elements, namely compliance requirements, transparency, enforcement, sanctions and remedies frameworks to apply to all organizations, including data processors. Its potential global impact is beyond doubt. However, the EU legal regimes are only legally binding among the 28 EU member states and as such the expansion of these rules is not possible outside Europe.

Another regional legally binding instrument in the sphere of data protection is the relatively new Convention on Cyber Security and Personal Data Protection (AU

[1631] ibid, art 19(h).
[1632] ibid, art 13.
[1633] Graham Greenleaf, 'The UN Special Rapporteur: Advancing a Global Privacy Treaty?' (2015) 136 Privacy Laws and Business International Report.
[1634] supra note 143.
[1635] supra note 167, p. 53.
[1636] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391 art 8.
[1637] The Treaty on the Functioning of the European Union (2007) OJ C 326/01 art 16.
[1638] Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (DPD) (1995) OJ L281/31.
[1639] General Data Protection Regulation (Reg(EU) 2016/679).

Convention),[1640] adopted by the African Union. The AU Convention represents a significant step towards the enhancement of human rights, in particular data protection in Africa. The AU Convention was adopted in July 2014. It has a broad scope and covers three substantial areas, namely electronic transactions, personal data protection, together with cyber security and cyber crime.[1641] In this sense, the Convention is very broad in scope as it seeks to regulate in one legal instrument Africa's most pressing and diverse problems in relation to information and communication technology, that is electronic transactions, data protection and cyber security. As regards data protection, the AU Convention has two main objectives. The first is the requirement that state parties are to 'establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data and to punish any violations of privacy without prejudice to the principle of free flow of data'.[1642] The second objective requires that such framework established by member states 'shall ensure that any form of data processing respects fundamental freedoms and rights of natural persons while recognizing the prerogative of the State, the rights of local communities and the purpose for which the businesses are established'.[1643] The AU Convention is applicable to any processing carried out on the territory of the 54 state parties of the African Union. The treaty contains many safeguards regarding the data protection that mirror the CoE Convention 108 and EU Data Protection Directive. However, it also contains a number of weak provisions, that may give room for misuse. One example is an exception in Article 14(2) that allows for processing of personal data without the data subject giving consent on the grounds of 'public interest'.[1644] Equally, Article 33(1)[1645] is seen as possibly giving too much authority to courts and investigatory judges to access personal data and conduct surveillance.[1646] Other problems relate not so much to the general nature and the content of the Convention, but its implementation. Since its adoption in June 2014 no African state has yet ratified it.[1647] The AU

[1640] African Union Convention on Cyber Security and Personal Data Protection (27 June 2014) EX.CL/846(XXV).
[1641] ibid.
[1642] ibid, art 8(1).
[1643] ibid, art 8(2).
[1644] ibid art 14(2)
[1645] ibid, art 33(1).
[1646] Henry Roigas, "Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection' (20 February 2015) CCDCOE *Incyder News* < https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html>
[1647] African Union Convention on Cyber Security and Personal Data Protection, Status List (1 June 2016)

Convention requires that at least 15 countries do so, before it can come into force. Some commentators point out that attaining this number of ratifications will probably take years before the Convention takes effect.[1648] Additionally, even if the specified number of ratifications is achieved, African states tend to merely ratify treaties, without taking the necessary steps to implement them. The AU Convention is not a self-executing treaty, but requires in Article 8 that 'each state party shall commit itself to establishing a legal framework', which means that its provisions will not be enforceable in courts without prior legislative implementation. Thus, the effect of the Convention on the region will take time to be fully ascertainable. It seems therefore that 'integration on an African-wide scale is extremely ambitious especially because of population and size of the African continent'.[1649] Equally, the reluctance of the African states to ratify the instrument means that its impact as a global data protection standard will take a long time to be established.

In view of the above, neither the EU data protection regime (being legally binding on EU member states only), nor the AU Convention (being still at the very early stages of adoption and implementation by state parties) seem to be able at this stage to provide the basis for the global data protection standards. In this sense, CoE Convention 108 is viewed as 'having potentially a universal application'.[1650] However, despite the many advantages of 'globalization' of Convention 108, some issues need further clarification, not least of which is the individual enforcement rights for non-Europeans and the relationship between the Convention and Article 17 ICCPR. Under the current regime, European countries cannot accede to Convention 108 without first being a party to the ECHR.[1651] Europeans are able to bring an action before the ECtHR and enforce Convention 108 indirectly, which places non-European at a disadvantage. One solution would be that Convention 108 places an obligation on all non-European countries seeking accession to Convention 108 to also accede to regional

< https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf>.

[1648] Lukman Adebisi Abdulrauf and Charles Maga Fombad, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?' (13 June 2016), Journal of Media Law, <http://www.tandfonline.com/doi/citedby/10.1080/17577632.2016.1183283?scroll=top&needAccess=true>.

[1649] ibid p. 23.

[1650] Christopher Kuner 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 Computer Law and Security Review 313.

[1651] supra note 190.

human rights agreements and/or be a party to the ICCPR and its 1st Additional Protocol.[1652] This would give those individuals an option to enforce their data protection rights via their national courts and allow them to make 'communications' (complaints) to the Human Rights Committee that Convention 108 is not observed by their country. Such a complaint mechanism would empower the Committee to make recommendations (but not binding decisions) to member states placing non-Europeans, whose state ratified both Convention 108 and the ICCPR 1st Additional Protocol, closer to the position of the Europeans.[1653] The Special Rapporteur Cannataci has endorsed Convention 108 as one of the key contributors to global protection of privacy and his mandate includes the identifying of the principles and best practice for protecting privacy at international level.[1654]

In view of the fragmented nature of the existing legally binding data protection regimes, the lack of an international organization to oversee the implementation and adoption of a global standard and the differences between the various regional systems of data protection laws, the adoption of an international legal framework is challenging. Nevertheless, the Council of Europe Convention 108 presents at present perhaps the best candidate for an international data protection benchmark. Another option, discussed in the next part of this chapter, is the use of soft law to aid privacy and help towards reducing mass surveillance through diplomatic means.

PART II: THE USE OF SOFT LAW AND CONFIDENCE BUILDING MEASURES

a. Solution 5- Soft Law Instruments

i. Soft Law in International Law Making

Soft law is best understood as a descriptive tag for a variety of non-legally binding instruments used in contemporary international relations by states and international organizations.[1655] It

[1652] Optional Protocol to the International Covenant of Civil and Political Rights (UNGA 2200A(XXI) (entered into force 23 March 1976).
[1653] supra note 146.
[1654] supra note 58.
[1655] Malcolm D. Evans, *International Law* (Oxford University Press, 2015), p. 120.

comprises of, *inter alia*, inter-state conference declarations,[1656] UN General Assembly instruments,[1657] together with resolutions, declarations, codes of conduct, guidelines and recommendations. Soft law agreements are not subject to international treaty law, (Article 2(1)(a) of the Vienna Convention on the Law of the Treaties), particularly its central principle of *pacta sunt servanda* and therefore the legal consequences arising from non-fulfilment of the key commitments contained in these instruments.[1658] In this sense, international law does not attribute to soft law the status of a source of law,[1659] as it does not directly produce customary international law. However, it may nevertheless produce certain legal effects. These can 'range from providing the evidence of the state practice and *opinio juris* required to establish a rule of customary international, through providing assistance in the interpretation and application of conventional and customary law whose precise requirements remain unclear, to indicating the likely future course of international law's development'.[1660] Therefore, soft law can potentially be law- making in a similar way to multilateral treaties because it evidences at least an element of good faith commitment, a desire to influence state practice, or express some measure of law making intention.[1661] Soft law is not regarded by states as substitutes for treaties, but as an independent tool, which can be use to regulate their behaviour in cases where, a treaty may not be an option.[1662] As such, it may be a viable alternative to law making by treaty for a number of reasons. First, it may be easier for states to reach agreement, especially when they are not ready to assume legal obligations, but wish to undertake some kind of commitment short of a legally binding one. Secondly, soft law instruments are flexible and as such will normally be easier to supplement, amend or replace than treaties.[1663] Thirdly, treaties take a long time not only to negotiate, but also to replace, or amend. Fourthly, soft law instruments may provide more immediate evidence of international support and consensus than a treaty, whose impact is heavily qualified by reservations and the need to wait for ratification and entry into force.[1664] Finally, the soft law norm may be the short term solution chosen in order to

[1656] for example, the Rio Declaration on Environment and Development 1992.
[1657] for example, the Universal Declaration of Human Rights 1948; Declaration of the Rights of Indigenous Peoples 2007.
[1658] Hartmut Hillgenberd, 'A Fresh Look at Soft Law' (1999) European Journal of International Law, 499-515, p. 513.
[1659] ibid, 514.
[1660] Stephen Hall, 'Researching International Law' in Mike McConville and Wing Hong Chui *Research Methods for Law* (Edinburgh University Press 2007), p. 203.
[1661] ibid, p. 120.
[1662] supra note 212, 515.
[1663] ibid.
[1664] ibid.

prepare the consensus necessary until a hard law rule may emerge in the long run, whether in the form of a new legally binding agreement, or a customary rule derived from state practice.[1665]

ii. UN General Assembly Resolutions on the Right to Privacy in the Digital Age

A number of soft law instruments have emerged at the UN level in the aftermath of the Snowden revelations. Among these are UN GA resolutions on the right to privacy in the digital age.[1666] Resolution 68/167, discussed in Chapter 4 of this study, initiated the UN process to protect privacy and other human rights online and was followed by resolution 69/166.[1667] This latter resolution reiterated that 'surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework' and that 'any interference with the right to privacy must not be arbitrary or unlawful'.[1668] The Resolution also for the first time referred explicitly to the collection of metadata,[1669] the responsibility of business enterprises to respect human rights[1670] and stated that any measure taken by states to supress, or prevent terrorism must comply with states obligations under international human rights.[1671] Moreover, it called on member states to 'provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human right obligations'.[1672] A year later the UN Human Rights Council (HRC) adopted resolution 28/16 which also urged states to provide 'an effective remedy' and encouraged the Human Rights

[1665] Antonio Segura-Serrano, 'Internet Regulation: A Hard Law Proposal', (2006) Jean Monnet Working Paper 10/06 < http://www.jeanmonnetprogram.org/wp-content/uploads/2014/12/061001.pdf>, p. 7.
[1666] supra note 53.
[1667] ibid.
[1668] ibid.
[1669] ibid. The preamble acknowledged that metadata 'can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity'.
[1670] ibid. UN Human Rights Council, 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie' (21 March 2011) UN Doc A/HRC/17/31,
[1671] ibid.
[1672] ibid para 4(e).

Council to identify 'principles, standards and best practice' for protection of privacy.[1673] Consequently, the HRC decided to appoint for a period of three years a special rapporteur on the right to privacy, whose mandate includes, *inter alia*, 'to identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices as the national, regional and international levels and to submit proposals and recommendations to the Human Rights Council'.[1674]

These are significant developments, which testify to the deep concern with state sponsored cyber surveillance. They may also have an impact on states behaviour in cyberspace, if they become customary international law. Generally, UN General Assembly resolutions are non-binding, but they do constitute evidence of state practice and understanding of the law. Therefore, in time they may be converted into a binding customary law.[1675] This would depend on states' practice, including the consistency in voting for the resolutions and the existence of *opinio juris.* The International Court of Justice in the *Legality of the Threat or Use of Nuclear Weapons* Advisory Opinion[1676] stated that:

> [t]he General Assembly Resolutions, even if they are not binding, may sometimes have normative value. They can in certain circumstances, provide evidence important for establishing the existence of a rule or the emergence of *opinion juris*. To establish whether this is true of a General Assembly resolution, it is necessary to look at its content and the conditions of its adoption; it is also necessary to see whether an *opinio juris* exists as its normative character. Or a series of resolutions may show the gradual evolution of the *opinio juris* required for the establishment of a new rule.

Both resolution 68/167 and 69/166 have been adopted without a vote and at least one seems to be a result of a political compromise.[1677] Therefore, it could be said that these resolutions are influential in that they emphasise the role and importance of international human rights law in

[1673] UN Human Rights Council, Resolution 28/16 The Right to Privacy in the Digital Age, (1 April 2015) UN Doc A/HRC/28/18.
[1674] ibid, para 4(c).
[1675] Malcolm Show, *International Law* (Cambridge University Press, 2008), p. 115.
[1676] *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion ICJ Reports, 1996, 226, pp. 254-5.
[1677] Adam Jusitce, 'UN Committee Spotlights "Highly Intrusive" Digital Spying' (2014) Reuters < http://www.reuters.com/article/us-spying-un-idUSKCN0J92I120141125>. A reference to metadata surveillance as an intrusive act was removed from resolution 69/166 to appease the Five Eyes alliance.

cyberspace, particularly in relation to state sponsored surveillance. However, at this stage they probably have only a political, rather than normative value. Nevertheless, in time they may be converted into legally binding rules, as a result of either formalization into a binding treaty, or by acceptance as a customary rule, provided that the necessary conditions (consistent state practice and *opinio juris*) have been fulfilled.

iii. Soft Law and Data Protection

The first UN instrument dealing directly with data privacy was a 1968 resolution of the General Assembly 2450,[1678] which resulted in a report of 1976 urging states to adopt data privacy legislation covering computerised personal data systems in the public and private sector and listing minimum standards for such legislation.[1679] In 1990 the UN GA adopted a set of non-legally binding Guidelines Concerning Computerized Personal Data Files (UN Guidelines).[1680] The Guidelines lay down minimum guarantees for inclusion in national data privacy laws[1681] and encourage international organizations (governmental and non-governmental) to process personal data in a responsible, fair and privacy friendly manner.[1682] The Guidelines contain some progressive elements, such as for example the 'principle of accuracy',[1683] the 'principle of purpose specification'[1684] and the 'principle of interested-person access'.[1685] They also address the flow of data across borders stipulating that:

[1678] UN General Assembly Resolution 2450 of 19 December 1968 UN Doc E/CN.4/1025.
[1679] Points for Possible Inclusion in Draft International Standards if the Protection of the Rights of the Individuals against Threats Arising from the Use of Computerized Personal Data Systems' UN Doc E/CN.4/1233.
[1680] Guidelines Concerning Computerized Personal Data Files (UN General Assembly Resolution 45/95 of 14 December 1990) UN Doc E/CN.4/1990/72.
[1681] ibid, Part A.
[1682] ibid, Part B.
[1683] ibid. Part A- Principles Concerning the Minimum Guarantees That Should Be Provided in National Legislations, para 2 (Principle of Accuracy):

> [p]ersons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

[1684] ibid, para 3 (Principle of Purpose Specification):

> [t]he purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned […]'

[1685] ibid, para 4 (Principle of interested-person access):

> [e]veryone who offers proof of identity has the right to know whether information

> [w]hen the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.[1686]

However, the Guidelines have not been very popular and made an insignificant practical impact.[1687] One reason may be the lack of definitions of its central terms, such as 'personal data', 'personal data file', and 'comparable' or 'reciprocal' safeguards, which makes these terms more diffuse, loose and confusing.[1688]

A fair number of other non-legally biding soft law regional data privacy initiative have been undertaken, many outside Europe. Notable in this regard are the Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data; the Asia-Pacific Economic Cooperation (APEC) [1689] 'Privacy Framework' [1690] and the Association of South East Asian Nations (ASEAN)[1691] harmonized data privacy regimes.[1692] Beyond these relatively recent initiatives is a whole host of bodies and interest groups advocating strong regimes for protecting of

---

> concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries, and when it is being communicated to be informed of the addressee. Provision should be made for the remedy, if need be with the supervisory authority […]. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

[1686] ibid, para 9 (Principle of Transborder Data Flows).
[1687] ibid.
[1688] Bygrave, supra note 167, p. 53.
[1689] ibid p. 75. The APEC states are Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, the Russian Federation, Singapore, Taiwan, Thailand, the USA and Vietnam.
[1690] ibid. This is another non-legally binding regional instrument inspired by and modelled upon the OECD Guidelines.
[1691] ibid, p. 79. The ASEAN comprises ten nations, namely Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.
[1692] ibid. The regime aims to develop harmonized legal infrastructure for e-commerce but little information is publically available as to precisely what kind of harmonized regimes ASEAN is aiming at apart from the fact that they are to accord with best practices/ guidelines'.

personal data, such as the Data Protection Working Party set up under Article 29 of the EU Data Protection Directive (A29WP) mentioned in Chapter 1 and 4 of this thesis, the International Working Group of Data Protection and Telecommunications, the Asia-Pacific Privacy Authorities as well as civil society groups, such as Electronic Privacy Information Centre and Privacy International.[1693]

iv. Soft Law as a Tool to Enable Data Transfers

The issue of transborder data flows has historically been problematic as different countries offer varied standards of data protection. This was one of the main reasons for the European Union adopting a legally binding data protection framework, with the Data Protection Directive having the greatest international impact on data transfers to countries outside the EU. Articles 25-26 of the Directive contain a comprehensive ban on transfers to states that do not provide an adequate level of protection of personal data and reflects European officials' mistrust the US legislation, which was viewed as insufficiently protective of them.[1694] As a result of these concerns, an international understanding between the US and the EU had to be reached in order to avoid disrupting data flows. This was achieved by means of a non-legally binding instrument, called the *Safe Harbour Agreement* between the US and the EU.[1695] The scheme allowed for the flow of personal data from the EU to US organizations that through self-certification voluntarily agreed to abide by a set of data privacy principles based loosely on the EU Data Protection Directive. Initially the scheme was recognized as a 'resounding success, both in terms of raising the level of privacy compliance in the USA and in facilitating the recognition by the US business that privacy is a critical factor to success in the global marketplace'.[1696] However, it soon became subject of criticism for the role it played in obtaining data from PRISM by majority of private companies, who became party to it. Reportedly a number of major US based corporations were collaborating in PRISM and related surveillance programmes of the NSA, enabling the latter to gain ready access to personal data

[1693] ibid, p. 19.
[1694] supra note 195, p. 16.
[1695] Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.
[1696] Damon Greer, 'Safe Harbour-a Framework That Works' (2011) 1 International Data Privacy Law, p. 143.

kept on, or transmitted between the corporations' servers.[1697] This collaboration has been allegedly over the above what has been legally required of these corporations.[1698] According to the European Commission, the *Safe Harbour* scheme has been 'one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU.'[1699] This led to the Court of Justice of the European Union (CJEU) annulment of the scheme in *Maximilian Schrems v Data Protection Commissioner*.[1700] The main reason was that the law and practice of the US did not offer sufficient protection against the NSA surveillance by the public authorities of the personal data transferred from Europe to that country. The CJEU noted that the scheme was applicable solely to the US undertakings and not to the US public authorities. Furthermore, national security, public interest and law enforcement requirements of the US prevailed over the *Safe Harbour Agreement*, so that US companies were bound to disregard, without limitation, the protective rules laid down by that scheme where they conflicted with such requirements. Indeed, the CJEU observed that the agreement enabled interference by the US public authorities with the fundamental rights of European citizens. Specifically, the US authorities were able to access the personal data transferred from the EU member states to the US and process them in a way incompatible with the purposes, for which they were transferred and beyond what was strictly necessary and proportionate to the protection of national security.[1701]

From an international law perspective, the *Safe Harbour Agreement* was not an international treaty, as it was neither signed nor ratified and therefore not subject to the Vienna Convention on the Law of the Treaties.[1702] It is an example of an informal international cooperation. It also illustrates the fact that being non-binding, it was relatively quick and easy for the European Commission and the US authorities to replace it. This was achieved by negotiating a new scheme, called the *EU-US Privacy Shield* in July 2016, not even a year after the *Safe Harbour Agreement* was annulled. The *Privacy Shield's* aim is to provide companies on both sides of the Atlantic with the mechanism to comply with EU data protection requirements when

---

[1697] Yann Padova, "Prism Scandal Threatens EU-US 'Safe Horbour' Agreement" (12 November 2014), <http://www.euractiv.com/section/justice-home-affairs/opinion/prism-scandal-threatens-eu-us-safe-harbour-agreement/>.
[1698] ibid.
[1699] Fanny Coudert, 'Schrems vs Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities' (15 October 2015) European Law Blog, < http://europeanlawblog.eu/?p=2931>.
[1700] *Schrems*, supra note 65.
[1701] ibid.
[1702] Segura-Serrano, supra note 222, p. 17.

transferring personal data from the European Union to the United States in support of transatlantic commerce.[1703] This framework is said to impose stronger obligations on US companies to protect Europeans' personal data and it is based on a set of new, robust principles, not previously found in the *Safe Harbour Agreement*. Among these are the principles of transparency obligations of the US government access to data, several possibilities regarding the redress mechanism for individuals, as well as annual joint review mechanism. As to the safeguards and transparency obligations of the US, the US government has given the EU a separate, written assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversights mechanisms.[1704] The US has ruled out indiscriminate mass surveillance on personal data transferred to the US, whilst bulk collection of data would only be used under specific preconditions and needs to be as targeted and focused as possible.[1705] Furthermore, for the first time the P*rivacy Shield* promises that any individual who considers that their data has been misused under the scheme will benefit from several accessible and affordable resolution options, including free of charge alternative dispute resolution, resort to their national Data Protection Authorities and, as a last resort, an arbitration mechanism.[1706] Redress possibility in the area of national security for the EU citizens will be handled by an Ombudsperson independent from the US intelligence service.[1707] The additional safeguards, in the form of an annual joint review, promises that the European Commission and the US Department of Commerce will conduct the review and the Commission will issue a public report to the European Parliament and the Council.

v. Soft Law and Access to Data by Law Enforcement Agencies

In the sphere of transfers of data for the purposes of obtaining evidence in criminal investigations by the law enforcement agencies (LEAs) explored in Chapter 4 of this thesis,

---

[1703] US Department of Commerce Fact Sheet, 'Overview of the EU-US Privacy Shield Framework for Interested Participants' (12 July 2012) <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf>.
[1704] European Commission Press Release, 'European Commission Launches EU-US Privacy Shield: Stronger Protection for Transatlantic Data Flows' (12 July 2016) <http://europa.eu/rapid/press-release_IP-16-2461_en.htm>.
[1705] ibid.
[1706] ibid.
[1707] ibid.

the Council of Europe in 1987 adopted Recommendation No. R (87)15 (the Recommendation) on the Use of Personal Data in the Police Sector. These soft law agreements amongst European states provides guidance for the collection, storage, use and communication of personal data for police purposes that are subject of automatic processing.[1708] Although not legally binding, the Recommendation has been widely adopted across Europe-in 30 out of 47 Council of Europe member states.[1709] It restricts data transfers to foreign authorities by providing that this can be done only by police bodies.[1710] All other transborder transfers are allowed on specific grounds:- namely, if there exists a clear legal provision under national or international law, or in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger, is necessary for the suppression of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence under ordinary law.[1711] An investigation into the practice of states carried out twenty-five years since the adoption of the Recommendation revealed[1712] that many European states *prima facie* regulate police use of personal data in a way compatible with the Recommendation. The Report found disparities in the way that states chosen to implement Recommendation, but bearing in mind that it is a soft law instrument, it conceded that it still left its mark across Europe. Greater harmonization within the European states was nevertheless recommended. Meanwhile a legally binding EU Directive (Draft Directive 5833/12) on processing of personal data for police purposes is currently under way.[1713] However, even if greater legislative harmonization of the Recommendation is to take place regarding its implementation, the open-textured norms and broad, general clauses (such as the 'legitimate interest test') will inevitably continue to be

[1708] Recommendation No. R (87) 15, Scope and Definitions:

> '[t]he principles contained in this recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing.'

[1709] Council of Europe Report, 'Recommendation R(87)15- Twenty Five Years Down the Line' (23 September 2013) < http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf>.

[1710] ibid, art 5(4) International Communication: Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

> a. if there exists a clear legal provision under national or international law,
> b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced.

[1711] ibid.

[1712] supra note 266.

[1713] Council of the European Union, Proposal for a Directive 5833/12 (16 December 2015).

interpreted and applied differently across varied legal cultures and traditions.[1714] In addition and perhaps more importantly, the Report emphasized that data controlled by private commercial organizations (such as Google, Facebook, Chrome etc.,) are open to scrutiny and potential abuse by both the law enforcement and intelligence agencies, as was brought to the public attention by Snowden in 2013.[1715] It was also acknowledged that LEAs require timely, but measured access to personal data in order to prevent and detect crime, as delays could potentially put human life, dignity and privacy at risk. This creates a need for pre-authorization,[1716] which can only be properly provided by binding laws and an oversight by an agency with powers, which transcend national jurisdictions. The Report concluded that none of this is achievable without the right legally binding framework. It noted that at present neither the Council of Europe through the Recommendation, nor the European Union in its Draft Directive 5833/12 provide a legal framework, that responds adequately to the realities, where national LEAs increasingly intrude into the personal data of the citizens of other states and where the data is under the control of a data controller in a third jurisdiction.[1717]

The highlighted developments in the field of data protection and transborder data flows reveal a cluttered ideological landscape with cross-cutting sets of norms and interests, such as human rights, trade and commerce, national security and law enforcement. Whilst soft law instruments, such as the Guidance of the OECD and the UN have proved influential in the development of the field of data protection, they seem under used or more or less abandoned. That does not diminish however the role that non-binding schemes play in shaping this area. The *Privacy Shield* is a good example of the flexibility of such instruments, in that it relatively easily replaced its predecessor the *Safe Harbour Agreement* following its invalidation by the CJEU. Bearing this in mind, it could be said that the use of these soft law agreements contributes to the development of international law as they guide state behaviour is the sphere of data protection and the transfers to data to a certain extent. As such, they are a valuable alternative to law making by treaty. In addition to these agreements, a number of recent diplomatic developments also point towards greater, informal cooperation among states discussed below.

[1714] supra note 269, p. 32.
[1715] ibid, p. 38.
[1716] ibid, pp. 38-39.
[1717] ibid.

vi. Confidence Building Measures

Confidence Building Measures (CBM) 'are actions and procedures undertaken within the context of policy, legal and/or institutional framework(s) for the purpose of enhancing openness and transparency, assuring mutual understanding and reducing misunderstandings, threats and tensions among States'.[1718] They have long been used by the international community for the purpose of promoting peace and security and can be traced to the 1975 Helsinki Final Act,[1719] followed by the 1986 Stockholm Document on Confidence and Security Building Measures and Disarmament in Europe,[1720] together with the 1990 Vienna Document.[1721] According to the UN Disarmament Commission the main objectives of these measures are:

> [t]o reduce or even eliminate the cause of mistrust, fear, misunderstanding and miscalculation with regard to relevant military activities and intentions of other States, factors which may generate the perception of an impaired security and provide justification for the continuation of the global and regional arms build-up […] to reduce the risk of surprise attacks and of the outbreak of war by accident; and thereby, finally, to give effect and concrete expression to the solemn pledge of all nations to refrain from the threat or use of force in all its forms and to enhance [international] security and stability.[1722]

[1718] Ram S. Jakhu, 'Transparency and Confidence-Building Measures for Space Security' in Aley Lele (ed.), *Decoding the International Code of Conduct for Outer Space Activities* (Pentagon Security International 2012), 35-46, p. 36.
[1719] Organization for Security and Co-operation in Europe, Conference on Security Cooperation, 'Conference on Security Co-operation in Europe: Final Act' (1975).
[1720] Organization for Security and Co-operation in Europe, 'Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe' (19 September 1986).
[1721] Organization for Security and Co-operation in Europe, 'Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Co-operation in Europe' (17 November 1990).
[1722] UN General Assembly, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, UN Doc A/S-15/3 (28 May 2006).

CBMs have been adopted as either 'stand alone actions on in combination with other means: (a) to complement legally binding treaties, particularly those that facilitate verification of arms limitation and disarmament agreements; (b) to lay the foundations, as a first step, that could build the momentum for the future legal agreements or other binding instruments; and (c) to reduce mistrust, fear and misunderstanding in specific areas of human activity.'[1723]

Recognizing the importance that the internet plays in the delivery of basic services, on the critical national infrastructures and economic growth of nations, international community has engaged in the process of cyber diplomacy to build a global consensus on how to apply existing international law in cyberspace and develop norms of responsible state behaviour and of confidence building measures. These efforts have been initiated and coordinated by four consecutive United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGEs).[1724] The first group of experts was convened in 2004 at Russia's instigation with an aim to analyse international legal provisions relating to various aspects of international information security and study existing concepts and approaches.[1725] Another two reports from the UN GGE followed in 2010 and 2013.[1726] It was not however until the Report of the 2015 Group that a catalogue of confidence building measures aimed at reducing the risks of misperceptions and conflicts linked to the attacks on the information and communications technology enabled infrastructure was agreed.[1727] The 2015 UN GGE report reiterated the agreement reached by the 2013 UN GGE that international law, in particular the UN Charter applies to states' use of information and communications technologies.[1728] It also 'identified as of central importance the commitments of [s]tates to […] respect for human rights and fundamental freedoms and non-intervention in the internal affairs of other states.'[1729] The Report 'emphasised that States

[1723] supra note 275, p. 36.
[1724] Patryk Pawlak, 'Confidence-Building Measures in Cyberspace: Current Debates and Trends' in Anna Maria Osula and Henry Roigas (eds.), *International Cyber Norms: Legal, Policy and Industry Perspectives* (NATO CCD COE Publications, Tallinn 2016), pp.129-153.
[1725] ibid, p. 136.
[1726] UN GA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security' UN Doc A/68/98 (24 June 2013).
[1727] UN GA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015).
[1728] ibid, p 12.
[1729] ibid, p. 12.

should guarantee full respect for human rights, including privacy and freedom of expression'.[1730] The Group recommended that states should consider the adoption of a number of confidence building measures, among them 'the voluntary provision […] of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT [information and communication technology] enabled infrastructure.'[1731] The successive UN GGE reports therefore have laid down the foundations for the discussion about the confidence building measures in cyberspace, which also form foundations for the effort undertaken within regional organizations, such as the Organization for Security and Co-Operation in Europe and the ASEAN Regional Forum.[1732]

In recent years a number of bilateral agreements between some states have emerged, which are viewed as a way to provide additional guarantees that their signatories will behave responsibly in cyberspace. These include the US-Russia agreement of June 2013 (an agreement to reduce the risk of conflict in cyberspace through real time communications about incidents of national security concerns)[1733] and Russia-China agreement of May 2015 (a non-aggression agreement to refrain from cyber attacks against each other and to jointly respond to technologies that may have a destabilizing effect on political and socio-economic life or interfere with internal affairs of the state).[1734] It has to be said however that to date, confidence building measures concentrated on the need to address security challenges in cyberspace and not specifically on setting out the norms for responsible signals intelligence collection. However, in September 2015 the US and China have reached a cybersecurity agreement (Cyber Agreement), which aims at refraining from conducting mutual commercial espionage.[1735] Cyber espionage is understood as the theft of trade secrets, intellectual property and negotiating

[1730] ibid. p. 1.
[1731] ibid, p. 9.
[1732] supra note 281, p. 135.
[1733] Ellen Nakashima, 'U.S. and Russia Sign Pact to Create Communication Link on Cyber Security' (17 June 2013) *The Washington Post* <https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html?utm_term=.dc45f6655099>.
[1734] Andrew Roth, 'Russia and China Sign Cooperation Pact' (8 May 2015) *The New York Times* < https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0>
[1735] Scott Warren Harold, 'The US-China Cyber Agreement: A Good First Step' <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>

tactics with the intent of using the information to provide economic benefit to an commercial enterprise.[1736] The US-China Cyber Agreement provides for increased communication and cooperation between the two countries to investigate and prevent cyber crimes emanating from their territories and states that neither country's government would knowingly conduct or support cyber-enabled theft of intellectual property.[1737] It was also agreed that both countries are committed to identifying, developing and promoting appropriate norms of state behaviour in cyberspace within the international community and establishing a high-level joint dialogue mechanism on fighting cybercrime and related issues.[1738] The US-China agreement is undoubtedly the first step towards establishing of the international norms of state behaviour in cyberspace, in particular in relation to the espionage activities. Until the agreement was reached, China was reluctant to recognize economic espionage, as a distinct category of espionage.[1739] In this sense, President's Xi agreement that the Chinese government does not engage in, or knowingly support the theft of intellectual property in order to provide competitive advantage to private companies, is a recognition that there exists a type of cyber espionage distinct from national security espionage.[1740] This view has long been held by the US. Accordingly, cyber intelligence gathering pertaining the collection of information about economic and financial matters for the purposes of benefiting national security are routine intelligence activities not acts of cyber economic espionage.[1741] If both countries agree that spying for corporate profit is distinct from and less acceptable than state spying for national security purposes, this could have a profound effect on international norms. It may even eventually lead to the official recognition of another distinct form of espionage- cyber surveillance and the gradual setting out of norms to deal with that problem too.

Confidence building measures have the undoubted benefit of opening an international dialogue about matters, in relation to which states find difficult to reach a legally binding agreement. They are not regarded as substitute for treaties, but are perceived as standalone measures having normative value, or as supplementary mechanisms to other legally binding and non-legally binding measures. States have not yet addressed the issue of mass cyber

---

[1736] Gary Brown and Christopher D. Yung, 'Evaluating the US-China Cybersecurity Agreement, Part 1: the US Approach to Cyberspace' (19 January 2017) *The Diplomat* <http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>.
[1737] ibid.
[1738] ibid.
[1739] ibid.
[1740] ibid.
[1741] ibid.

surveillance through the mechanism of confidence building measures. Having said that, as shown above, a bilateral agreement has been reached between the US and China regarding cessation of economic cyber espionage. The voluntary and non-legally binding nature of such agreements means that they may be expanded to cover new policy areas, such as privacy protection challenged by mass surveillance. In this sense, they may contribute to opening a dialogue regarding not only cyber espionage, but also mass cyber surveillance and play a positive role in re-gaining the lost trust between states and international level. Eventually, they may also lead to the development of binding international law norms and/or international customary law.

CONCLUSION

The picture that emerges from the foregoing analysis is one of a fragmented landscape replete with legally and non-legally binding norms relating to privacy and data protection, which exist in a highly politicised cyber environment. This chapter recognized that limiting cyber surveillance will be incremental and achieved through a combination of updating and harmonizing the existing international human rights and data privacy legally binding norms, soft law agreements and diplomacy. There are no 'quick fixes'.

The privacy of communications is protected by international law (ICCPR, ECHR and ACHR) and these legally binding frameworks apply to the digital environment. This chapter analysed the need to both update and supplement these laws in the light of increasing state surveillance powers. The chapter has also identified a need to safeguard how data is accessed and processed by the intelligence and law enforcement agencies across jurisdictions in a way that protects digital communications. Although such a regime has been in existence for some time in the form of Convention 108, it remains regional in scope and the process to develop a global data privacy rules has only just begun. On an international level, data protection and data transfers are regulated by the ICCPR and a series of soft law agreements, most notable of which are the EU-US schemes. The 2013 Snowden disclosure of the NSA and its Five Eyes partners unconstrained surveillance, as well as unrestricted access to data held in foreign jurisdictions by law enforcement agencies, both in breach of the right to privacy of communications and data protection, saw a renewed interest in governing cyberspace through a hard law instrument.

There seems to be a broad consensus that cyberspace and the internet ought to be governed on this basis. A failed attempt was made to that end in 2011 and 2015 with a proposal of the *Draft International International Code of Conduct for Information Security*. Equally, a separate Additional Protocol to the ICCPR specifically addressing cyber surveillance and privacy has been put forward but rejected by the US. Nevertheless, a submission has been made by the Republic of Malta in 2015 to the UN General Assembly that the internet regulation should continue on the multistakeholder model but be based on the Common Heritage of Mankind applied by analogy with Article 136 UNCLOS 1982 to that domain. This indicates a renewed interest in the Common Heritage of Mankind with regards to its application to the internet governance and the future discussion in the UN General Assembly should reveal how receptive the wider international community is to this idea.

Having said that, negotiating a binding global cyber treaty is bound to take a long time and be fraught with difficulty, as evidenced by the protracted political processes involved in the internet governance thus far. In addition, apart from the loose consensus that the internet ought to remain open and that international law, including human rights law, applies it is still unknown how exactly the international human rights legal framework is to fit in and what institution should be in charge of overseeing the implementation of such a treaty. Faced with this reality, an interim solution could be a multilateral treaty regulating only selected aspects of unlawful behaviour in cyberspace, particularly cyber surveillance. Addressing this problem through a regional treaty for the European states aimed at regulation of the working methods of the intelligence agencies has recently been proposed by the Council of Europe. However, states' reaction to the proposal has been rather muted.

For these reasons, the most realistic solution at this stage appears to be the reliance on and further development of soft law instruments, together with the broadening of the scope of confidence building measures to cover mass cyber surveillance. In addition to these non-legally binding and diplomatic efforts, the work to expand the scope of the Council of Europe Convention 108 must continue together with the redefining of the scope of the protected right under Article 17 ICCPR fit for the 21st by the UN human rights treaty bodies.

Chapter 6: 'Concluding Observations'

The catalyst for this research were the 2013 disclosures of mass surveillance of Edward Snowden. The thesis focused on the mass surveillance activities of states, as against private multinational entities, since states remain the major actors and participants in the international legal system[1742] and are the primary focus for the social activities of humankind and thus for international law. [1743] This state sponsored surveillance forms part of their broader cyber espionage activities. There is sufficient evidence based in current state practice to suggest that these activities are not only set to continue in the current form, but that they will gain in propensity because of innovation and improvements in digital technologies. The thesis therefore advanced that cyber surveillance ought to be treated as a disparate and separate sub-category of cyber espionage by international law for the purposes of its future regulation. This could facilitate the formulation and development of a much needed legal framework aimed at regulating the working methods of state intelligence and law enforcement agencies.

All major United Nations organizations, (such as the General Assembly), human rights treaty bodies, (including the Human Rights Council and the Office of the High Commissioner for Human Rights), regional human rights organizations (such as the Council of Europe), not to mention the courts (the Court of Justice of the European Union and the European Court of Human Rights) expressed uniform condemnation of these large scale and unjustified privacy violations. It has been widely recognized that the right to privacy of communications contained *inter alia* in Article 17 ICCPR and Article 8 ECHR applies equally online as well as offline. Yet, as this thesis showed these legal frameworks are no longer adequate to address the threats to privacy and other rights in the rapidly evolving digital environment. For most part, the law is outdated, too general and fragmented to provide sufficient protection for individuals world-wide against the power of states to continue in their unfettered signals intelligence gathering practices ostensibly for national security purposes. In addition, it remains largely unsettled how the right to online privacy relates to states' cyber surveillance conducted abroad. An example of such uncertainty is the lack of consensus among the International Group of Experts preparing

[1742] Malcolm Show, *International Law* (Cambridge University Press, 2008), p. 196. Other participants in contemporary international law law are international and regional organizations, non-governmental organizations, public companies, private companies and individuals.
[1743] ibid, p. 197.

the *Tallinn Manual 2.0* in relation the extraterritorial application of human rights treaties.[1744] This is a fundamental, yet unsettled matter, which is exacerbated by the unjustifiable discrimination made in the legislation of the Five Eyes, which differentiates between internal/external communications and/or those between nationals/non-nations of the country conducting surveillance. Equally, the granting of surveillance powers of interception in domestic laws that provides for different procedural standards depending on whether the intercepted communications are external/internal, or foreign/domestic is discriminatory and contrary to the concept of universal human rights. This distinction is meaningless in the cyber context, as most internet communications will inevitably involve data travelling through a multitude of jurisdictions, even if both the sender and the recipient reside in the same country.

The human rights treaty bodies and regional human rights organizations have made repeated calls on states to bring their secret, often outdated and inadequate legislation authorising the activities of the intelligence agencies in line with the human rights obligations. State practice evidences that these calls have not been heeded. In many respects, a number of states adopted more draconian surveillance powers in their domestic systems in the time that this research has been conducted. In this sense, the practice of states and the wishes of international human rights organizations operate as 'parallel universes', almost totally disregarding each other.

This situation makes reform necessary. What does not help however is the fact that international human rights framework lags behind the rapid technological changes brought about by the 'digital revolution'. This in part accounts for calls from some states in the aftermath of the 2013 Snowden disclosures for a global hard law solution in the form of a new digital international human rights treaty by means of a new additional protocol to Article 17 ICCPR. Although the specially appointed in 2015 Special Rapporteur on the right to privacy, Professor Cannataci, has recognized the need to develop international law relevant to privacy, he emphasised that a new global all encompassing international convention covering all of

[1744] Micheal N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2017). See the commentary to Rule 34- '[t]the International Group of Experts could achieve no consensus as to whether [s]tate measures that do not involve an exercise of physical control may qualify as 'power or effective control' in the sense of this Rule. In particular, no consensus could be reached as to whether [s]tate activities conducted through cyberspace can give rise, as a matter of law, to power or effective control over an individual located abroad, thereby triggering the extraterritorial applicability of that [s]tate's international human rights law obligations'.

privacy and internet aspects is not envisaged. Equally, the US expressed no interest in such a solution. The alternative ways to address the problem is through the process of modernizing and supplementing the existing privacy standards by the human rights treaty bodies, for example by replacing the outdated General Comment No. 16. Other options include the process of Universal Periodic Review of states' compliance with their privacy obligations.

As there is no body of international law (either treaty or customary law rules) to regulate peacetime espionage, there is nothing to draw an analogy from regarding cyber espionage. This is partly due to the fact that historically states have been reluctant to subject peacetime espionage to regulation through international treaties. This situation has changed markedly with the wielding of mass surveillance programmes world-wide post 11 September 2011. Consequently, some states together with international human rights organizations called for specific 'no-spy' hard law instruments to address these practices. There can be no doubt that such a solution is needed, but whether it is achievable depends on the political will of states, in particular those with the greatest cyber surveillance capabilities. Bearing in mind the recent trends towards the adoption of more draconian surveillance laws, in such countries as the UK (the Investigatory Powers Act 2016) or the US (the Cybersecurity Sharing Act 2015), coming to fruition of such an agreement seems allusive. Hard law regulation of state intelligence and law enforcement agencies is at this stage most likely to be achieved either through the cooperation of a small group of states, agreeing to a legally binding regional treaties (for example the Council of Europe or the Shanghai Cooperation Organization member states), or soft-law bilateral instruments (such as the US-China Cyber Espionage Agreement 2015), which may eventually lead to hard law and/or the development of customary international law rules.

Moreover, that the international community will come together and agree to a cyber treaty to regulate a whole host of cyber activities in one international document may be desirable, but seems far off. This thesis had considered the theoretical foundations for such an instrument, proposing the application by analogy of some of the legal structures contained in the United Nations Convention on the Law of the Sea 1982 (UNCLOS 1982). The tendencies in state practice indicate that the content layer of cyberspace, as a legal domain can be best analogized with the Exclusive Economic Zone/Continental Shelf regimes. It does not have the characteristics of sovereign territory, *terra nullius* or a global common. Many states show increasing tendencies to regulate activities over their parts of the content layer, whilst performing unlawful interception and bulk collection of content and metadata at home and abroad. Regulation of these activities may be possible, at least in theory, through an explicit recognition of separate but interrelated zones (akin to the Exclusive Economic

Zone/Continental Shelf regimes set out in the UNCLOS 1982). Furthermore, the applicability and utility of the principle of Common Heritage of Mankind to the internet has been recognized and endorsed in international forums, such as the UN General Assembly. It may well serve to protect future free flow of information.

Above all, it is states and their intelligence and law enforcement agencies who must have clear operational standards in order to discharge their national security/law enforcement duties and do so within the rule of law. This can only be achieved if international law defines such parameter, together with meaningful judicial oversight on national level, enforcement and redress mechanisms for non-compliance. At the moment the law on privacy and data protection is fragmented and replete with often outdated mixture of soft law instruments and treaties- on international, regional and domestic levels.

As this thesis has shown, much has been debated on surveillance since Edward Snowden 2013 disclosures. His revelations as well as information obtained in official inquiries or exposed by journalists, academics and civil society provided information in relation to the global surveillance programmes of the UK and the US. This study has focused principally on the activities of these two countries. The question that is pertinent at this stage is 'has state practice changed since the 2013 Snowden disclosures as a result of these world wide condemnations'? The research conducted since 2013, in particular that of the University of Cambridge Faculty of Law in a study titled *Boundaries of Law: Exploring Transparency, Accountability and Oversight of Government Surveillance Regimes* (*Boundaries of Law*),[1745] reveals that the answer to that question is negative. The study showed continued and exponential growth in indiscriminate, generalized mass surveillance between 2013-2017. It went beyond domestic and global surveillance of the UK and the US and based its analysis on a diverse selection of 14 counties from five different continents, namely Columbia, Democratic Republic of the Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, the United Kingdom and the United States.[1746] The key findings paint a bleak picture that the *Boundaries of Law* summarised in ten points:

1. 'globally, legal surveillance frameworks are ineffectual. [..] The overwhelming majority of countries lack effective checks and balances on mass surveillance

[1745] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, 'Boundaries of Law: Exploring Transparency, Accountability and Oversight of Government Surveillance Regimes' (March 2017), Paper No 16/2017, University of Cambridge Faculty of Law < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490 >.
[1746] ibid, p. 15.

powers. Not only are legal surveillance frameworks on "international communications" very weak in the US and the UK, but the laws and practices in may other countries are just as bad, and in some cases worse. These frameworks are so feeble that they allow governments to interfere arbitrarily with the right to confidentiality of communications of hundreds of millions of people worldwide by collecting data in bulk without proven cause for suspicion';[1747]

2. the right to privacy is guaranteed in principle, but not respected in practice. In all 14 countries the right to confidentiality of correspondence is expressly protected (either through a constitution or the incorporation of international human rights standards into the domestic legal system). The countries surveyed impose serious substantive and formal constraints on interception in criminal cases. However, these constrains tend only to apply to the interception of the content of communications and are often undermined by loopholes, secret laws, extra-legal proceedings and interference with network operators and telecommunication service providers so as to weaken these safeguards in practice;[1748]
3. there is even less constraint on access to metadata than on content data;
4. 'national security' is so broadly defined, it is meaningless. The study considered this as one of its 'most warring findings' stating that 'vague laws often allow unlimited or barely limited access to both metadata and the content of user communications by law enforcement and/or national security agencies, outside of the normal framework for criminal investigations in the name of "national security"'.[1749] It explains that 'the Johannesburg Principles on National Security, Freedom of Expression and Access to Information'- a document which was drafted by civil society and endorsed by the UN Special Rapporteurs stresses that the notion 'national security' should be limited to real, immediate threats to the very existence of the state or the democratic order. However, the study found that 'in many countries the concept is stretched to include for example the fight against organized crime and the protection of the economic interests of the state (France, Germany), the prevention of incitement to commit [apparently any] offences (India), anything relevant to the country's 'international affairs (the USA), or any 'national interest'

[1747] ibid, p. 8.
[1748] ibid.
[1749] ibid.

(Kenya). In other cases, it is deliberately undefined (the UK), or left to the discretion of the authorities (Egypt)';[1750]

5. mass surveillance rarely requires judicial authorisation. Mass surveillance in many countries may be authorised by government (Myanmar, Pakistan); a minster (the UK); the prime minister (France); the president (the US); senior officials (India); the police, the military and the intelligence services (Columbia, DR Congo, Egypt); or indeed 'any authorised agency' (Turkey). Kenya, Russia and South Africa requires judicial authorisation, but no evidence of any actual crime or plot is required and 'national security' is defined so broadly that the threshold for granting authorisation is very low. Consequently, the relevant judges are given such little leeway to reject requests that it cannot be considered effective judicial control in practice';[1751]
6. governments can demand direct access to telecommunications infrastructure through 'back doors'. The study concluded that the authorities of most surveyed states under their laws demand that Telecommunication Service Providers (TSPs) and Mobile and Other Network Operators ((M)NOs) install devices to facilitate interception and that this would be interpreted as including 'back doors'. This grants the authorities direct access to the systems of these providers and operators that can not be monitored by the companies themselves;[1752]
7. laws under which untargeted mass surveillance takes place are secret and opaque. Although under international law all legal rules, in particular those that allow for interference with fundamental rights, must be publically accessible, in most surveyed countries some laws and primary rules appear to be kept secret (for example Columbia, Russia and Pakistan). This also relates to the subsidiary rules and guidelines on or interpretation of the law (DR Congo, Egypt, Kenya, Myanmar, India, South Africa and Turkey). Even in the US and the UK the most important rules and guidelines and legal interpretations underpinning surveillance have been kept secret until exposed by Snowden or forced into open litigation. In France the recently adopted law (the 2015 French 'Patriot Act') contains a provision that allows for secret decrees by the Conseil d'Etat to regulate the details of the relevant surveillance. In addition, there is very little transparency about the actual practices.

[1750] ibid.
[1751] ibid, p. 5.
[1752] ibid.

In Columbia, Pakistan, Russia and the UK for example, the law either expressly prohibits the TSPs and (M)NOs from realising statistical information on interception, or allows the authorities to prohibit it;[1753]

8. there is a trend towards countries conducting surveillance under semi-permanent states of quasi-emergency. In most of the surveyed countries the authorities are granted extremely wider-ranging powers at times of war and national emergencies 'threatening the life of the nation'. However, the study found that mass surveillance powers are granted in laws that are supposed to apply within the normal constitutional frameworks. Thus, laws that would not normally be deemed acceptable are becoming an integral part of the permanent legal fabric of the surveyed countries. They are creating a 'semi-permanent quasi-emergency' legal framework, not fully in accordance with the normal rules but also not formally seen as emergency law. For example, following the recent attacks in Paris the French president has declared the country to be 'at war' with the 'Islamic State' and is seeking to change the constitution to give the authorities wider, less judicially constrained powers. Such action, rather than relying on a temporary derogation for a defined war or emergency underlines the insidious effects of permanent 'special' anti-terrorist laws;[1754]
9. an alarming amount of mass surveillance happens illegally anyway. In most surveyed countries mass surveillance was conducted outside the official, known legal frameworks altogether (France, Germany, South Africa, Columbia, Egypt, Kenya and Pakistan). In others (Myanmar, Russia and Turkey), the law is so unclear as to make is impossible to distinguish between legal and extra-legal activities;[1755]
10. oversight systems are often non-existent or ineffective because they are not independent. In six of the countries studied (DR Congo, Egypt, Myanmar, Pakistan, Russia and Turkey) there is effectively no independent oversight over the use of the powers of mass surveillance. In other countries, the oversight systems are in place but they have proved to be ineffective (the US, the UK). In Germany large surveillance operations, including some carried out with or on behest of the US NSA were not known to the oversight body, the G10.[1756]

[1753] ibid, p. 10.
[1754] ibid.
[1755] ibid, p. 11.
[1756] ibid.

The *Boundaries of Law* concluded that 'the discrepancy between continuing government surveillance practices and the relevant international human rights and rule of law standards is breath-taking'.[1757] It warned that 'the resulting concentration of secret powers in the hands of intelligence agencies may prove deeply corrosive to democracy, commerce and the rule of law.'[1758] Clear global standards must therefore be put in place to call on states to establish appropriate checks and balances on their surveillance powers.

Recommendations for Future Research

State sponsored mass surveillance is but one manifestation of the profound changes that rapid technological progress of the 'Silicon Valley' has had and will continue to have not only on human rights, but across economies, societies and democracies.[1759] The involvement of the companies, such as Google, Microsoft, Facebook, Apple in the mass surveillance apparatus is beyond the scope of this study. There can be no doubt however, that future research into the activities of these 'technology giants' in relation to facilitating mass surveillance (inadvertently, or otherwise) will call for the stringent regulation by internationally binding standards, including the international human rights framework. At the moment, such a framework does not exist. However, the United Nations Human Rights Council "Guiding Principles on Business and Human Rights Implementing the UN 'Protect, Respect and Remedy Framework'"[1760] do apply. The Principles recognize the '[s]tates existing obligations to respect, protect and fulfil human rights and fundamental freedoms',[1761] together with the 'role of business enterprises as specialised organs of society performing specialised functions, [who are] required to comply with all applicable laws and to respect human rights.'[1762] The Principles relate to 'all [s]tates and all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure'.[1763] However, they do not create new international law obligations, but 'should be read [..] in terms of their objective of

[1757] ibid.
[1758] ibid.
[1759] *BBC*, 'Secretes of Silicon Valley', (2017) <http://www.bbc.co.uk/programmes/b0916ghq>.
[1760] UN HRC, "Guiding Principles on Business and Human Rights Implementing the UN 'Protect, Respect and Remedy Framework'" (2011) UN Doc A/HRC/17/31.
[1761] ibid.
[1762] ibid.
[1763] ibid.

enhancing standards and practices with regard to business and human rights so as to achieve tangible results for affected individuals and communities and thereby also contributing to a socially sustainable globalization.'[1764]

The next part of this chapter will demonstrate that such non-legally binding norms, as the 'Ruggie Principles' seem insufficient in the light to the ongoing technological developments. Indeed, the challenge for international law is to maintain relevance to a word-wide market dependency that is developed and controlled by an industry spending billions of dollars annually. The following considers likely areas of technological progress in the digital world that will have direct ramifications on cyber surveillance (by state and non-state actors). These include, but are not limited to: (a) quantum computers; (b) encryption and deciphering; (c) Big Data; (d) the Internet of Things (IoT); (e) Psychrographics and Psychometrics; (f) Artificial Intelligence (AI) and Machine Intelligence (MI).

(a) Quantum Computers

The largest computer in the world was announced in June 2016 at the International Super Computer Conference in Germany.[1765] It is the Chinese Sunway TaihuLight with a memory capacity of 20 petabytes (2×10^{16}), which can execute almost 10^{17} calculations per second.[1766] In the article titled 'Qudits: The Real Future of Quantum Computing'[1767] it is claimed that quantum computers will be at least one thousand times faster (10^{20}) than the Chinese Sunway TairhuLight machine, with backing storage capacity in the yottabytes range (10^{28}).[1768] Forecasts of their commercial availability range from ten to thirty years.[1769] Such machines will potentially have enormous impact, especially on governments' capacity for cyber surveillance and deciphering.

[1764] ibid.
[1765] Stephen J. Vaughan-Nicols, 'Linux and China Rule Supercomputing's Top 500 in 2016' (20 June 2016) < http://www.zdnet.com/article/linux-and-china-rule-supercomputing-in-2016/>.
[1766] ibid.
[1767] Charles Q. Choi, 'Qudits: The Real Future of Quantum Computers' (28 June 2017) <http://spectrum.ieee.org/tech-talk/computing/hardware/qudits-the-real-future-of-quantum-computing>.
[1768] ibid.
[1769] ibid.

(b) Encryption and Deciphering

The encryption and deciphering (the ability 'to scramble and unscramble' data-easy to do and difficult to undo) is vital in maintaining the confidentiality of information, whether that relating to business, commercial transactions, banking, personal medical records, or government secrets.[1770] Public key cryptography[1771] was invented at GCHQ in 1973 by Clifford Cox but only declassified in 1997.[1772] In 1978 Rivest, Shamir and Adleman published a similar system (the RSA cryptosystem).[1773] Their algorithm solved the practical difficulty of factoring large prime numbers.[1774] Today, as aptly summarised by one commentator

> [c]omputing power is used to both make and brake codes as the cost of computing plummets, cryptographic systems that once offered adequate protection for data become insecure. By the same token, however, cheaper computers also make it cost effective to encrypt data where once it would have been uneconomic. Paradoxically, then, plummeting computing costs have enabled the widespread use of encryption to defend information security and increase the ability of moderate to large organizations (in the private sector and governments) to afford the computing resources needed to successfully attack once-capable encryption systems. To balance these shifting forces the Unites States must grapple with multiple and often conflicting objectives.[1775]

[1770] Kenneth Flamm, 'Deciphering the Cryptography Debate' (21 July 1997) <https://www.brookings.edu/research/deciphering-the-cryptography-debate/>.
[1771] Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt. In *Global Sign*, 'What is Public Key Cryptography?' <https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/>.
[1772] Simon Singh, *The Code Book* (Doubleday 1999) pp. 279-292.
[1773] R.L. Riverst, A. Shamir and L. Adleman, 'A Method for Obtaining Digital Signature and Public Key Cryptosystem' (1978) < https://people.csail.mit.edu/rivest/Rsapaper.pdf>.
[1774] ibid.
[1775] supra note 29.

These tensions and the balancing of interest is of course not only confined to the US, but effect the larger international community.[1776] The *Apple Encryption Dispute*,[1777] discussed in Chapter 4 of this thesis clearly illustrates the need for a uniform policy to balance the operational objectives of the security and law enforcement on the one hand and the potentially catastrophic consequences of the private sector having to compromise encryption standards imposed on them through legislation. An example of such legislative measures is the US 'encryption draft bill', proposed by the US Senate Intelligence Committee and leaked to the public 2016.[1778] The draft bill would authorise US state and federal judges to order 'any person who provides a product or method to facilitate a communication or the processing or storage of data' to 'provide data in intelligible form or technical assistance in unlocking encrypted data' and that 'any such person who distributes software or devices must ensure they are capable of complying with such order'.[1779] Equally worrisome are calls from the UK Prime Minister Theresa May, who in the aftermath of the London terrorist attacks in June 2017 demanded internet regulation, placing particular emphasis on the private sector to effectively abolish encryption.[1780]

These governmental policy trends coupled with the projected operating speed of quantum computers (greater than 10^{20} operations per second), which will greatly enhance the intelligence and security services' ability to decipher encrypted signals, at the very least necessitates research and informed public debate on such issues as data security, privacy, the role of the private sector and the effectiveness of these proposed measures in fighting/preventing terrorism.

[1776] see for example UN HRC, 'Report of the Special Rapporteur on the right to privacy, Joseph Cannataci' (24 February 2017) UN Doc A/HRC/34/60.
[1777] *Apple v FBI* Concerning Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone, US District Court for the Central District of California, Nos. 16-cm-00010 and 15-mj-00451.
[1778] *Reuters*, 'Leak of Senate Encryption Bill Prompts Swift Backlash' (2016) <https://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0X52CG>.
[1779] The Senate of the United States, Draft Encryption Bill <https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf>.
[1780] *Forbes*, 'UK Prime Minister Demands Internet Regulation Following London Terror Attacks' (5 June 2017) < https://www.forbes.com/sites/emmawoollacott/2017/06/05/why-theresa-may-is-really-calling-for-a-ban-on-encryption/>.

(c) Big Data

Big Data concerns the use of very large amounts of data retained on computer storage devices that can then be analysed in a variety of ways to reveal patterns, trends, associations and much more especially related to human behaviour and interactions.[1781] The origin of the term is indeterminate.[1782] The analysis of interrelationships of names, addresses and frequency of correspondence by internet is referred to as metadata and used by the intelligence and security services to help identify the activity of terrorists groups in particular.[1783] The data collected today on each individual, by a myriad of players covers all aspects of human behaviour including, education attainment, grocery preferences, travel, entertainment, health, banking and financial services, leisure activities to www surfing and especially telecommunications.[1784] The sole purpose of predictive analysis is to simulate, or emulate accurately an individual's future behaviour.[1785] To supermarkets and the like this means the ability to predict an individual's, or community's current and future buying habits and manipulate these results for huge commercial and financial gain. For others, including the intelligence and security services it could mean something more insidious, such as the ability to monitor, predict and manipulate the behaviour of each individual, as described below in the section dealing with psychrographics/psychometrics. Edward Snowden disclosed in 2014 that the NSA captures and stores from the internet the equivalent of all the data in British Library every 8 minutes.[1786] Such volumes of stored and processed data are only possible because of current computer process speeds and storage capabilities. Quantum computing, it is predicted, will increase such ability by three orders of magnitude or more.[1787]

[1781] SAS, 'Big Data. What Is It and Why It Matters', <https://www.sas.com/en_gb/insights/big-data/what-is-big-data.html>.
[1782] ibid.
[1783] David Lyon, 'Surveillance, Snowden and Big Data: Capabilities, Consequences, Critique' (2014) Bid Data Society < http://journals.sagepub.com/doi/pdf/10.1177/2053951714541861>.
[1784] ibid.
[1785] ibid.
[1786] Paul Szoldra, 'This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks' (16 September 2016) <http://uk.businessinsider.com/snowden-leaks-timeline-2016-9 >.
[1787] *Kubric,* 'How Quantum Computing May Revolutionize Big Data' <http://kubrickgroup.com/2016/12/16/how-quantum-computing-may-revolutionize-big-data-rahul-patel/ >.

(d) The Internet of Things

The Internet of Things (IoT) is a term that 'encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other'.[1788] The IoT is made up of devices, from simple sensors to smartphones and wearables, connected together.[1789] It will be a major future source of information for Big Data.

In 1999, Kevin Ashton, in a presentation to *Proctor and Gamble* coined the phrase 'the Internet of Things', by which he meant interconnection 'in real time' via the internet of everyday objects having 'embedded sensors' that are programed to 'talk to each other'.[1790] This is ubiquitous connectivity, of which there is no limit to the range of such talking objects- everything from cars to refrigerators, kettles to TV sets, buttons on clothes to animal collars, central heating to tins of beans. Each of these items defining a specific feature/location/activity of the owner will transmit continuously over the internet and thereby contribute to the sum total of stored knowledge of that individual and item. Over time there will be nothing that is not known about each one of us.

Whilst many believe such 'convenience facilities' will make life simple and commerce hyper efficient, they are nothing more than 'listening devices' that will eventually entrap us all by surveillance. In February 2016 James Clapper, the former director of US national intelligence, speaking to the US Senate publically acknowledged for the first time that the intelligence agencies might take advantage of the new possibilities presented by having computers built in ever-more home appliances.[1791] In his words 'in the future intelligence services might use (the Internet of Things) for identification, monitoring location, tracking and targeting for recruitment, or to gain access to networks or use credentials.'[1792] In 2015 the Korean TV

[1788] *Wired*, 'What is the Internet of Things? *Wired* Explains' <http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot >.
[1789] ibid.
[1790] *Newsweek*, 'Meet Kevin Ashton, Father of the Internet of Things' (25 February 2015) <http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html>.
[1791] Rob Price, 'US Chief: We Might Hack Your Fridge to Spy on You' (10 February 2016) < http://uk.businessinsider.com/spy-chief-james-clapper-admits-spies-will-use-internet-of-things-devices-for-surveillance-2016-2>.
[1792] ibid.

manufacturer advised its customers to switch off their sets at the mains as the devices were able to transmit conversations in the home.[1793]

Communications related to IoT are a two-way process; that is the devices can be made to send and receive data/instructions. Thus, whilst convenient instructions can be traded between refrigerator and supermarket, such devices are also open to malicious instruction by government and hackers. Motor vehicles, central heating, hospital instruments, factory robots could all be open to 'Stuxnet' like attacks with catastrophic consequences. Furthermore, this 'meta intelligence' of connecting everything to everything else could easily lead to dehumanisation of homo sapiens. Initially Google was a search engine, now it searches us. Similarly, Facebook connected friends, now those friends are the content of Facebook. Gartner Inc., of Stamford, Connecticut (the world's leading information technology research and advisory company) forecast that within the US, China and Europe there will be 8.4 billion IoT connections in 2017, rising to 20bn by 2020 (being 67% of the total) and representing spending of $12 trillion.[1794] Edward Snowden warned that such enormous amounts of IoT data collected, stored and analysed by commercial enterprises and state security services could subvert the law.

(e) Psychrographics and Psychometrics

In 1928 Edward Barnays published his influential work, *Propaganda,* in which he argued that public relations is not a gimmick but a necessity, stating that '[c]onscious and intelligent manipulation of the organised habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government, which is the true ruling power of [the] country'.[1795]

Psychographics is the study and classification of people according to their attitudes, aspirations and other psychological criteria.[1796] Psychometrics is the process of measuring

[1793] *BBC News,* 'Not in Front of the the Telly: Warning over 'Listening' TV' (9 February 2015) < http://www.bbc.co.uk/news/technology-31296188 >.
[1794] Gartner, Press Release, 'Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, up 31 Percent from 2016' (7 February 2017) <http://www.gartner.com/newsroom/id/3598917>.
[1795] Edward J. Barnays, *Propaganda* (JG Publishing 2004).
[1796] Business Dictionary, 'What is Psychographics?' <http://www.businessdictionary.com/definition/psychographics.html >.

mental capacities and processes.[1797] Both of these are long established marketing tools that have possibly become insidious techniques in the hands of the 'Silicon Valley Data Barons', used *inter alia* to manipulate the outcome of general elections. For example, in 2012 Facebook published a paper in *Nature* reporting on their producing 340 000 extra voters in the 2010 US Congressional elections using a form of subliminal messaging.[1798] Subsequently, Jeff Hancock of Cornell University transmitted 'news feeds' having skewed positive and negative content for the purpose of manipulating the moods of 700,000 unwitting Facebook users.[1799] This 'mood manipulation experiment', using their own emotional language, showed that emotional contagion occurred among those Facebook users.[1800]

In 2014 Google beat Facebook in buying the British embryo psychographics modelling company, Deep Mind, for $500m.[1801] Deep Mind's technical objectives are 'making computers think like human beings'.[1802] Dr Michael Kosinski of Stanford School of Business is a psychologist and data scientist who co-ordinates the 'My Personality Project'.[1803] Part of the project, working on a data base of 6million Facebook volunteer records, entails the development of algorithms that are able to predict from 'digital footprints' a large number of the most precise personal characteristics and motivations of each individual.[1804] These can include education, religion, food, music, reading, TV programmes and holiday preferences etc. By these means Google and others are, in specialist operations such as Deep Mind, able to build 'virtual dopplegangers' of each individual with the ultimate intention of being able to predict the actual individual's needs before they realise it themselves.

Antonio Garcia Martinez, from 2011 to 2013 developed Facebook's means of making money by combining their experience of subliminal manipulation with their huge membership data

---

[1797] Psychometric Society, 'What is Psychometrics' <https://www.psychometricsociety.org/content/what-psychometrics>.
[1798] Zoe Corbyn, 'Facebook Experiment Boosts US Voters Turnout' (12 September 2012) <http://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401 >.
[1799] H. Rogers Segelken and Stacey Shackford, 'News Feeds: "Emotional Contagion" Sweeps Facebook' (10 June 2014) < http://news.cornell.edu/stories/2014/06/news-feed-emotional-contagion-sweeps-facebook>.
[1800] ibid.
[1801] Catherin Shu, 'Google Acquires Artificial Intelligence Start Up Deep Mind for More Than $500m' (26 June 2014) < https://techcrunch.com/2014/01/26/google-deepmind/ >.
[1802] ibid.
[1803] University of Cambridge, The Psychometrics Centre, 'Dr Michael Kosinski Computational Social Scientist' < https://www.psychometrics.cam.ac.uk/about-us/directory/michal-kosinski>.
[1804] ibid.

base and selling the facility to third parties. In May 2017 the *Guardian* published comments by Martinez where he warned that 'we are sleepwalking towards a technical apocalypse'.[1805] He disclosed that Facebook were able, by the use of complex computer algorithms, to apply psychographic-type targeting to a market population subset that were susceptible to a particular message. According to Martinez, online marketing was new, lightning fast and real time with success being monitored via a 'click through rate'.[1806] According to his account '[they] were able to manipulate their membership for their own ends and those of others who paid them'.[1807]

The true significance of the combination of psychographics, Big Data and computer processing capacity was demonstrated in Jamie Bartlett's *BBC 2* programme 'Secrets of Silicon Valley' broadcast on 13 August 2017.[1808] In the programme Bartlett uncovered a remarkable marketing strategy named 'Project Alamo', involving specialist technical skills from both sides of the Atlantic to promote presidential candidate Donald Trump during the 2016 US presidential elections.[1809] Theresa Hong, the director of Donald Trump's campaign stated in that programme that 'without Facebook, Trump couldn't have won'.[1810] To aid the campaign, Cambridge Analytica (a London psychometrics/psychographics operation) were hired just five months before polling day. According to the 'Secrets of Silicon Valley', Donald Trump's election programme had two thrusts, one- to boost him and the other- to denigrate Hillary Clinton in the eyes of her followers.[1811] Using a 'legacy data base' of three years information from Senator Cruz's failed presidential campaign and Facebook's membership, Cambridge Analytica bombarded them with up to 100 different adverts per day, each tailored to maximise on identified motivations.[1812] It is claimed that more than 200 million voters were contacted by Project Alamo. Donald Trump won the election, having spent $85m with Facebook, compared with Hilary Clinton's $1.2bn. total spend.[1813]

Currently there are seem to be no national, or international legal constraint to the use of psychometrics/psychographics for whatever purpose. It seems that these methods could be used

---

[1805] *The Guardian*, 'I'm and Ex-Facebook Exec: Don't Believe What They Tell You About Adds' (2 May 2017) <https://www.theguardian.com/technology/2017/may/02/facebook-executive-advertising-data-comment.
[1806] ibid.
[1807] ibid.
[1808] supra note 18.
[1809] ibid.
[1810] ibid.
[1811] ibid.
[1812] ibid.
[1813] ibid.

without constraint to influence/skew democratic processes in any country in the world, depending on the financial clout of an individual(s) wishing to hire such services. In the President Trump's example, clearly the outcome of the democratic process was influenced by dubious information and means, over which there was no moral, nor legal filter. This largely has been made possible through the operation of the US 1996 Communications Decency Act (CDA), section 230. This is a landmark internet legislation that provides immunity from liability for provides and user of the 'interactive computer service', who publish information provided by others.[1814] Without section 230 CDA 1996 it is probable that the large internet companies, such as Facebook would not exist at all, or would be a shadow of their current form in terms of wealth and power. It also illustrates that one country's legislation can and does have a profound social and political effect world-wide. If section 230 of the CDA 1996 were to be amended or repealed to make Facebook legally responsible for the online content, that and other similar companies would be forced to censor material of a sensitive, libellous and/or untruthful nature. Such a change in the law would also reduce the financial muscle of Facebook and thereby their political power.

(f) Artificial Intelligence (AI) and Machine Intelligence (MI)

Artificial Intelligence (IA) and Machine Intelligence (MI) is a combination of computing capacity and complex algorithms, such as the Deep Mind, described above.

On the 27 October 1949 a large interdisciplinary meeting was held in Manchester University, the work place of Alan Turing, to consider 'Discussion on the Mind and the Computing Machine'.[1815] The following year Alan Turing published a paper titled 'Computing Machinery and Intelligence', in which he introduced the term 'imitation game'.[1816] He speculated that '[i]f an interrogator could not distinguish between a human being and a computer by questioning then it would be unreasonable not to call the computer intelligent'.[1817] In other words, AI is

[1814] Codified as 47 U.S.C.§230, the section states that '[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.

[1815] Turing Sources, 'Discussion on the Mind and the Computing Machine, 27 October 1949' <http://www.turing.org.uk/sources/wmays1.html >.

[1816] Alan Turing, 'Computing Machinery and Intelligence' (1950) *Mind* <https://www.csee.umbc.edu/courses/471/papers/turing.pdf >.

[1817] ibid.

applied when a machine mimics 'cognitive' functions that we associate with other human beings such as learning and solving problems.[1818]

Nowadays capabilities generally classified as AI and MI include the understanding of human speech, high level strategy games such as chess and Go, reasoning, perception and military simulations. [1819] The specialist skills involved in developing these technologies include computing, maths, psychology, linguistics, psychology, neuroscience and many others.

Whilst there are many potential benefits of AI,[1820] there are serious potential dangers and undesirable risks in these technologies, probably with unintended consequences. Martin Ford, in his book *The Rise of the Robots: Technology and the Threat of Mass Unemployment*, warns of 30% unemployment within ten years caused by the replacement of humans by machines.[1821] Such jobs cover the whole spectrum from lawyers, through clerks to delivery drivers, much of medical diagnosis and prescribed treatments.[1822] Only dentists seem to be indispensable. Interviewed for *BBC News* in October 2015 Professor Stephen Hawking raised the danger stakes warning that:

> [t]he development of full artificial intelligence could speed the end of the human race. Once humans develop artificial intelligence it will take off on its own and redesign itself at an ever increasing rate. Humans, who are limited by slow biological evolution couldn't compete and would be superseded.[1823]

This 'Doomsday' vision was echoed in Nick Bostrom's book *Superintelligence: Paths, Dangers, Strategies,* where he noted that AI would be 'the last invention humans would need to make'.[1824] He forecast that the chance of Human Level Machine Intelligence (HLMI) being

---

[1818] ibid.

[1819] Jerry Kaplan, *Humans Need Not Apply: A Guide to Wealth and Work in the Age of Artificial Intelligence* (Yale University Press 2015).

[1820] see for exampled *Nuance,* 'It's Time to Take Off Your Tinfoil Hats: AI is Safe for Human Consumption' (15 January 2015) < http://whatsnext.nuance.com/in-the-labs/effects-of-artificial-intelligence-on-humanity/>. These include areas such as healthcare, education and economy.

[1821] Martin Ford, *The Rise of the Robots: Technology and the Threat of Mass Unemployment* (Oneworld Publications 2016).

[1822] ibid.

[1823] *BBC News*, 'Stephen Hawking-Will AI Kill or Save Humanity' (26 October 2016) <http://www.bbc.co.uk/news/technology-37713629 >.

[1824] Nick Bostrom, *Superintellignece: Paths, Dangers, Strategies* (Oxford University Press 2014).

reached by 2030 would be 10%, 50% by 2050 and 90% by 2090.[1825] The recent success of a program developed by Google, the Deep Mind, in defeating the world champion at the ancient game of GO shows that AI is developing faster than thought possible.

The above summary distils to the core developments of computing and its subsequent applications, largely for profit in the recent years. The emotive vocabulary in common use by the 'digital commercial community' exploiting the technology includes 'connectivity, hyper-efficiency, real-time and so on'. The words 'security, privacy, confidentiality, honourable, fair, good, freedom' are largely absent. These feature in the vocabulary of human rights activists and organizations. Cupidity is usually the main corporate and individual objective. There is a myriad of questions demanding answers, especially dealing with moral and legal issues. Of particular interest are:

- where is the (international) law in all of this?
- when will it catch up with these technological developments?
- what will the process be?
- how will it ensure that it envelopes the 'Silicon Valley Technology Barons"?
- could section 230 of the US Communications Decency Act 1996 be changed?

These and other questions are a fertile ground for further research.

CONCLUSION

This research has a narrow focus, in that it considers the privacy violations of a handful of technologically advanced states. The prism through which the study has been conducted has highlighted a range of aspects within the 'digital world' that are of concern not only to human rights organizations but also society at large.

The overview included in the section laying out some of the areas of future research has opened up a Pandora's box, contents of which will demand continued close scrutiny. Circumspection is needed when viewing these technical and application developments in the framework of human rights law. The rate, at which technical developments are taking place and their potential harmful consequences are of concern to many working within that environment. Equally, the

[1825] ibid.

intelligence and security services are looking to protect the state and its citizens against internal and external antagonistic forces. Part of their task is to keep watch on developments within the digital domain, some of which they use in their own duties. Axiomatically, those within the digital sphere driven by cupidity and/or intellectual challenge will identify opportunities suiting their motivations well ahead of most of us. In doing so, they are more likely to see blurred legal boundaries and justify their objectives with a skewed logic.

There is a need for a set of sound social principles for both those 'developing' the digital world and for states, as principal international law makers, that would define their activities as being for the general good and operating within the rule of law. There is a lot of merit in not leaving these practices to a system of self-regulation, but imposing legal parameters. Even so, for the law to be effective, it needs to be supported within the range of relevant principles and practical means of enforcement and oversight. With respect to the security/law enforcement services, the operative objectives and modus operandi must be lawful, necessary and proportionate to the task.[1826] Published definitions of these objectives, together with stated public oversight and meaningful reporting, whilst protecting national and international interests are essential. Accountability to the democratic, elected body on operational violations must be clearly reported and dealt with through the processes of the law. Domestic legislation authorising mass surveillance must continue to be challenged in the courts.[1827]

[1826] see for example the Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance (10 July 2013), which set out set of 10 principles with a singular goal of ensuring that laws, policies and practices relating to communications surveillance adhere to international human rights laws and standards. <https://necessaryandproportionate.org/principles >.

[1827] see successful challenge by Tom Watson MP to the UK Data Retention and Investigatory Powers Act 2014, *The Guardian,* 'High Court Rules Data Retention and Surveillance Legislation Unlawful' (17 July 2015) <https://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful >; also the legal challenge by Liberty to the Investigatory Powers Act 2016 launched in January 2017, *the Guardian,* 'Liberty Launces Legal Challenge to 'State Spying' in the Snooper's Charter' (10 January 2017) < https://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful >.

A whole host of legal challenges lie ahead in terms of how exactly is online privacy to be protected and how is is it to fit within the broader cyber security and internet governance agendas. A rhetorical question that this thesis end with is how realistic is it that a critical mass of states would agree to impose any legal constraints on themselves and the 'technology giants' since states have and continue to violate their human rights obligations?

SELECTED BIBLIOGRAPHY

Legislation

Treaties

International

-The Antarctic Treaty 1951;
-Charter of the United Nations 1945;
-Constitution and Convention of the International Telecommunications Union 1992;
-UN Convention on the Law of the Sea 1982;
-Convention on Rights and Duties of States (Montevideo Convention) 1933;
-Convention on International Civil Aviation (Chicago) 1944;
-Geneva Conventions Additional Protocol relating to the Protection of Victims of International Armed Conflicts 1977 (AP I);
-Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land 1907;
-International Covenant on Civil and Political Rights 1966;
-Optional Protocol to the International Covenant of Civil and Political Rights (UN GA 2200A (XXI) 1976;
-International Covenant on Economic, Social and Cultural Rights 1976;
-UN Statutes of the International Court of Justice 1946;
-Vienna Convention on the Law of the Treaties 1969;
-The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the Outer Space Treaty) 1967;
-The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the Moon Treaty) 1979;
-Vienna Convention on the Law of the Treaties 1969;

Regional

-Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security 2009;
-African Union, African Charter on Human Rights and People's Rights 1981;
-African Union, African Union Convention on Cyber Security and Personal Data 2014;
-Organization of American States, American Convention on Human Rights (Pact of San Jose) 1969;
-Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Individual Data 1981;
-Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001;
-Council of Europe, Convention on Cybercrime 2001;
-Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms 1950;

-Council of Europe, Draft Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Modernized Convention) 2016

European Union

-The Treaty on the Functioning of the European Union, 2007;
-Charter of Fundamental Rights of the European Union, 2012
-Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 OJ L 281/31/;
-Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 OJ L 119/1 in force on 25 May 2018;

Domestic Legislation

The United Kingdom

-Investigatory Powers Act 2016;
-Regulation of Investigatory Powers Act 2000;
-Telecommunications Act 1984;

The United States

-Foreign Surveillance Intelligence Act 1978 amended by the 2008 Amendment Act;
-Stored Communications Act 1989;
-Communications Decency Act 1996;

South Africa

-Regulation of Interception of Communications and Provision of Communications- Related Information Act 2002;

Australia

-Telecommunications (Interception and Access) Act 1979;

Canada

-Criminal Code of Canada (Invasion of Privacy) 1985;

New Zealand

-Government Communication Security Bureau Act 2003;

Table of Cases

International Court of Justice

-Accordance with International Law of the Universal Declaration of Independence in Respect of Kosovo, Advisory Opinion 22 July 2010;
-Asylum Case (Columbia v Peru) Judgement 20 November 1950;
-Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Bosnian Genocide Case) Judgement (Merits) 26 February 2007;
-Eritrea/Yemen Arbitration (Phase One: Territorial Sovereignty and Scope of Dispute) 9 October 1999;
-Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) 1 July 2000;
-Case Concerning Delimitation of the Maritime Boundary on the Gulf of Maine Area Judgement 12 October 1984;
-Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v Nigeria) Judgement (Merits) 10 October 2002;
-Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) 27 June 1986;
-Case Concerning United States Diplomatic and Consular Staff in Teheran (United States of America v Iran) Judgement 24 May 1980;
-The Case of the SS 'Lotus' (France v Turkey) 1927;
-Corfu Channel Case (United Kingdom v Albania) Judgment (Merits) 9 April 1945;
-Fisheries Case (United Kingdom v Norway) Judgement 18 December 1951;
-The Factory at Chorzów (Claim for Indemnity) (Germany v Poland) Judgment 1928;
- Gabčíkovo–Nagymaros Project (Hungary/Slovakia) Judgment 1997;
-Isle of Palmas Arbitration (the Netherlands v the United States) 1928;
-Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion 8 July 1996;
-Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories, Advisory Opinion 9 July 2004;
-Legal Status of Eastern Greenland (Denmark v Norway) Judgment 5 September 1933;
-Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion 8 July 1996;
-North Sea Continental Shelf Cases (Federal Republic of Germany v Denmark; Federal Republic of Germany v the Netherlands) Judgment 20 February 1969;

International Criminal Tribunal for the Former Yugoslavia

-Prosecutor v Duško Tadić, Case No IT-94-1 Appeals Chamber Judgment 1999;

Human Rights Committee

-Lopez Burgos v Uruguay (52/1979);
-Giouse Canepa v Canada (558/1993);
-Cornelis van Hulst v the Netherlands (903/00);
-Angel Estrella v Uruguay (74/89);

-Pinkney v Canada (27/78);
-Tooten v Australia (488/1992);

European Court of Human Rights

-Al-Skeini and Others v United Kingdom (2011) ECHR;
-Amann v Switzerland (2000) 30 EHRR 843;
-Association of European Integration and Human Rights and Ekmdzhiev v Bulgaria (2007) ECtHR 62540/00;
-Bankovic and Others v Belgium (2007) 57 EHRR;
-Benedict v Slovenia (Application No. 62357/14);
-Big Brother Watch and Others v United Kingdom (Application No. 58170/13);
-Brunet v France (2014) ECtHR 21010/09;
-Bureau of Investigative Journalism and Alice Ross v United Kingdom (Application No. 623322/14);
-Copland v United Kingdom (2007) 45 EHRR 858;
-Doerga v the Netherlands (2004) (Application No. 50210/99);
-Halford v United Kingdom (1997) 24 EHRR 523;
-Haralambie v Romania (2009) (Application No. 21737/03);
-Huvig v France (1990) (Application No. 11105/87);
-Jaloud v the Netherlands (2014) (Application No 47708/08)
-Kennedy v United Kingdom (2010) ECtHR 26839/05;
-Khan v United Kingdom (2000) (Application No. 35394/97);
-Klass and Others v Federal Republic of Germany (1978) 2 EHRR 214;
-Kruslin v France (1999) (Application No. 11801/85);
-Kopp v Switzerland (1999) (Application No. 23224/94);
-Leander v Sweden (1987) 9 EHRR 433;
-Liberty and Others v United Kingdom (2009) 48 EHRR 1;
-Loixidou v Turkey (1995) 20 EHRR;
-Malone v United Kingdom (1985) 7 EHRR 14;
-M.K. v France (2013) ECtHR 19522/09;
-MM v United Kingdom (2012) (Application No. 24029/07);
-Öcalan v Turkey (2003) 41 EHRR;
-Peck v United Kingdom (2003) (Application No. 4467/98);
-S and Marper v United Kingdom (2009) 48 EHRR 1169;
-Robathin v Austria (2012) ECtHR 30457/06;
-Rotaru v Romania (2000) (Application No. 28341/95);
-Shimovolos v Russia (2011) ECtHR 30194/09;
-Silver and Others v United Kingdom (1983) (Application No. 5947/72
-Sunday Times v United Kingdom (1979) (Application No. 6538/74);
-Szabo and Vissy v Hungary (2016) ECtHR 37138;
-Telegraph Media Nederland Landelijde Media BV v the Netherlands (2012) (Application No. 39315/06);
-10 Human Rights Organizations v United Kingdom (Index No. 60/1415/2015);
-Uzun v the Federal Republic of Germany (2010) (Application No. 36623/05);
-Weber and Saravia v Federal Republic of Germany (2006) (Application No. 54934/00);
-Wieser v Autria (2008) 46 EHRR;
-Vogt v Federal Republic of Germany (1996) (Application No. 17851/91);
-Zakharov v Russia (2015) ECtHR 47143/06;

The Court of Justice of the European Union

-Case C-362/14 Maximilian Schrems v Data Protection Commissioner (2015) ECJ;
-Joind Cases C-293/12 and 594/12 Digital Rights Ireland Ltd. And Seitilinger and Others (2014) ECJ;

Inter –American Commission on Human Rights

-Roach and Pinkerton v United States Case 9. 647;

Inter-American Court of Human Rights

-Alexandre v Cuba (1999) Case No. 11.589;
-Steve Clark v Granada (1996) Case No. 10.325;
-Escher v Columbia IACHR Series C No. 200;
-Tristan Donoso v Panama (2009) IACHR Series C No. 193;

National Courts

France

-UEJF et LICRA v Yahoo! Inc. et Yahoo France, Tribunal de Grande de Paris, No RG:00/05308;

The United Kingdom

-R v Perrin [2002] EWCA Crim. 747;
-Harrods Ltd. v Dow Jones Co. Inc. [2003] EWHR 1162 (QB);
-Liberty and Others v the Security Services, SIS, GCHQ (2015) IPT/13/77/H;
-Human Rights Watch Inc. and Others v the Secretary of State for Foreign and Commonwealth Office and Others (2016) ALL ER (D) 105;

The United States

- Apple v FBI Concerning Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone, US District Court for the Central District of California, Nos. 16-cm-00010 and 15-mj-00451
-Klayman v Obama No. 14-5004 (DC Cir. 2015)
-In the Matter of a Warrant to Search a Certain E-Mail Account: Controlled and Maintained by Microsoft Corporation, 15 F. Supp. 3d 466 (SDNY 2014);
-In the Matter of a Warrant to Search a Certain E-Mail Account: Controlled and Maintained by Microsoft Corporation, the US Court of Appeals for the Second Circuit (2016) Docket no. 14-2985;
-United States v Verdugo-Urquidez (1999) 494 US 259;

Reports and Other Non-Binding Instruments

United Nations

-Universal Declaration of Human Rights, adopted 10 December 1948, UN General Assembly Resolution 217 A(III);
-Declaration of the Rights of Indigenous Peoples 2007;
-Rio Declaration on Environment and Development 1992;

-UN General Assembly Resolution 1472 (XIV) UN Doc A/43/51 (1959);
-UN General Assembly Resolution 1721 (XVI) UN Doc A/5026 (1961);
-UN General Assembly Resolution 2450 (19 December 1969 UN Doc E/CN.4/1025;
-UN General Assembly Resolution 2574 UN Doc A/RES/2574 (1970);
-UN General Assembly, 'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations' Adopted by General Assembly Resolution 2625 (XXV) (24 October 1970);
-UN General Assembly Resolution 45/91 Guidelines Concerning Computarized Data Files (14 December 1990) UN Doc E/CN.4/1990/72;
-UN General Assembly, 'Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms' Adopted by General Assembly Resolution 53/144 (9 December 1998);
-UN General Assembly, Resolution 60/251 (2006) UN Doc A/Res/251;
-UN General Assembly, 'Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament' (28 May 2006) UN Doc A/S-15/3;
-UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc 68/167 (14 December 2013);
-UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc 66/169 (14 December 2014);
-UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc A.3/71/L.39/Rev.1 (16 November 2016);
-UN General Assembly, 'Report of Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/68/98 (24 June 2013);
- UN General Assembly, 'Report of Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015);

-Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, UN Doc A/66/358 (14 September 2011);
- Letter dated 9 January 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, UN Doc 69/723 (13 January 2015);

-UN Secretary General, Report of the Working Group on Internet Governance (2005);

-International Telecommunications Union, World Summit on the Information Society Geneva 2003-Tunis 2005. Declaration of Principles (2005) Doc WSIS-03/Geneva/Doc/4-3;
-International Telecommunications Union, Tunis Agenda for Information Society (2005) WSIS-05/TUNIS/DOC/6(Rev 1.)-E;
-Declaration of Principles of the World Summit on the International Society, 'Building the Information Society: A Global Challenge in the New Millennium' (2003) WSIS-03/Geneva/Doc/4-E

-International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (2001);
-UN General Assembly International Law Commission, 'Second Report on the Identification of Customary International Law' (20 November 2014) UN Doc A/CN/4/672;
- UN General Assembly, International Law Commission, 'Identification of Customary International Law. Text of the Draft Conclusions Provisionally Adopted by the Drafting Committee' UN Doc A/CN/.4/L.872 (30 May 2016);

-Declaration of the United Nations Conference on the Human Environment (Stockholm Declaration) (1972)
-Declaration of Principles Governing the Sea-Bed and the Ocean Floor and the Subsoil Thereof, Beyond the Limits of National Jurisdiction, UN Doc A/RES/2749 (XXV) (1970);

-United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (2013);
-UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to the Freedom of Opinion and Expression, Frank La Rue' UN Doc A/HRC/23/40 (17 April 2013);
-UN Human Rights Council, 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie' (21 March 2011) UN Doc A/HRC/17/31;
-UN General Assembly, 'The Right to Privacy in the Digital Age. Report of the Office of the High Commissioner for Human Rights' UN Doc A/HRC/27/37 (30 June 2014);
-UN Human Rights Council, Fifty-Third Session, Summary Record of the 1405th Meeting (1995) UN Doc CCPR/C/SR.1405;
-United Nations Office of the High Commissioner for Human Rights, 'Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid' (2016);
-UN Commission on Human Rights, 'Report by Special Rapporteur David Weissbrodt' (2003) UN Doc E/CN.4/Sub.2/2003/23;
-UN Human Rights Council, Joint Statement on Right to Privacy, 24th Regular Session (2013);
-UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rigths on the Internet' (2012) UN Doc A/HRC/20/8;
-UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' UN Doc A/HRC/32/L.20 (27 June 2016);

-UN Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC' (2014) UN Doc A/69/397;
-UN Human Rights Council, 'Human Rights and Arbitrary Deprivation of Nationality. Report of the Secretary General' (2013) UN Doc A/HRC/25/28;

-UN Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40;
-UN Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism, Martin Scheinin' (2009) UN Doc A/HRC/13/137;
-UN Human Rights Council, Office of the High Commissioner, 'The United Kingdom's Human Rights Record to be Reviewed by the Universal Periodic Review' (1 May 2017);
-UN Human Rights Council, 'Draft Report of the Working Group on the Universal Periodic Review. United States of America' (2011) UN Doc A/HRC/16/11;
-UN Human Rights Council, 'Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci' (8 March 2016) UN Doc A/HRC/31/64;

-UN Human Rights Council, 'General Comment No. 15. The Position of Aliens under the Covenant' (1986) UN Doc HRI/Gen/Rev.9/(Vol.1);
-UN Human Rights Council, 'CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence and the Protection of Honour and Reputation' (1988) UN Doc HRI/GEN/1/Rev.1;
-UN Human Rights Council, 'General Comment No. 18: Non-Discrimination' (1989) UN Doc HRI/GEN/1/Rev. 1;
-UN Human Rights Council, 'General Comment No. 27. Freedom of Movement (Art 12)' (1999) UN Doc CCPR/C/21/Rev.1/Add.9;
-UN Human Rights Council, 'General Comment No. 31. Nature of the General Legal Obligations Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13;
-UN Human Rights Council 'General Comment No. 34 on Freedom of Opinion and Expression (Article 19 ICCPR)' (2011);

-UN Human Rights Committee, 'Report of the UN Human Rights Committee' (1994) UN Doc 5/50/40;
- UN Human Rights Committee, Consolidation of Reports Submitted by States Parties under Article 40 of the Covenant (2005) UN Doc CCPR/C/USA/3;
-UN Human Rights Committee, Concluding Observations of the UN Human Rights Committee on the US Report under the ICCPR' (2006) UN Doc CCPR/C/USA/CO/3;
-UN Human Rights Committee, Concluding Observations of the UN Human Rights Committee on the US Report Under the ICCPR (2014) UN Doc CCPR/C/USA/4;

Regional

The Council of Europe

-Council of Europe Parliamentary Assembly, 'Mass Surveillance' (18 March 2015) Doc 13737;
-Council of Europe Article 29 Working Party, 'Article 29 Working Party's Comments on the Issue of Direct Assess by Third Countries' Law Enforcement Authorities to Data Stored in Other Jurisdictions as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime' (5 December 2013) (Ares.2013) 3645289-05/12/2013;

-Council of Europe Commissioner for Human Rights Nils Muižnieks, 'The Rule of Law on the Internet and in the Wider World' (2014);
-Council of Europe Cybercrime Convention Committee (T-CY), 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY'. Report Prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction Adopted by the 12th Plenary of the T-CY (2-3 December 2014);
-Council of Europe Explanatory Report to the Convention on Cybercrime, ETS 185 (2001);
-European Court of Human Rights, 'National Security and European Case-Law. Report of the Council of Europe Research Division' (2013);
-Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, Resolution 2045 (2015);
-Council of Europe, Draft Explanatory Report to Draft Modernized Convention 108 (2016);
-Council of Europe, Recommendation No. R(87)15;
-Council of Europe Report, 'Recommendation R(87)15-Twenty Five Years Down the Line' (23 September 2013);

The European Union

-Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000) OJ L 215/7;
-European Union Council Framework Decision 2008/977/JHA (2008);
-Court of Justice of the European Union, Press Release, 'The Court of Justice Declares the Data Retention Directive to Be Invalid' (2014);
-Court of Justice of the European Union, Press Release No. 117/15 (2015);
-European Commission Press Release, 'European Commission Launches EU-US Privacy Shield: Stronger Protection for Transatlantic Data Flows' (12 July 2016);

Inter-American Commission on Human Rights

-Inter-American Commission on Human Rights, Office of the Special Rapporteur for the Freedom of Expression, 'Report of the Special Rapporteur-Freedom of Expression and the Internet' (2013) OEA/Ser.L/V/II;

Other Documents Including Military Manuals, Official Government Statements, Operational Handbooks, National Security Strategies and Doctrines

The North Atlantic Treaty Organization

-NATO, 'Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization' adopted by the Heads of State and Government at the NATO Summit in Lisbon (19-20 November 2010);
-Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (2013);
-Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (2017);

Europe

-Organization for Security and Co-Operation in Europe, 'Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe' (18 September 1986);
-Organization for Security and Co-operation in Europe, 'Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Cooperation in Europe' (17 November 1990);

Domestic

The United States of America

-The US National Security Agency, 'Mission and Strategy' (3 May 2016);
-US Department of Homeland Security and Federal Bureau of Investigation, 'GRIZZLY STEPEE-Russian Malicious Cyber Activity. Joint Analysis Report' (29 December 2016);
-US Department of Defence Dictionary of Military and Associated Terms. Joint Publications (8 November 2010 as amended to 2016);
-US Department of Defence, Office of the General Counsel, 'Law of War Manual' (2016);

-The White House, Office of the Press Secretary, 'Remarks by the President on Review of Signals Intelligence' (17 January 2017);
-Office of the Director of National Intelligence, 'Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans and Why Disclosures Aids Our Adversaries' (18 June 2013);
-The US Department of Justice, Office of Public Affairs, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labour Organization for Commercial Advantages' (19 May 2014);
-The White House Office of the Press Secretary, 'Presidential Policy Directive-Signals Intelligence Activities. Policy Directive/PPD-28' (17 January 2014);
-Transcript of President Obama's January 17 Speech on NSA Reform (17 January 2014);
-Richard A. Clarke et al., *The NSA Report. Liberty and Security in a Changing World. The President's Review Group on Intelligence and Communication Technologies* (Princeton University Press 2014);

-Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies (December 2013);
-US Senator for California, Diane Feinstein, 'Feinstein on NSA Compliance' (2013);
-The White House, 'Information Operations, Joint Publications 3-13' (27 November 2012);
-Terry Kramer, US Ambassador and Head of Delegation, Wold Conference on International Telecommunications Union, 'Remarks' (13 December 2012);

-US Department of Commerce Fact Sheet, 'Overview of the EU-US Privacy Shield Framework for Interested Participants' (12 July 2012);
-Statement by Delegation of the United States of America, 'Other Disarmament Issues and International Security Segment of Thematic Debate on the First Committee of the Sixty-seventh Session of the United Nations' (2 November 2012);
-US Department of Defence, 'Strategy for Operating in Cyberspace' (July 2011);
-The White House, 'International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World' (May 2011);
-US Department of Defence, 'Department of Defence Cyberspace Policy Report: A Report to Congress Pursuant to the National Defence Authorisation Act for the Fiscal Year 2011' (November 2011);
-US Department of State, Hilary Rodham Clinton, 'Remarks on Internet Freedom' (2010);
-Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers (2009);
-US Department of Defence, 'National Defence Strategy' (2008);
-Chairman of the Joint Chiefs of Staff, 'The National Military Strategy for Cyberspace Operations' (December 2006);
-US Department of Defence, 'Strategy for Homeland Defence and Civil Support' (2005);
-Bylaws for Internet Corporation for Assigned Names and Numbers;
-US Department of Defence, 'An Assessment of International Legal Issues in Information Operations' (May 1999);
-Memorandum of Understanding Between the US Department of Commerce and Internet Corporation for Assigned Names and Numbers (25 November 1998);
-US Department of the Air Force, 'Cornerstones of Information Warfare' (1997);
-United States Presidential Proclamation No. 2667: Policy of the United States with Respect to the Natural Resources of the Subsoil and Sea Bed and the Continental Shelf (1945);

The United Kingdom

-The National Archives, 'Newly Released GCHQ Files: UKUSA Agreement' (June 2012);
-UK HMG, 'GCHQ Oversight' (17 April 2016);
-UK HMG Government, 'UK Cyber Security Strategy, Protecting and Promoting the UK in the Digital World' (November 2011);
-UK HMG Government, 'National Cyber Security Strategy 2016-2021' (2016);
-William Hague, 'Chair Statement' (2 November 2011);
-British Prime Minister's Office, 'PM Statement on Disorder in England 11 August 2011';

Canada

-Canada's Cyber Security Strategy (2011)

The Russian Federation

-The Government of the Russian Federation, 'Basic Principles for State Policy for the Russian Federation in the Field of International Information Security to 2020';
-The Government of the Russian Federation, *Draft Convention on International Information Security* (28 October 2011);
-Ministry of the Foreign Affairs of the Russian Federation, 'National Security Concept of the Russian Federation' (2000);

-Boris Vasiliev, Office of the Special Coordinator of the Ministry of Foreign Affairs, 'Sovereignty, International Cooperation and Cyber Security' (2013);

The Federative Republic of Brazil

-Address by Her Excellency Dilma Rousseff of the Federative Republic of Brazil and the General Assembly of the United Nations (New York 24 Semtember-1 October 2013);

The Republic of Malta

-Statement by Dr Alex Sceberras Trigona, Special Envoy to the Prime Minister of the Republic of Malta Permanent Mission of the Republic of Malta to the United Nations, World Summit on International Society Review Process, New York (15 December 2015);

Books

-Ian Brownlie, *Principles of Public International Law* (Oxford University Press 2012);
-Simon Davis, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (Pan Books 1997);
-Lee A. Bygrave, *Data Privacy. An International Perspective* (Oxford University Press 2014);
-Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press 2004);
-Allen Dulles, *The Craft of Espionage* (New York, David West Group Co. 1963);
William Gibson, *Neuromarcer* (New York: Ace Books 1984);
-Malcolm Evans, *International Law* (Oxford University Press 2010);
-Sara Joseph and Mellissa Castan, *The International Covenant on Civil and Political Rights. Cases, Materials and Commentary* (Oxford University Press 2014);
-David Harris et al., *Law of the European Convention on Human Rights* (Oxford University Press 2009);
-Christopher Joyner, *Governing the Frozen Commons: The Antarctic Regime and Environmental Protection* (University of South Carolina Press 1998);
-Vaughan Lowe, *International Law* (Oxford University Press 2011);
-Stephen Krasner, *Sovereignty: Organized Hypocrisy* (Princeton University Press 1999);
-Lawrence Lessing, *Code and Other Laws of Cyberspace* (Basic Books 2006);
-Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of the Borderless World* (Oxford University Press 2006);
-Peter Malanczuk, *Akehurst's Modern International Law* (Routledge 2002);
-Mike McConville and Wing Hong Chui (eds.), *Research Methods for Law* (Edinburg University Press 2007);
-Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (The MIT Press 2010);
-Gbenga Oduntan, *Sovereignty and Jurisdiction in the Airspace and Outer Space* (Routledge 2012);
-Chris Reed, *Internet Law: Text and Materials* (Cambridge University Press 2004);
-Thomas Rid, *Cyber War Will Not Take Place* (C. Hurt and Co. Publishers 2013);
-Javaid Rehman, *International Human Rights Law* (Persons Education Limited 2010);

-Donald Rothwell and Tim Stephens, *The International Law of the Sea* (Hart Publishing 2014);
-Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014);
-Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations* (Cambridge University Press 2014);
-Malcolm Show, *International Law* (Cambridge University Press 2008);

Chapters in Books, NATO Publications and Conference Proceedings

-Constantine Antonopoulos, 'State Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace* (Edgar Elgar Publishing 2015);
-Kamal Baslar, 'The Concept of Common Heritage of Mankind in International Law' in Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations* (Cambridge University Press 2014);
-Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' in Anna Maria Osula and Henry Roigas (eds.) *International Cyber Norms: Legal, Policy and Industry Perspective* (NATO CCD COE Publications 2016);
-Russell Buchan, 'Cyber Espionage in International Law' in Nicholas Tsagourias and Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015);
-Kenneth Geers, 'Pandemonium: Nation States, National Security and the Internet. The Tallinn Papers' (2014) (NATO CCD COE Publications on Strategic Cyber Security);
-Keir Giles, 'Russia's Public Stance on Cyberspace Issues' (2012) NATO CCD COE;
-Keir Giles and William Hagestad II, 'Divided by Common Language: Cyber Definitions in Chinese, Russian and English' (2013) 5th International Conference on Cyber Conflict 2013;
-Stephen Hall, 'Researching International Law' in Mike McConville and Wing Hong Chui *Research Methods for Law* (Edinburgh University Press 2007);
-Wolfgang Kleinwacher, 'The History of Internet Governance' in C. Moller and A. Amouroux (eds.,) *Governing the Internet: Freedom and Regulation in the OSCE Region* (Vienna: Organization for Security and Cooperation in Europe 2009);
-Uta Kohl, 'Jurisdiction in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015);
-Martin Libicki, 'The Coming of Cyber Espionage Norms' in H. Roigas et al. (eds.) *9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE Publications 2017);
-Patryk Pawlak, 'Confidence Building Measures in Cyberspace: Current Debates and Trends' in Anna Maria Osula and Henry Roigas (eds.,) *International Cyber Norms: Legal, Policy and Industry Perspective* (NATO CCD COE Publications, Tallinn 2016);
-Mikk Raud, 'China and Cyber: Attitudes, Strategies, Organization' (2016) NATO CCD COE;
-Henry Roigas, 'Mixed Feedback on the African Union Convention on Cyber Security and Data Protection' (2015) NATO CCD COD Incyder News;
-Michael N. Schmitt and Liis Vihul, 'The Nature of International Cyber Norms' in Anna Maria Osula and Henry Roigas (eds.) *International Cyber Norms: Legal, Policy and Industry Perspective* (NATO CCD COE Publications 2016);
-Peter Z. Stockburger, 'Control and Capabilities Test: Toward a New *Lex Specialis* Governing State Responsibility for Third Party Cyber Incidents' in H. Roigas, et al. (eds.) *9th*

International Conference on Cyber Conflict: Defending the Core (NATO CCD COE Publications 2017);
-Rolf H. Weber and Dominic N. Stainger, 'Privacy versus Security. Identifying the Challenges in a Global Information Society' in Joanna Kulesza and Roy Batteste (eds.) *Cybersecurity and Human Rights in the Age of Surveillance* (Rowman and Littlefield 2016);
-Katharina Ziolkowski, 'Peacetime Cyber Espionage-New Tendencies in Public International Law' in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publications, Tallinn 2013);
-Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in International Affairs' in Richard Falk (ed.) *Essays on Espionage and International Law* (Ohio State University Press 1962);

Reports by Non-Governmental and Other Organizations

-David Anderson, 'A Question of Trust. Report of the Investigatory Powers Review' (June 2015);
-American Civil Liberties Union, 'Privacy and Civil Liberties Oversight Board Hearing on Section 702 of the FISA Amendment Act' (2014);
-Centre for European Policy Studies, 'Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights' (2015);
-Centre for a New American Security, 'America's Cyber Future: Security and Prosperity in Information Age' (201);
-Electronic Frontier Foundation, 'Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its Illegal and Unconstitutional Use';
-Electronic Privacy Information Centre, 'Executive Order 12333';
-European Commission for Democracy Through Law (the Venice Commission), 'The Democratic Oversight of Signals Intelligence Agencies', Study No. 719/2013 (2015);
-Liberty, 'Liberty's Evidence to the Intelligence and Security Committee's Inquiry into Privacy and Security' (14 February 2014);
-KPMG China, 'Overview of China's Cybersecurity Law' (2017);
-Douwe Korff et al., 'Boundaries of Law: Exploring Transparency, Accountability and Oversight of Government Surveillance Regime' (2017) University of Cambridge Faculty of Law Legal Series;
-Mandiant, 'APT1 Exposing One of China's Cyber Espionage Units' (2011);
-Necessary and Proportionate Coalition, 'Necessary and Proportionate Global Legal Analysis' (2014);
-Privacy International, 'Eyes Wide Open. Special Report' (26 November 2013);
-Privacy International, 'Two Years After Snowden' (June 2015);
-Royal United Services Institute for Defence and Security Studies, 'A Democratic Licence to Operate. Report of the Independent Surveillance Review' (2015);

Articles

- Lukman Adebisi Abdulrauf and Charles Mage Fombad, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?' (2016) 8 Journal of Media Law;
-Philip Alston, 'The Myopia of the Handmaidens: International Lawyers and Globalization' (1997) 3 European Journal of International Law;

-Christopher Baker, ‘Tolerance of International Espionage: A Functional Approach’ (2004) 19 American University International Law Review;
-William Banks, ‘Pragmatic Surveillance and FISA: Of Needles in Haystacks’ (2010) 88 Texas Law Review;
-Yochai Benkler, ‘From Consumers to Users: Shifting the Deeper Structures of Regulating Toward Sustainable Commons and User Access’ (2000) 52 Federal Communications Law Journal;
-Richard Bilder, ‘The Anglo-Icelandic Fisheries Dispute’ (1973) Wisconsin Law Review;
-Jutta Brunnee and Tamar Meshel, ‘Teaching and Old Dog New Tricks: International Environmental Law Lessons for Cyber Governance’ (2015) German Yearbook of International Law;
-Nicholas N. Cade, ‘An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code’ (2010) 37 Brooklyn Journal of International Law;
-Warren Chik, ‘Customary Internet-tional Law: Creating a Body of Customary Law for Cyberspace. Part 1: Developing Rules for Transitioning Custom into Law’ (2001) 26 Computer Law and Security;
-Ronald J. Deibert and Masashi Crete Nishihata, ‘Global Governance and the Spread of Cyber Controls’ (2012) 18 Global Governance: A Review of Multilateralism and International Organizations;
-Geoffrey Demarest, ‘Espionage in International Law’ (1996) Denver Journal of International Law and Policy;
-Ashley Deeks, ‘An International Legal Framework for Surveillance’ (2015) 55 Virginia Journal of International Law;
-Hannes Ebert and Tim Maurer, ‘Contested Cyberspace and Rising Powers’ (2013) 34 Third World Quarterly;
-Kristine Eichensehr, ‘The Cyber-Law of Nations’ (2015) 103 Georgetown Law Journal;
-Graham Greenleaf, ‘Regulating Cyberspace: Architecture v Law?’ (1998) 21 The University of New South Wales Law Journal;
-Anitai Etzioni, ‘NSA-National Security v Individual Rights’ (2015) 30 Intelligence and National Security;
-Patrick Franzese, ‘Sovereignty in Cyberspace: Can it Exist?’ (2009) 64 Air Force Law Review;
-Erik Franckx, ‘The 200-mile Limit: Between Creeping Jurisdiction and Creeping Common Heritage?’ (2007) 39 George Washington International Law Review;
-Illina Georgieva, ‘The Right to Privacy Under Fire-Foreign Surveillance Under the NSA and the GCHQ and Its Compatibility with Art 17 ICCPR and Art 8 ECHR’ (2015) 31 Utrecht Journal of International and European Law;
-L. Goldie, ‘International Principles of Responsibility for Pollution’ (1970) 9 Columbia Journal of Transnational Law;
-Damon Greer, ‘Safe Harbour-Framework That Works’ (2011) International Data Privacy Law’;
-Gloria Gonzalez Fuster, Paul De Hert and Serge Gutwirth, ‘SWIFT and the Vulnerability of Transatlantic Transfers’ (2008) International Review of Law, Computers and Technology;
-Jack Goldsmith, ‘Against Cyberanarchy’ (1998) 65 University of Chicago Law Review;
-Jack Goldsmith, ‘Regulating the Internet: Three Persistent Fallacies’ (1998) 73 Chicago-Kent Law Review;
-Stephen Grove, ‘The Concept of ‘Common Heritage of Mankind’: A Political, Moral and Legal Innovation?’ (1972) 9 San Diego Law Review
-Onna Hathaway et al., ‘The Law of Cyber Attack’ (2012) 100 California Law Review;

-Julia Kalpokiene and Ingas Kalpokas, 'Hostes Humani Generis: Cyberspace, the Sea and Sovereign Control' (2012) Baltic Journal of Law and Politics;
-Harmut Hillgenberd, 'A Fresh Look at Soft Law' (1999) European Journal of International Law;
-Sean Kanuck, 'Sovereignty Discourse on Cyber Conflict Under International Law' (2010) 88 Texas Law Review;
-Robert Krueger, 'An Evaluation of the United Nations Ocean Policy' (1971) 17 McGill Law Journal;
-Christopher Kuner, 'The European Union and the Search for an International Data Protection Framework' (2014) Gronigen Journal of International Law;
-Christopher Kuner, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 Computer Las and Security Review;
-Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law Makers' (2017) Leiden Journal of International Law;
-Peter Margulies, 'The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism' (2014) 82 Fordham Law Review;
-Tim Maurer, 'Cyber Norm Emergence at the United Nations-An Analysis of the Activities at the United Nations Regarding Cyber Security' (2011) Belfer Centre of Science and International Affairs;
-Marco Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal;
-Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance' (2015) 9 International Affairs;
-John E. Noyes, 'The Common Heritage of Mankind: Past, Present and Future' (2012) 40 Denver Journal of International Law and Policy;
-Joseph S. Nye, 'Nuclear Lessons form Cyber Security?' (2011) Strategic Studies Quarterly;
-Jordan J. Paust, 'Can You Hear Me Now? Private Communications, National Security and the Human Rights Disconnect' (2015) 15 Chicago Journal of International Law;
-David Post and David Johnson, 'Law and Borders-Rise of Law in Cyberspace' (1996) 48 Stanford Law Review;
-Michael Peterson, 'The Use of Analogies in Developing Outer Space Law' (1997) 51(2) International Organization;
-Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 International Journal of Law and Information Technology;
-Roger D. Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 Air Force Law Review;
-Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006) 10 Max Plank Yearbook of United Nations Law;
-Antonio Segura-Serrano, 'Internet Regulation: A Hard Law Proposal' (2006) Jean Monnet Working Paper;
-Malcolm N. Show, 'Territory in International Law' (1982) 13 Netherlands Yearbook of International Law;
-Thomas Schultz, 'Carving u the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface' (2008) 19 European Journal of International Law;
-Christina Skinner, 'An International Law Response to Economic Cyber Espionage' (2014) 46 Connecticut Law Review;
-Ann Marie Slaughter, 'Security, Solidarity and Sovereignty: The Grand Themes of UN Reform' (2005) 99 American Journal of International Law;
-Jeffrey H. Smith, 'State Intelligence Gathering and International Law: Keynote Address' (2007) 28 Michigan Journal of International Law;

-Bruno Simma and Dirk Pulkowski, 'Of Planes and Universe-Self-Contained Regimes in International Law' (2005) 17 European Journal of International Law;
-William M. Stahl, 'Unchartered Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity' (2011) 40 Georgia Journal of International and Comparative Law;
-Lance Strate, 'The Varieties of Cyberspace: Problems of Definition and Delimitation' (1999) Western Journal of Communications;
-Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2006) 28 Michigan Journal of International Law;

Encyclopaedic and Dictionary Entries

-Bryan A. Garner (ed.) *Black's Law Dictionary* (West Group 1999);
-Max Plank Encyclopaedia of Public International Law, 'Spies' (September 2015);
-The Penguin Encyclopaedia (Penguin Books Ltd., 2006)

Internet Sources[1828]

- Dimitri Alperovitch, 'Bears in the Midst: Intrusion into the Democratic National Committee' (15 June 2015) < https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>;
-Dimitri Alperovitch, 'Revealed: Operation Shady Rat. An Investigation of Targeted Intrusions into More Than 70 Global Companies, Governments and Non-Profit Organizations During the Last Five Years' (2011) < http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf >;
-James Ball and Benjamin Gottlieb, 'Iran Preparing Internal Version of Internet' (2012) *The Washington Post* < https://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html?utm_term=.0e6775c5395f >;
-John Barlow, 'A Declaration of Independence for Cyberspace' (1999) <https://www.eff.org/cyberspace-independence >;
-Peter Bergen et al., 'Do NSA's Bulk Surveillance Programs Stop Terrorists?' (13 January 2014) New American Foundation, < https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/>;
-Christopher Bronk, 'Who Leads? Avoiding the Balkanization of Cyberspace' (2014), The International Relations Security Network < http://www.css.ethz.ch/en/services/digital-library/articles/article.html/181188/pdf >;
-*BBC News*, 'Edward Snowden: Leaks that Exposed US Spy Programme' (17 January 2014) < http://www.bbc.co.uk/news/world-us-canada-23123964 >;
-*BBC News*, 'US Ready to Hand Over the Internet's Naming System' (18 August 2016) < http://www.bbc.co.uk/news/technology-37114313 >;
-*BBC News*, 'US Resists Control of Internet Passing to UN Agency' (3 August 2012) < http://www.bbc.co.uk/news/technology-19106420>;
-Big Brother Watch, 'Briefing Note: Why Communications Data (Matadata) Matter?' < https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf>;

[1828] These sources were accessed between September 2013 and September 2017.

-Nazli Choucri and Daniel Goldsmith, 'Lost in Cyberspace: Harnessing the Internet, International Relations and Global Security' (2012) Bulletin of the Atomic Scientist < http://thebulletin.org/2012/march/lost-cyberspace-harnessing-internet-international-relations-and-global-security >;
-Fanny Coudert, 'Schrems vs Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities' (15 October 2015) European Law Blog < https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/ >;
-*Cybersecurity*, 'Apple vs FBI: All You Need to Know' (29 March 2016) < https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html >;
-*The Daily Telegraph*, 'Flame: World's Most Complex Computer Virus Exposed' (28 May 2012) < http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html >;
-Bill Davidov, 'The Tragedy of the Internet Commons' (18 May 2012) *The Atlantic* < https://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/ >;
-*The Diplomat*, 'China's Emerging Cyberspace Strategy' (24 May 2016) < http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/>;
-*The Economist*, 'The Future of the Internet: A Virtual Counter-Revolution' (2010) < http://www.economist.com/node/16941635>;
-*The Diplomat*, 'Evaluating the US-China Cybesecurity Agreement, Part 1: the US Approach to Cyberspace' (2017) < http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ >;
-Kristen Eichensehr, 'International Cyber Governance: Engagement Without Agreement?' (2015) Just Security < https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/>;
-David Fidler, 'Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations' (2013) American Society of International Law < https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision >;
-Glen Geenwald and Rayan Gallagher, 'New Zealand Launched Mass Surveillance Project Whilst Publically Denying It' (15 September 2014) <https://theintercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/ >;
-Lev Grossman, 'Inside Apple CEO Tim Cook's Fight with the FBI' (17 March 2017) <https://www.realclearpolitics.com/2016/03/17/inside_apple_ceo_tim_cook039s_fight_with_the_fbi_378538.html >;
-*The Guardian*, 'Top Democrat's Emails Hacked by Russia after Aid Made Typo, Investigation Finds' (14 December 2016) < *The Guardian*, 'Top Democrat's Emails Hacked by Russia after Aid Made Typo, Investigation Finds' >;
-*The Guardian*, 'FBI Director Stands by Claim that North Korea was Source of Sony Cyber Attack' (7 January 2015) < https://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey >;
-*The Guardian*, "UK-US Surveillance Regime Was Unlawful 'For Seven Years'" (6 February 2015) < https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa >;
-*The Guardian*, 'NSA Listed Merkel Among Leaders Subject to Surveillance-Report' (29 March 2014) <https://www.theguardian.com/world/2014/mar/29/nsa-merkel-leaders-surveillance-documents-snowden>;
-*The Guardian*, 'Not So Secret: Deal at the Heart of the UK-US Intelligence' (25 June 2010)

< https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released >;
-*The Guardian*, 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications' (21 June 2013) < https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa >;
-*The Guardian*, 'Senate Passes Controversial Cybersecurity Bill CISA 74 to 25' (27 October 2015) < https://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote>;
-*The Guardian*, 'Mass Surveillance is Fundamental Threat to Human Rights, Says European Report' (26 January 2015) < https://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe >;
-Kelly J. Higgins, 'Nation State Cyber Espionage. Targeted Attacks Becoming Global Norm' (2015) < http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025 >;
-Duncan Hollis, 'Stewardship versus Sovereignty? International Law and the Appropriation of Cyberspace' (2012) CyberDialogue <http://rescommunis.olemiss.edu/category/cyber/ >;
-*Huffington Post*, 'Obama Says NSA Programe Saved Lives' (19 June 2013) < http://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html>',
-Lawrence Hurley, 'US Court Hands Win to NSA over Metadata Collection' (28 August 2015) *Reuters*, <http://www.reuters.com/article/us-usa-court-surveillance-idUSKCN0QX1QM20150828>;
-Geoff Huston, 'Opinion: ICANN, the ITU, WSIS and Internet Governance' *Cisco*, < https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-31/internet-governance.html >;
- Geoff Huston, 'ICANN, the ITU and WSIS and Internet Governance-Part II' (2004) < https://www.apnic.net/community/ecosystem/igf/articles/icann-wsis-part-ii/>;
-*The Independent*, 'Surveillance Revelations: Angela Merkel Proposes European Network to Beat NSA and GCHQ Spying' (16 February 2014) <http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html >;
-*Information Warfare Monitor*, 'Tracking GhostNet: Investigating a Cyber Espionage Network, (29 March 2009) < http://www.nartv.org/mirror/ghostnet.pdf >;
Glenn Greenwald, 'NSA Collecting Phone Records of Missions of Verizon Customers Daily' (6 June 2013) *The Guardian* < https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order >;
-*Japantimes*, 'Britain's GCHQ 'the Brains', American's NSA 'the Money' Behind Spy Alliance' (18 November 2013) < http://www.japantimes.co.jp/article-expired/ >;
-Wu Jianguo, 'Defending the Cyber Territory' (1 March 2000) Liberation Army Daily < http://fliphtml5.com/cbtz/smzv/basic >;
-Adam Justice, "UN Committee Spotlights 'Highly Intrusive' Digital Spying" (2014) <https://amp.ibtimes.co.uk/un-committee-spotlights-highly-intrusive-digital-spying-12865 >:
-Kaspersky, 'Red October: Diplomatic Cyber Attacks Investigation. Report' (14 January 2013) < https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/ >;
-Wolfgang Kleinwacher, 'Internet Governance Outlook 2013: 'Cold Internet War' or 'Peaceful Internet Coexistence'?' (2013) <http://www.circleid.com/posts/20130103_internet_governance_outlook_2013/>;
-Wolfgang Kleinwacher, 'Internet Governance Outlook 2014: Good News, Bad News, No News?' (2014) <http://www.circleid.com/posts/20131231_internet_governance_outlook_2014_good_news_bad_news_no_news/ >;

-Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11 IEEE Computer and Reliability Societies <https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf>;
-Tim Leslie and Marc Concoran, 'Explained: Australia's Involvement with the NSA, the US Spy Agency at Heart of Global Scandal' (19 November 2013) <http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786 >;
-Natasha Lomas, 'European Rights Body Again Rejects Mass Surveillance' (22 April 2015) < https://techcrunch.com/2015/04/22/european-rights-body-again-rejects-mass-surveillance/ >;
-Ewan MacAskill et al., 'The Legal Loophole that Allow GCHQ to Spy on the World' (21 June 2013) *The Guardian* < https://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world>;
-*Liberty*, 'Draft Investigatory Powers Bill: Liberty Calls for Full Redraft as Committee Report Highlights Major Concerns' (11 February 2016) <https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/draft-investigatory-powers-bill-liberty-calls-full-redraft >;
-*The Local*, 'What Has France Actually Done to Fight Terrorism' (19 July 2016) < https://www.thelocal.fr/20160719/what-has-france-done-to-fight-terrorism >;
-Marko Milanovic, 'Foreign Surveillance and Human Rights Part I: Do Foreigners Deserve Privacy? (25 November 2013) EJIL: Talk! < https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/>;
-Marko Milanovic, 'Foreign Surveillance and Human Rights: Part 2: Interpreting the ICCPR' (2015) EJIL: Talk! < https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-2-interpreting-the-iccpr/ >;
Mandiant, 'Mandiant APT1 Exposing One of China's Cyber Espionage Units. Report' (2013) < https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf >;
-Kieran McCarthy, 'UN Takeover of Internet Postponed Indefinitely' (5 November 2014) <https://www.theregister.co.uk/2014/11/05/un_takeover_of_internet_postponed_indefinitely >
-Michael Muller et al., 'Net Neutrality as Global Principles for Internet Governance' (5 November 2007) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798314 >;
-Milton Mueller et al. 'The Internet and Global Governance: Principles and Norms for a New Regime' (2007) 13 Global Governance <https://akgul.bilkent.edu.tr/Governance/ggov.2007.13.2.pdf >;
-Mark Milian, 'Keepers of the Internet Face Their Greatest Challenges Ever' (2011) < http://edition.cnn.com/2011/12/22/tech/web/icann/index.html >;
-*The New York Times,* 'NSA Breached Chinese Servers Seen as Security Threat' (22 March 2014) < https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html >;
-*The New York Times*, 'Russian and China Sign Cooperation Pact' (8 May 2015) < https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?mcubz=0 >;
-Carly Nyst, 'Interface Based Jurisdiction Over Violations of the Right to Privacy' (21 November 2013) EJIL: Talk! < https://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/ >;
-NATO CCD COE, In Brief, 'An Updated Draft of the Code Distributed in the United Nations-What's New?' (10 February 2015) < https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>;

-Elliot Noss, 'A Battle for the Soul of the Internet' (2005) < http://www.zdnet.com/article/a-battle-for-the-soul-of-the-internet/ >;
-Jann Padova, 'Prism Scandal Threatens EU-US Safe Harbour Agreement' (12 November 2014) < http://www.euractiv.com/section/justice-home-affairs/opinion/prism-scandal-threatens-eu-us-safe-harbour-agreement/>;
-Robert Pepper and Chip Sharp, 'Summary Report on the ITU-T World Conference on International Telecommunications' (3-14 December 2012) <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-59/161-wcit.html >;
-Marietje Schaake, 'Stop Balkanizing the Internet' (2012) *Haffington Post* <http://www.huffingtonpost.com/marietje-schaake/stop-balkanizing-the-internet_b_1661164.html>;
-Laura Poitras and Glenn Greenwald, 'NSA Whistleblower Edward Snowden: I Don't Want to Live in a Society that Does These Sort of Things' (9 June 2013) *The Guardian* < https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video >;
-David Post, 'Stand Down! UN 'Takeover of the Internet' Postponed Indefinitely' (7 November 2014) < https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/07/stand-down-un-takeover-of-the-internet-postponed-indefinitely/?utm_term=.18d2032e9c52 >;
-Privacy International, 'The Five Eyes' < https://www.privacyinternational.org/node/51>;
-Michael D. Swaine, 'Chinese Views on Cyber Security in Foreign Relations' (30 July 2013) Leadership Monitor <http://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf >;
-*The Saturday Evening Post*, 'A Brief History of the NSA: From 1917 to 2014' (17 April 2014) < http://www.saturdayeveningpost.com/2014/04/17/culture/politics/a-brief-history-of-the-nsa.html>;
-Ian Shapira, 'Obama Administration Joins Critics of US Non-profit Groups that Overseas Internet' (2010) < http://www.washingtonpost.com/wp-dyn/content/article/2011/02/28/AR2011022803719.html >;
-John Tye, 'Meet the Executive Order 12333: The Reagan Rule that Lets the NSA Spy on Americans' (14 July 2014) < https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html >;
-*The Washington Post*, 'US and Russia Sign Pact to Create Communication Link on Cyber Security' (17 June 2013) < https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html?utm_term=.ac4ec0598872 >;
- *Wired*, 'Chinese Military Group Linked to Hacks of More Than 100 Companies' (19 February 2013) < https://www.wired.com/2013/02/chinese-army-linked-to-hacks/>;
-*Wired*, 'US and China Reach Historic Agreement on Cyber Espionage*'* (25 September 2015) < https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/ >;
-*Wired, '*A Simple Guide to GCHQ's Internet Surveillance Programme Tempora' (24 June 2013) < http://www.wired.co.uk/article/gchq-tempora-101 >;
-Rui Zhang, 'China Headlines: Xi Slams 'Double Standards', Advocates Shared Future of Cyberspace' (17 December 2015) < http://news.xinhuanet.com/english/indepth/2015-12/16/c_134924012.htm >;
-Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China' Berkman Centre for Internet and Society < https://cyber.harvard.edu/filter