World wide warfare: Jus ad bellum and the use of cyber force

Roscini, M.

This is a copy of a chapter published in von Bogdandy, Armin and Wolfrum, Rüdiger and Philipp, Christiane E, (eds.) Max Planck Yearbook of United Nations Law. Martinus Nijhoff Publishers, Leiden, pp. 85-130. ISBN 9789004194212, 2010.

It is republished here with permission from the series editor.

World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force

Marco Roscini[*]

"So cyberspace is real.
And so are the risks that come with it."
Barack Obama[1]

A. von Bogdandy and R. Wolfrum, (eds.),
Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 85-130.

[*] I am grateful to Barbara Sonczyk for her research assistance and to Matt Evans for explaining to me the intricacies of cyber technologies. All errors are of course mine. This article is based on developments as of June 2010.

1 The White House, Office of the Press Secretary, "Remarks on securing the nation's cyber infrastructure", Press Release, 29 May 2009, <www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>.

I. Introduction: *hic sunt leones*

"Here be lions." This is what ancient Roman and medieval cartographers used to write on maps over unexplored territories, implying that unknown dangers could lie there. If "cyberspace" were a real location appearing on geographical maps and not just a virtual domain, we would probably read that expression over it.[2] Indeed, societies have be-

---

2 "Cyberspace" is defined in the United States National Military Strategy for Cyberspace Operations as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures" (United States Department of Defense (DoD), *The National Military Strategy for Cyberspace Operations*, December 2006, 3 <www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf>). Cyberspace, then, goes beyond the Internet and includes all networked digital activities. The updated Doctrine for the Armed Forces of the United States contains a slightly different definition of cyberspace ("[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers", Armed Forces of the United States, *Doctrine for the Armed Forces of the United States*, Joint Publication

come increasingly dependent on computers and computer networks, with vital services now relying on the Internet. However, the more technologically advanced a state is, the more vulnerable to cyber attacks: if computer networks become the "nerve system" of civilian and military infrastructures, incapacitating them means paralyzing the country.[3] The threat no longer comes exclusively from the proverbial teenage hacker, but also from ideologically motivated individuals ("hacktivists"), states and criminal and terrorist organizations.[4] Geographical distance and frontiers are also irrelevant, as a target could be hit on the other side of the world in a matter of seconds. The problem is likely to acquire more and more importance in the upcoming years. If cyber attacks have had so far limited material consequences, there is general agreement among experts that such attacks will increase in the future, both in number and severity.[5] As noted by the United States National Strategy to Secure Cyberspace, "the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving."[6] Cyber technologies and expertise are relatively easy and cheap to acquire, which allows weaker states and even non-state actors to cause considerable damage to countries with superior conventional military

---

1, 2 May 2007 – Incorporating Change 1, 20 March 2009, at GL-7 <www.dtic.mil/doctrine/new_pubs/jp1.pdf >).

3 The United States National Strategy to Secure Cyberspace, for instance, acknowledges that "[b]y 2003, our economy and national security became fully dependent upon information technology and the information infrastructure", United States Government, *The National Strategy to Secure Cyberspace*, February 2003, 6 <www.us-cert.gov/reading_room/cyberspace_strategy.pdf>. The new United States National Security Strategy also recalls that "[t]he very technologies that empower us to lead and create also empower those who would disrupt and destroy", *National Security Strategy*, May 2010, 27 <www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

4 As noted in the Australian Cyber Security Strategy, "[t]he distinction between traditional threat actors – hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services – increasingly appears to be blurring", Australian Government, *Cyber Security Strategy*, 2009, 3 <www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf>.

5 McAfee Report, *In the Crossfire – Critical Infrastructure in the Age of Cyber War*, 2010, 11 <http://resources.mcafee.com/content/NACIPReport >.

6 United States National Strategy to Secure Cyberspace, see note 3, 6.

power: a cyber attack could for instance disable power generators, cut off the military command, control and communication systems, cause trains to derail and airplanes to crash, nuclear reactors to melt down, pipelines to explode, weapons to malfunction.

It is therefore hardly surprising that cyber security has become a general concern of the international community, with the UN General Assembly adopting a series of resolutions on the issue emphasizing that "the dissemination and use of information technologies and means affect the interests of the entire international community,"[7] that "the criminal misuse of information technologies may have a grave impact on all States"[8] and that these technologies "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security."[9] The General Assembly also endorsed the holding of the World Summit on the Information Society, that took place, in two phases, in Geneva in 2003 and Tunis in 2005.[10]

One of the perspectives from which an international lawyer can study the problem of cyber security is that of *jus ad bellum*, i.e. the rules that regulate the use of armed force by states in their international relations.[11] In fact, although – as will be seen – identification is problematic, several states have been the target of cyber attacks of which other states were suspected. In certain cases, the cyber attacks were an end in themselves. The United States, for instance, has been the target

---

7 See, e.g., the Preambles of Resolutions A/RES/55/28 of 20 November 2000, A/RES/56/19 of 29 November 2001, A/RES/59/61 of 3 December 2004, A/RES/60/45 of 8 December 2005, A/RES/61/54 of 6 December 2006, A/RES/62/17 of 5 December 2007, A/RES/63/37 of 2 December 2008, A/RES/64/25 of 2 December 2009.

8 See, e.g., the Preambles of Resolutions A/RES/55/63 of 4 December 2000, A/RES/56/121 of 19 December 2001.

9 See, e.g., the Preambles of Resolutions A/RES/58/32 of 8 December 2003, A/RES/59/61 of 3 December 2004, A/RES/60/45 of 8 December 2005, A/RES/61/54 of 6 December 2006, A/RES/62/17 of 5 December 2007, A/RES/63/37 of 2 December 2008, A/RES/64/25 of 2 December 2009.

10 For the documents adopted at the Summit, see <www.itu.int/wsis/index.html>.

11 Another perspective would be the applicability of *jus in bello* (i.e., international humanitarian law) to cyber warfare, which is however outside the scope of the present article. On this aspect, see M.N. Schmitt, "Wired Warfare: Computer Network Attack and *jus in bello*", in: M.N. Schmitt/ B.T. O'Donnell (eds), *Computer Network Attack and International Law*, 2001, 187 et seq.

of several attacks, allegedly originating from China.[12] Most famously, in April 2007 Estonia was the victim of a three week cyber attack that shut down government websites first and then extended to newspapers, TV stations, banks and other targets.[13] Peacetime cyber attacks have also hit, among others, the United Kingdom,[14] Taiwan,[15] South Korea,[16] Lithuania[17], Kyrgyzstan[18], Switzerland[19] and Montenegro.[20] In other

---

12 See, for instance, the 2003 "Titan Rain" attack, that infiltrated governmental computer networks in the United States for four years through the installation of back door programs to steal information, S.J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law* 27 (2009), 192 et seq. (204).

13 D.B. Hollis, "Why States Need an International Law for Information Operations", *Lewis and Clark Law Review* 11 (2007), 1023 et seq. (1024-1025). The attack followed the Estonian Government's decision to remove a Russian war monument, the "Bronze Soldier", from the Tallinn city centre.

14 J. Richards, "Thousands of cyber attacks each day on key utilities", *The Times*, 23 August 2008. According to the Annual Report 2009-2010 of the United Kingdom Intelligence and Security Committee, the greatest threat of electronic attacks to the United Kingdom comes from states, in particular from the Russian Federation and China, <www.cabinetoffice.gov.uk/media/348175/isc-annualreport0910.pdf>, United Kingdom Intelligence and Security Committee, *Annual Report 2009-2010*, March 2010, 16.

15 S.W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law and Criminology* 97 (2006-2007), 379 et seq. (402).

16 M. Weaver, "Cyber attackers target South Korea and US", *The Guardian*, 8 July 2009.

17 In June 2008, after the Lithuanian Parliament adopted a law prohibiting the public display of Soviet symbols, political and private websites were defaced, S. Rhodin, "Hackers Tag Lithuanian Web Sites With Soviet Symbols", *The New York Times*, 1 July 2008.

18 D. Bradbery, "The fog of cyberwar", *The Guardian*, Technology Supplement, 5 February 2009, 1.

19 M. Barkoviak, "Swiss Ministry Suffers Cyber Attack", *Daily Tech*, 28 October 2009 <www.dailytech.com/Swiss+Ministry+Suffers+Cyber+Attack/article16629.htm>.

20 A cyber attack forced the shut down of more than 150 websites, including the postal service and several banks' websites in March 2010. The attack apparently originated in Kosovo <www.uspoliticsinfo.com/article/Cyber attack%20shut%20150%20Montenegrin%20websites/?k=j83s12y12h94s27k02>.

cases, the cyber attacks preceded or were contextual to an armed conflict or operation. It appears, for instance, that immediately after the beginning of Operation Allied Force in 1999, hackers tried to disrupt NATO's e-mail communication system by overloading it, while the United States considered penetrating into Yugoslavia's computer networks to disrupt its military operations but eventually cancelled the plan because of doubts on its legality.[21] The Russian Federation used cyber warfare in the second Chechen war against the insurgents' websites in order to prevent them from delivering anti-Russian propaganda.[22] The cyber attacks on Georgia in July-August 2008, that occurred immediately before and during the armed conflict with the Russian Federation, caused the governmental websites to go off line and slowed down Internet service. Furthermore, websites were defaced and their content replaced with Russian nationalistic propaganda.[23] Cyber attacks also targeted several of Israel's governmental websites during the 2008-2009 Operation Cast Lead in the Gaza Strip.[24]

In spite of this increasing number of cases, there still does not seem to be enough research on how the existing rules on the use of force apply, if at all, to cyber attacks. Most of the few existing publications on *jus ad bellum* and cyber force are written by American scholars and practitioners, published in American journals and taking mainly United States documents into account, with a view to establishing whether the United States is entitled to react in self-defense in case of a cyber attack against it. The scope of this article is broader, as it expands the focus to include the practice of other technologically advanced states and also goes beyond the law of self-defense.

---

21 Shackelford, see note 12, 205; D.B. Silver, "Computer Network Attack as a Use of Force under Article 2 (4) of the United Nations Charter", in: Schmitt/ O'Donnell, see note 11, 74; N. Solce, "The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force", *Albany Law Journal of Science and Technology* 18 (2008), 293 et seq. (315).

22 <www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf> Cooperative Cyber Defense Centre of Excellence (CCDCOE), *Cyber Attacks Against Georgia: Legal Lessons Identified*, November 2008, 5.

23 J. Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*, 13 August 2008. "Defacement" is the replacement of the content of the website in order to change its visual appearance.

24 <http:csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_ Conflict.pdf>, J.A. Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict", Centre for Strategic and International Studies (CSIS), October 2009, 8.

The analysis will be limited to the use of cyber force by a state against another state: cyber attacks conducted by non-state actors will be discussed only for the purpose of determining when they can be attributed to a state. Therefore, this article will deal neither with cyber crime, i.e. the offences against the confidentiality, integrity and availability of computer data and systems committed by individuals or private entities for personal gain (for instance, theft of money from bank accounts), which is mainly treated under domestic criminal laws,[25] nor with cyber terrorism, which is the unlawful use of cyber technologies by terrorist organizations or individuals for ideological purposes.

Chapter II. will clarify the terminology and attempt to give some definitions. Issues of state responsibility in relation to the use of cyber force will then be discussed in Chapter III., with a view to establishing when the conduct of hackers can be imputed to a state. Chapter IV. will determine whether a cyber attack amounts to a use of force under Article 2 para. 4 of the UN Charter, while Section V. will discuss the remedies available to states being victims of cyber attacks. Finally, an attempt will be made to establish if any customary international law rules have already been developed with regard to the right to invoke self-defense against a cyber attack.

II. Definitions

Cyber attacks fall within the broader category of what are traditionally known as information operations. "Information operations" (of which "information warfare" is a subcategory undertaken in the context of an armed conflict)[26] are the "integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, cor-

---

25 But see the 2001 Council of Europe's Convention on Cyber Crime, which seeks to harmonize national laws, improve investigative techniques and increase cooperation among nations in the field. The Convention entered into force in 2004. An additional protocol adopted in 2002 and entered into force in 2006 requires the parties to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

26 M.N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Colum. J. Transnat'l L.* 37 (1998-1999), 885 et seq. (890 – 891).

rupt, or usurp adversarial human and automated decision making while protecting our own."[27] According to the 2006 United States National Military Strategy for Cyberspace Operations, "computer network operations" (CNO) include computer network attacks (CNA), computer network defense (CND) and "related computer network exploitation enabling operations" (CNE).[28] Although they are often labeled in the press as "cyber attacks", CNE operations are different as they focus on intelligence collection and observation rather than on network disruption and can be preliminary to an attack.[29] They can aim at disseminating information for propaganda purposes, for instance through the defacement of websites.[30] CNE operations could also aim at stealing sen-

---

27 United States National Military Strategy for Cyberspace Operations, see note 2, GL-2; Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13, 13 February 2006, GL-9 <www. dtic.mil/doctrine/new_pubs/jp3_13.pdf>. According to a previous DoD document, information operations include "[a]ny action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces" (United States DoD, *An Assessment of International Legal Issues in Information Operations*, May 1999, 5 <www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>). Information operations include not only information warfare, but also information assurance, defined as "[i]nformation operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities", Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, see above, GL-9. Information assurance, thus, involves not only military action, but also government and private sector activities, D.T. Kuehl, "Information Operations, Information Warfare, and Computer Network Attack – Their Relationship to National Security in the Information Age", in: Schmitt/O'Donnell, see note 11, 37.

28 United States National Military Strategy for Cyberspace Operations, see note 2, GL-1.

29 S. Watts, "Combatant Status and Computer Network Attack", *Va. J. Int'l L.* 50 (2010), 391 et seq. (400 et seq.).

30 During the 2008 attacks on Georgia, for instance, the websites of Georgia's President, Minister of Foreign Affairs and National Bank were defaced and replaced with a series of pictures of Mikhail Saakashvili and Adolf Hitler (CCDCOE Report, see note 22, 7-8). The use of the Internet for propaganda purposes is also well-known to terrorist organizations: see *Security for the Next Generation*, The National Security Strategy of the United

sitive information from computers. In this regard, "trap doors" and "sniffers" are particularly useful tools for cyber espionage: the former allow an external user to access software at any time without the computer's owner being aware of it, while the latter are programs executed from a remote computer that intercept and record data passing over a network in order to steal user IDs and passwords. Espionage is, however, not prohibited by international law, although it is usually criminalized at the domestic level.[31]

This article will not deal with CNE operations, but only with CNA and CND, i.e. those computer network operations that go beyond mere exploitation and are accompanied by a hostile intent: such attacks aim at altering or destroying the information contained in the targeted computer or computer network with the purpose of incapacitating the adversary's command, control and communication system and/or of causing damage extrinsic to the targeted computer/network. The most used methods to incapacitate a computer or computer network are, apart from its physical destruction, the corruption of its hardware ("chipping")[32] or software, or flooding it with so much information to cause its collapse ("denial of service" (DoS)). Popular software tools designed to interfere with the normal functioning of a computer are Trojan horses, logic bombs, viruses and worms, which can be installed in a computer through chipping, hacking, or by simply e-mailing them.[33] A virus is a self-replicating program that usually attaches itself to a legitimate program on the target computer, modifying it and subsequently

---

Kingdom: Update 2009, June 2009, 105, <www.cabinetoffice.gov.uk/media/216734/nss 2009v2.pdf>.

31 Y. Dinstein, "Computer Network Attacks and Self-Defense", in: Schmitt/O'Donnell, see note 11, 101; R.W. Aldrich, "How do you know you are at War in the Information Age?", *Houston Journal of International Law* 22 (1999-2000), 223 et seq. (252). It appears, for instance, that a 2009-2010 cyber-spying operation originating from China stole classified Indian security documents and accessed e-mails from the office of the Dalai Lama, T. Branigan, "Cyber-spies based in China target Indian Government and Dalai Lama", *The Guardian*, 6 April 2010.

32 "Chipping" involves "integrating computer chips with built-in weaknesses or flaws", T.A. Morth, "Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the U.N. Charter", *Case Western Reserve Journal of International Law* 30 (1998), 567 et seq. (572).

33 S.J. Cox, "Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War", *Houston Law Review* 42 (2005-2006), 881 et seq. (888 - 889).

affecting other programs and, if the computer is connected to a network, other computers as well. A worm replicates itself in its entirety into other computers but, unlike viruses, does not usually modify other programs: it captures the addresses of the target computer and resends messages throughout the system so to cause a general slowdown and potentially a crash. Viruses and worms can be hidden in Trojan horses, an apparently innocuous code fragment that actually conceals a harmful program or allows remote access to the computer by an external user. Time and logic bombs are a type of Trojan horse designed to execute at a specific time or by certain circumstances, respectively. As to DoS attacks, they aim at flooding a target's network with requests in order to overload and incapacitate it. When the DoS attack is carried out by a large number of computers, it is referred to as a "distributed denial of service" (DDoS) attack. Estonia was the victim of a DDoS attack in 2007, when requests from more than a million computers based in over 100 countries hijacked and linked through the use of botnets[34] flooded governmental and private websites and caused servers to crash.[35] In January 2009, Kyrgyzstan was also the target of a DDoS attack allegedly originating from the Russian Federation, which took 80 per cent of the Internet traffic to the west offline.[36]

The most famous definition of CNA is probably that of the United States DoD, which describes them as "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[37] This often cited definition distinguishes between two types of CNA, those target-

---

34 "Botnets" (short for "robot networks"), which are the source of most spam, are networks of infected computers hijacked from their unaware owners by external users; linked together, such networks can be used to mount massive DDoS attacks, McAfee Report, see note 5, 6. The Mariposa botnet, started in 2008 and recently dismantled, was one of the world's biggest with up to 12.7 million computers controlled, C. Arthur, "Alleged controllers of 'Mariposa' botnet arrested in Spain", *The Guardian*, 3 March 2010.

35 Hollis, see note 13, 1024 - 1025.

36 Bradbery, see note 18, 1.

37 United States National Military Strategy for Cyberspace Operations, see note 2, GL-1. This definition is criticized by Dinstein, who argues that "[h]ad [it] be legally binding – or had it factually mirrored the whole gamut of the technological capabilities of the computer – the likelihood of a CNA ever constituting a full-fledged armed attack would be scant", Dinstein, see note 31, 102.

ing the computer or computer network and those targeting the information contained in the computer or computer network. It is unclear whether the DoD's definition encompasses "the manipulation of a computer network to achieve an effect extrinsic to the network itself, as opposed to merely rendering the network ineffective."[38] The recent Manual on International Law Applicable to Air and Missile Warfare, adopted by the Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University in 2009, reformulates the DoD's definition of CNA to also cover operations that "manipulate" computer information and that aim "to gain control over the computer or computer network."[39] The Commentary to the Manual specifies that the attack "can be directed against an individual computer, specific computers within a network, or an entire computer network" and that not all CNAs are attacks as defined by Rule 1 (e), i.e. "act of violence, whether in offence or in defence."[40] Both the DoD and HPCR definitions, however, focus on the computer system as a target and therefore also include conventional attacks on computer network facilities.[41] The 2006 United States Joint Doctrine for Information Operations takes a narrower approach when it defines CNAs as "actions taken *through the use of computer networks* to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves,"[42] but does not mention attacks aimed at causing damage extrinsic to the computer or computer network.

This article will use the expressions "cyber force" and "cyber attacks" in order to be consistent with *jus ad bellum* language.[43] "CNA"

---

38 Silver, see note 21, 76.

39 HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, 15 May 2009, Rule 1 (m) <http://ihlresearch.org/amw/HPCR%20Manual.pdf>. Although the HPCR Manual is not a draft treaty, it is significant as it presents a methodical restatement of existing international law based on the general practice of states accepted as law and treaties in force.

40 <http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf> *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, March 2010, 34 .

41 Kuehl, see note 27, 44 - 45.

42 Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, see note 27, II-5 (emphasis added).

43 According to the Oxford English Dictionary, "cyber" means "relating to information technology, the Internet, and virtual reality", J.A. Simpson/E.S.C. Weiner, *The Oxford Compact English Dictionary,* 2003, 268.

is also somehow misleading, as the target of the cyber operation could be not only computer networks, but also individual computers or certain computers within a network, as well as websites. In the context of this study, thus, "cyber attacks" are a hostile use of cyber force, which could be an isolated act, the first strike of an armed conflict, an attack in the context of an already initiated armed conflict, or a reaction against a previous conventional or cyber attack. By "cyber force", the present author will refer to operations taken by a state against another state, in offense or in defense, through the use of information resident in individual computers, some computers within a network or entire computer networks, with the purpose of incapacitating the target computer, computer network or website and/or of producing damage extrinsic to the computer or network. This definition, which focuses on computers and computer networks as weapons and not as targets, does not cover - and therefore excludes from the scope of this article - kinetic attacks on computer facilities (as the operation must be carried out through computers or computer networks),[44] cyber espionage and cyber propaganda (as the purpose of the operation must be either incapacitating the network and/or causing extrinsic physical damage).

III. Identification and Attribution Problems

Even before discussing attribution, when it comes to cyber force there is an identification problem. Anyone launching cyber attacks can disguise their origin thanks to tricks like IP spoofing or the use of botnets.[45] Anonymity is in fact one of the greatest advantages of cyber warfare: even though the attacks might appear to originate from computers located in a certain country, this does not necessarily mean that that country, or even the owners of the computers involved, were behind such actions.[46] The 2007 attack on Estonia, for instance, originated

---

44 Bombing a communication facility through kinetic means would be an information operation, but not a cyber attack. Existing *jus ad bellum* and *jus in bello* rules apply without problems to the use of traditional weapons against a computer and computer networks.

45 D. Delibasis, *The Right to National Self-Defence in Information Warfare Operations*, 2007, 303.

46 Brenner, see note 15, 424. The 2003 United States National Strategy to Secure Cyberspace emphasizes that "[t]he intelligence community, DoD, and the law enforcement agencies must improve the Nation's ability to quickly

from countries such as the United States, Egypt, Peru and the Russian Federation, while the 1998 "Solar Sunrise" attack that broke into the United States DoD's system was carried out by an Israeli teenager and Californian students through a computer based in the United Arab Emirates.[47]

It is, however, not impossible that the state responsible for the cyber attack is eventually identified. For instance, the cyber attack might be followed by a conventional attack that will reveal the author.[48] Further developments in computer technology and Internet regulations might also make it easier to identify the source of the cyber attack.[49] Assuming that the authors are identified, the problem arises as to whether the attack can be attributed to a state under the law of state responsibility so to trigger the application of the *jus ad bellum* rules. Indeed, unlike in traditional warfare, cyberspace attacks can easily be carried out not only by states, but also by groups and even individuals: all it takes is a computer, software and a connection to the Internet.[50] According to the United States DoD, "state sponsorship may be convincingly inferred from such factors as the state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks."[51] This is, however, too vague. The answers should be searched for in the first part of the Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission (ILC) in 2001 and subsequently endorsed by the General Assembly.[52]

In this context several scenarios can be identified. The first and easiest one is the case of "uniformed" hackers. Although details of state military cyber capabilities are classified, it appears that several national armies have already established cyber units. China is for instance re-

---

attribute the source of threatening attacks or actions to enable timely and effective response", see note 3, 50.

47 Shackelford, see note 12, 204, 231.

48 Dinstein, see note 31, 112.

49 Ibid.

50 R. Barnett, "A Different Kettle of Fish: Computer Network Attack", in: Schmitt/ O'Donnell, see note 11, 22.

51 DoD, *An Assessment*, see note 27, 21-22.

52 Read the text of the articles in: ILC (ed.), *Yearbook of the International Law Commission*, 2001, Vol. II, Part Two, 26 et seq.

ported to have formed cyberspace battalions and regiments[53] and Israel also appears to have its own soldiers working in an "Internet warfare" team.[54] The United States has recently established a military Cyber Command, to counter cyber attacks.[55] Germany's army has also its own cyber unit, the Department of Information and Computer Network Operations,[56] while Italy is reported to be considering establishing one.[57] It goes without saying that the uniformed hackers' conduct would be imputable to the state of which they are *de jure* organs.[58] This conclusion would not change if the hackers were civilian, and not military organs of a state. The United Kingdom, for instance, has established a Cyber Security Operations Centre that will monitor the Internet for threats to the United Kingdom and coordinate incident response.[59] Australia and Brazil have done the same.[60] It could also be that the hackers are members of government agencies or parastatal entities, like privatized corporations or independent contractors empowered by law to exercise some degree of governmental authority: in all

---

53 S.M. Condron, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law and Technology* 20 (2006-2007), 373 et seq. (405); E.T. Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence", *Stanford J. Int'l L.* 38 (2002), 207 et seq. (212); Watts, see note 29, 405.

54 D. Eshel, "Israel Adds Cyber-Attack to IDF", 10 February 2010, <www.military.com/features/ 0,15240,210486,00.html>.

55 P. Beaumont, "US appoints first cyber warfare general", *The Observer*, 23 May 2010, 10.

56 J. Goetz/ M. Rosenbach/ A. Szandar, "National Defense in Cyberspace", *Spiegel Online International*, 2 November 2009.

57 T. Kington, "Italy Weighs Cyber-Defense Command", *Defense News*, 31 May 2010, <www.defensenews.com/story.php?i=4649478>.

58 According to article 4 of the 2001 ILC Articles on State Responsibility, "[t]he conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State."

59 United Kingdom Government, *Cyber Security Strategy of the United Kingdom*, June 2009, 5 <www.cabinetoffice.gov.uk/media/216620/css0906.pdf>.

60 McAfee Report, see note 5, 36. Information on Australia's Cyber Security Operations Centre is available at <www.dsd.gov.au/infosec/csoc.html>.

such cases, their conduct will be attributed to the state "provided the person or entity is acting in that capacity in the particular instance."[61]

The hackers could also be not *de jure* organs of a state, but rather individuals or corporations hired by states in order to conduct cyber attacks.[62] A well-known example is the Russian Business Network (RBN), a cybercrime firm specializing in phishing, malicious code, botnet command-and-control, DoS attacks and identity theft, which is suspected of having executed the cyber attacks against Georgia.[63] When can the conduct of such individuals and corporations be attributed to the state? Article 8 of the ILC Articles provides that, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." In the Nicaragua case, the ICJ argued that, "United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras*, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself [...] for the purpose of attributing to the United States the acts committed by the *contras* in the course of their military or paramilitary operations in Nicaragua". What has to be proven is that "that State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed."[64] While the ICJ claimed that,"[t]he rules

---

61 ILC Articles on State Responsibility, article 5, see note 52.

62 J.A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", *Duke Law and Technology Review* 3 (2010), paras 12-18 <www.law.duke.edu/journals/dltr/articles/pdf/2010 dltr003.pdf>. Such corporations are allegedly paid by governments to carry out elements of the cyber attacks, Watts, see note 29, 411.

63 CCDCOE Report, see note 22, 11; Markoff, see note 23.

64 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), ICJ Reports 1986, 14 et seq. (64 para. 115). In the Genocide case, the ICJ returned to the point and clarified that "[i]t must […] be shown that this 'effective control' was exercised, or that the State'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" (Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Merits, Judgment of 26 February 2007, <www.icj-cij.org>, para. 400).

for attributing alleged internationally wrongful conduct to a State do not vary with the nature of the wrongful acts in question in the absence of a clearly expressed *lex specialis*",[65] according to the International Criminal Tribunal for the former Yugoslavia (ICTY) "[t]he degree of control may […] vary according to the factual circumstances of each case."[66] The ICTY then adopted a much less restrictive test to attribute the conduct of militarily organized armed groups to a foreign state. Under the ICTY "overall" control test, for the actions of such groups to be imputed to a state it is sufficient that the state "has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group […] regardless of any specific instructions by the controlling State concerning the commission of each of those acts."[67]

A commentator has suggested that, due to the inherently clandestine nature of cyber activities and the technical difficulty of identifying the authors, the *Tadić* test should be preferred to the *Nicaragua* test when cyber attacks are concerned.[68] This view cannot be shared: indeed, it is exactly because of the identification problems linked to cyber activities that the "effective control" test is preferable, as it would prevent states from being frivolously accused of cyber attacks (especially if the victim state claims a right to self-defense against them). Furthermore, the above mentioned view misses an important point: the ICTY applies the overall control test only to the case of an "organised and hierarchically structured group, such as a military unit or, in case of war or civil strife, armed bands of irregulars or rebels."[69] "[O]rganised and hierarchically structured" cyber insurgents do not seem to exist yet.[70] For the case of

---

65 Ibid., para. 401.

66 ICTY, Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999, <www.icty.org>, para. 117.

67 Ibid., para. 137. The ICJ noted that "the [ICTY] 'overall control' test has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf", ICJ Application of the Convention, see note 64, para. 406.

68 Shackelford, see note 12, 235.

69 Tadić, see note 66, para. 120.

70 It has however been suggested that certain armed groups, such as Hamas and Hezbollah, may have hired cyber criminals in order to conduct cyber operations, Lewis, see note 24, 8.

a "private individual who is engaged by a State to perform some specific illegal acts in the territory of another State (for instance, […] carrying out acts of sabotage)" and of unorganized, non-military and non-hierarchical groups of individuals, such as RBN, the ICTY retains the effective control test, i.e. the need to prove the issue of specific instructions concerning the commission of the illegal act or the state's public retroactive approval of the individual's actions.[71] With specific regard to cyber attacks, then, there is no substantial practical discrepancy between the ICJ and the ICTY approaches, as both would probably lead in most cases to the application of the effective control test.

A third scenario is when the hackers are neither *de jure* nor *de facto* state organs, but their conduct has been incited by state agents, for instance in websites, chat rooms and e-mails. In 2001, for example, after a United States Navy spy plane collided with a Chinese jet fighter in the South China Sea, websites appeared offering instructions to hackers on how to incapacitate United States government computers.[72] Russian blogs, forums and websites also published instructions on how to ping flood Georgian government websites as well as a list of vulnerable Georgian websites.[73] There is no express regulation of incitement in the ILC Articles on State Responsibility.[74] Incitement would thus entail state responsibility for the incited actions only to the extent it amounts to direction and control (article 8).[75] After inciting the actions, however, state authorities might subsequently publicly endorse them: in the Hostages case, the ICJ held that, although the initial attack on the United States Embassy in Teheran was not attributable to Iran, the subsequent endorsement by the Iranian authorities and the decision to perpetuate the occupation transformed the occupation and detention of the hostages into acts of the state.[76] Article 11 of the ILC Articles on State Responsibility confirms that, "[c]onduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State

---

71 Tadić, see note 66, para. 118.

72 N. Weisbord, "Conceptualizing Aggression", *Duke J. Comp. & Int'l L.* 20 (2009), 1 et seq. (20).

73 CCDCOE Report, see note 22, 9-10.

74 When expressly provided, however, incitement can be an unlawful act *per se*, see, e.g., article III of the 1948 Genocide Convention.

75 See ILC, see note 52, 65.

76 United States Diplomatic and Consular Staff in Teheran (United States v. Iran), ICJ Reports 1980, 3 et seq. (35 para. 74).

acknowledges and adopts the conduct in question as its own." Public acknowledgement of cyber attacks by state agents is however unlikely to occur: as already noted, cyber technologies are the perfect tool for covert operations.

Finally it could be that the cyber attacks originate from computers located in a certain state without any state involvement. In such case, the hackers' conduct could not be imputed to that state, which might, however, be held responsible for not taking the necessary and reasonable measures to prevent or stop the attack (for instance, by disabling the Internet access of the perpetrators). The state's wrongful act, however, would not be the cyber attack, but rather the breach of its obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[77] It appears, for instance, that, even though no evidence was found of state organizations directing the attack, the Russian Federation at least tolerated the attacks against Estonia and Georgia originating from Russian hacker sites.[78] The Russian Federation also did not cooperate with Estonia in tracking down the mastermind behind the botnets and a request for bilateral investigation under the Mutual Legal Assistance Treaty between the two countries was rejected by the Russian Supreme Procurature.[79]

IV. Cyber Attacks and the Prohibition of the Threat and Use of Force in International Relations

When attributed to a state, a cyber attack is a violation of the customary principle of non-intervention "on matters in which each State is permit-

---

77 Corfu Channel (United Kingdom v. Albania), ICJ Reports 1949, 4 et seq. (22). A/RES/55/63 of 4 December 2000 recommends that states ensure "that their laws and practice eliminate safe havens for those who criminally misuse information technologies" (para. 1).

78 CCDCOE Report, see note 22, 13; Bradbery, see note 18, 1. Another report claims that the Russian Federation refused to intervene with regard to the hacker attacks against Georgia in 2008 (Project Grey Goose, *Russia/Georgia Cyber War – Findings and Analysis*, 17 October 2008, 8, <www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>). It has also been suggested that the May 2007 attacks on Estonia would have not been possible without the blessing of Russian authorities, J. Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired Magazine*, Issue 15.09, 21 August 2007.

79 Shackelford, see note 12, 208.

ted, by the principle of State sovereignty, to decide freely", such as "the choice of a political, economic, social and cultural system, and the formulation of foreign policy."[80] Several of the situations described in the 1981 UN General Assembly Declaration on Non-intervention would perfectly cover cyber attacks.[81] In particular, the Declaration recalls, "[t]he right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, inter alia, on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order" (op. para. I (c)). It is worth noting that not only cyber attacks, but also certain CNE operations could amount to an unlawful intervention, e.g. cyber propaganda through the defacement of websites aimed at fomenting civil strife in the target state or the sending of thousands of e-mails to voters in order to influence the outcome of political elections in another state.[82]

It is more difficult to establish whether cyber attacks also amount to a use of force in international relations. It is common knowledge that Article 2 para. 4 of the UN Charter provides that, "[a]ll Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." This provision, which is widely thought to reflect customary international law and, at least with regard to its core, also *jus cogens*,[83] contains two prohibitions, that of the

---

80 ICJ Reports 1986, see note 64, 107 et seq. (para. 205). The principle of non-intervention has been incorporated in a plethora of agreements, but it is not expressly mentioned in the UN Charter. According to the ICJ, however, the principle is "part and parcel of customary international law" (ibid., 106, para. 202). See, in general, R. Sapienza, *Il principio del non intervento negli affari interni*, 1990.

81 A/RES/36/103 of 9 December 1981.

82 See para. II (j) of the Declaration on Non-Intervention.

83 The customary nature of Article 2 para. 4 has been recognized by the ICJ, ICJ Reports 1986, see note 64, 88 et seq. (paras 187-190). See also Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ Reports 2005, 136 et seq. (171 para. 87). Several authors have argued that the core prohibition contained in Article 2 para. 4, that of aggression, is now a peremptory norm of general international law, R. Ago, "Eighth Report on State Responsibility", in: ILC (ed.), *Yearbook of the In-*

threat and of the use of force. A "threat of force" under Article 2 para. 4 can be defined as an explicit or implicit promise, through statements or actions, of a future and unlawful use of armed force against one or more states, the realization of which depends on the threatener's will.[84] Two situations can be envisaged in the context of the present study. The first is the threat of a use of force with traditional weapons communicated through cyber means. Article 2 para. 4 does not specify the methods through which a threat should be carried out and thus "communicating a threat via the Internet would be on the same theoretical footing as communicating a threat by traditional methods."[85] The cyber threat could also warn of a possible cyber attack by the threatening state. Whether this is a threat under Article 2 para. 4 depends on whether the use of (cyber) force envisaged in the threat is unlawful. Indeed in its 1996 Advisory Opinion on the Legality of the Use of Nuclear Weapons, the ICJ linked the legality of threats to the legality of the use of force in the same circumstances.[86]

The question to answer for both the threat and the use, then, is whether cyber force can be considered a type of "force" in the sense of Article 2 para. 4. The general criteria for the interpretation of treaties are spelt out in article 31 para. 1 of the 1969 Vienna Convention on the Law of Treaties.[87] If one applies the contextual and literal criteria, the results are inconclusive. Indeed, according to the Black's Law Dictionary, "force" means "[p]ower, violence, or pressure directed against a person or thing."[88] The ordinary meaning of "force" is thus broad

---

ternational Law Commission, 1980, Vol. II, Part One, 44; R. Müllerson, "Jus ad bellum: Plus Ça Change (Le Monde) Plus C'Est la Même Chose (Le Droit)?", *Journal of Conflict and Security Law* 7 (2002), 149 et seq. (169); N. Ronzitti, *Diritto internazionale dei conflitti armati*, 2006, 33.

84 M. Roscini, "Threats of Armed Force and Contemporary International Law", *NILR* 54 (2007), 229 et seq. (235).

85 Aldrich, see note 31, 237.

86 Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, 226 et seq. (246 para. 47).

87 It is true that the UN Charter was adopted before the 1969 Vienna Convention on the Law of Treaties and that the Convention does not apply to treaties concluded before its entry into force, but the rules on interpretation contained therein are generally thought to be a codification of customary international law, G. Ress, "The Interpretation of the Charter", in: B. Simma (ed.), *The Charter of the United Nations: A Commentary*, Vol. I, 2002, 18.

88 B.A. Garner (ed.), *Black's Law Dictionary*, 2009, 717.

enough to cover not only traditional armed force but also other types of coercion. As far as the context is concerned, the expression "force" also appears in the Preamble of the Charter and in Arts 41 and 46 where it is preceded by the adjective "armed", while in Article 44 it is clear that the reference is to military force only.[89] This contextual argument has often been used by commentators to maintain that, as elsewhere in the Charter "force" means armed force, this must hold true for Article 2 para. 4 as well, even in the absence of any specification.[90] The opposite argument could, however, also be made: when the drafters wanted to refer to "armed force", they said so expressly and, as this was not done in Article 2 para. 4, they might have wanted to refer to a broader notion of force. A teleological interpretation of Article 2 para. 4 seems to support a narrow reading of the provision that limits it to armed force only: indeed, the overall purpose of the Charter is "to save succeeding generations from the scourge of war",[91] not to ban all forms of coercion. The *travaux préparatoires* also reveal that the drafters did not intend to extend the prohibition to economic coercion and political pressures.[92] A Brazilian amendment prohibiting also "the threat or use of economic measures in any manner inconsistent with the purposes of the UN" was rejected at the San Francisco Conference.[93] Subsequent UN documents, such as the 1970 Declaration on Friendly Relations[94]

---

89 Article 41 of the UN Charter includes the "complete or partial interruption of [...] telegraphic, radio, and other means of communication" in the list of measures "not involving the use of armed force"; this however is not helpful in the qualification of cyber force, as cyber blockades are only one example of cyber force and, in any case, the effects of cyber attacks on computerized societies can be far more drastic than those envisaged by the Charter's drafters in relation to the interruption of communications, H.B. Robertson, Jr., "Self-Defense against Computer Network Attack under International Law", in: Schmitt/ O'Donnell, see note 11, 138; Schmitt, see note 26, 912.

90 A. Randelzhofer, "Article 2 (4)", in: Simma, see note 87, 118.

91 UN Charter, Preamble.

92 According to article 32 of the 1969 Vienna Convention on the Law of Treaties, the preparatory works of a treaty are a supplementary means of interpretation.

93 *Documents of the United Nations Conference on International Organization*, 1945, Vol. VI, 559, 720-721.

94 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV) of 24 October 1970.

and the 1987 Declaration on the Non-Use of Force[95] support the view that Article 2 para. 4 only refers to "armed force", while the principle of non-intervention extends to other forms of coercion.[96]

Even conceding that Article 2 para. 4 only prohibits "armed" force, the question is what "armed" means and if cyber attacks can be considered a use of "armed" force. According to Black's Law Dictionary, "armed" means "[e]quipped with a weapon" or "[i]nvolving the use of a weapon."[97] A weapon is "[a]n instrument used or designed to be used to injure or kill someone."[98] Almost every object can be used as a weapon, if the intention of the holder is hostile. In its Advisory Opinion on the Legality of the Use of Nuclear Weapons, the ICJ made clear that Arts 2 para. 4, 51 and 42 of the UN Charter "do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed."[99] There is then no reason why weapons should necessarily have explosive effects or be created for offensive purposes only. The use of certain dual-use non-kinetic weapons, such as biological or chemical agents, against a country would undoubtedly be treated by the victim state as a use of force under Article 2 para. 4.[100] According to Brownlie, this is so because they are commonly referred to as forms of "warfare" and because they can be used to destroy life and property.[101] Both arguments would suit cyber attacks as well. In particular, the criterion to establish whether a new technology has become a form of warfare is "whether the technique is associated with the armed forces of

---

95 Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, A/RES/42/22 of 18 November 1997.

96 Randelzhofer, see note 90, 118; Schmitt, see note 26, 906-908; M. Benatar, "The Use of Cyber Force: Need for Legal Justification?", *Göttingen Journal of International Law* 1 (2009), 375 et seq. (384-385).

97 Garner, see note 88, 123.

98 Ibid., 1730.

99 ICJ Reports 1996, see note 86, 244 para. 39.

100 The ICJ implicitly recognized that the use of non-kinetic weapons can lead to a violation of Article 2 para. 4 when it qualified the arming and training of the contras by the United States as a threat or use of force against Nicaragua, ICJ Reports 1986, see note 64, 118 para. 228. Military or other hostile use of environmental modification techniques have also been considered a weapon: see the 1976 Convention on the Prohibition of Military or any Hostile Use of Environmental Modification Techniques.

101 I. Brownlie, *International Law and the Use of Force by States*, 1963, 362.

the State that uses it," and not only with, say, intelligence agencies.[102] The fact that several states have included cyber technology in their military doctrines, refer to it as "cyber warfare" and have set up military units with specific cyber expertise supports the view that Trojan horses, worms, viruses and so on are indeed regarded as "just another weapons system, cheaper and faster than a missile, potentially more covert but also less damaging."[103] It is true that the indirect effects of cyber attacks are often more important than the direct effects, but that could well apply to many kinetic attacks as well. For instance, a series of unauthorized military incursions into the territory of another state that produce no material damage but have the indirect effect of destabilizing the country would still amount to a violation of Article 2 para. 4. Similarly, if the Stock Exchange or other financial institutions were to be bombed and the markets disrupted as a consequence, this would certainly be

---

102 Silver, see note 21, 84.

103 J. Lewis, "To Protect the U.S. Against Cyberwar, Best Defense is a Good Offense", *U.S. News and World Report*, 29 April 2010, <www.usnews.com/articles/opinion/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense.html>. Schmitt also notes that "[w]ith the advent of CNA, today the computer is no less a weapon than an F-16 armed with precision weapons", M.N. Schmitt, "Computer Network Attack: The Normative Software", *Yearbook of International Humanitarian Law* 4 (2001), 53 et seq. See, for instance, the partly classified United States 2006 National Military Strategy for Cyberspace Operations, which is "the comprehensive military strategy for the United States Armed Forces to ensure United States superiority in cyberspace", see note 2, 1. The United States Air Force had already argued in 1995 that information is a separate realm for warfare in addition to air, land, sea and space, United States Department of Air Force, *Cornerstones of Information Warfare*, 1995, <www.c4i.org/cornerstones.html>. The 2008 United States National Defense Strategy refers to "terrorism, electronic, cyber and other forms of warfare", United States DoD, *National Defense Strategy*, June 2008, 11 <www.defense.gov/news/2008%20national%20defense%20strategy.pdf>. The new 2010 United States National Security Strategy refers to the need to ensure that "the U.S. military continues to have the necessary capabilities across all domains – land, air, sea, space, and cyber", 2010 United States National Security Strategy, see note 3, 22. It appears that China, North Korea, South Korea, the Russian Federation, Cuba, Japan, Germany, France, Iraq, Israel and Bulgaria have also included cyber attacks into their military doctrines and strategies, Solce, see note 21, 298; D.M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China", *Am. U. Int'l L. Rev.* 17 (2002), 642 et seq. (652).

considered a use of armed force, and not economic coercion, even though the economic consequences of the action would by far outweigh the physical damage to the buildings: one cannot see why the same conclusion should not apply when the Stock Exchange, instead of being bombed, is shut down by a cyber attack.[104]

An interpretation of Article 2 para. 4 that covers cyber force as defined above is also supported by article 31 para. 3 (b) of the Vienna Convention on the Law of Treaties, according to which a treaty has to be interpreted also taking into account "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation." Indeed, several states have expressed the view that cyber force is a type of armed force. The United States Joint Vision 2020 expressly refers to the employ of non-kinetic weapons in the area of information operations.[105] The 2004 National Military Strategy of the United States of America refers to "weapons of mass effect", which "rely more on disruptive impact than destructive kinetic effects" and gives the example of cyber attacks on United States commercial information systems or against transportation networks, which "may have a greater economic or psychological effect than a relatively small

---

104 See W.G. Sharp Sr., *Cyberspace and the Use of Force*, 1999, 90-91. For cyber attacks that do not directly cause physical damage or injury, Schmitt develops seven criteria to distinguish them from other forms of coercion not amounting to the use of force: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility, Schmitt, see note 26, 914-915. These criteria, however, are not without problems. Indeed, certain forms of economic coercion, like an oil embargo, could cause much more severe damage than certain minor uses of armed force, such as cross-border incursions or skirmishes. Furthermore, there are uses of armed force that are not intended to cause any direct physical damage or human losses, for instance, interventions to protect nationals abroad or cross-border operations in "hot pursuit" of criminals. With regard to the immediacy criterion, the so-called logic or time bombs, designed to produce their effects only at a certain time or when certain circumstances occur, can cause damage well after the cyber intrusion has taken place. Finally, the presumptive legitimacy criterion (violence is presumptively illegal, while other forms of coercion, like economic and political, are presumptively legal) does not take into account the fact that many states have now enacted laws against cyber crime, Silver, see note 21, 90.

105 <www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdfJoint Chiefs of Staff>, *Joint Vision 2020 – America's Military: Preparing for Tomorrow,* June 2000, 23.

release of a lethal agent."[106] In his remarks on the new White House cyber security office, President Obama also qualified attacks on defense and military networks as a "weapon of mass disruption."[107] The Russian Federation has been supporting for many years the conclusion of a "disarmament" agreement banning the development, production and use of particularly dangerous information weapons.[108] When submitting its views to the UN Secretary-General, in particular, the Russian Federation declared that "information weapons" can have "devastating consequences comparable to the effect of weapons of mass destruction."[109] Therefore, "the use of Information Warfare against the Russian Federation or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not."[110] The United Kingdom Under-Secretary for security and counter-terrorism also declared that a cyber attack that took out a power station would be an act of war,[111] and the Estonian Defense Minister equated cyber blockades to naval blockades on ports preventing a state's access to the world.[112]

---

106 *The National Military Strategy of the United States of America – A Strategy for Today; a Vision for Tomorrow*, 2004, 1 <www.defense.gov/news/mar2005/d20050318nms.pdf>.

107 "Remarks on securing the nation's cyber infrastructure", see note 1.

108 J. Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia", *The New York Times*, 15 April 2010.

109 P.A. Johnson, "Is It Time for a Treaty on Information Warfare?", in: Schmitt/ O'Donnell, see note 11, 443.

110 Quote from the speech of a senior Russian military officer, reported in: V.M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?", *Naval Law Review* 51 (2005), 132 et seq. (166).

111 J. Doward, "Britain fends off flood of foreign cyber-attacks", *The Observer*, 7 March 2010, 19.

112 NATO Parliamentary Assembly, *NATO and Cyber Defence*, 173 DSCFC 09 E bis, 2009, para. 59 <www.nato-pa.int/default.asp?SHORTCUT=1782>. Blockades are one of the examples of aggression given in A/RES/3314 (XXIX) of 14 December 1974. Commentators have also noted that "[t]he effects of naval blockades and information warfare attacks can be similar. Naval blockades prevent the transport of people and products into the target country or area, and may paralyze an economy. In the past, where intercontinental communication was largely by ship, a blockade would keep out information as well. An information warfare attack may also make transport of people and products impossible, paralyzing an economy, and it too may block the spread of information (especially in an

V. Remedies Against Cyber Attacks

1. Resort to the UN Security Council

Assuming that the victim state is able to identify the origin of the cyber attack and attribute the conduct to a state, several remedies are at its disposal. First, it (or any other UN member)[113] could refer the situation to the Security Council under Article 35 para. 1 of the UN Charter and the Council might recommend the appropriate methods to settle the dispute (Article 36 para. 1). If the Security Council also establishes that the situation amounts to a threat to the peace, breach of peace or act of aggression, it could also exercise its powers under Chapter VII. Whether or not cyber attacks can be considered breaches of peace or acts of aggression,[114] they, and even certain CNE operations, could well potentially amount to a "threat to the peace". Even though, in the drafters' idea, this notion was limited to the international use of conventional armed force,[115] its scope has been progressively expanded and virtually anything can be (and has been) qualified as a threat to the peace by the Security Council.[116] The assessment would obviously depend on the specific circumstances of each case. For instance, as the United States DoD emphasizes, the fact that "a computer network attack […] caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council."[117] Furthermore, "any serious CNA conducted by contenders in long-standing global flash-points (e.g., India-Pakistan, Turkey-Greece) risks ignition. On the other hand, it is possible to envision computer attacks among

---

'infoblockade')", L.T. Greenberg/ S.E. Goodman/ K.J. Soo Hoo, *Information Warfare and International Law*, 1998, 19.

113 A non-member can "bring to the attention of the Security Council or of the General Assembly any dispute to which it is a party if it accepts in advance, for the purposes of the dispute, the obligations of pacific settlement provided in the present Charter", Article 35 para. 2 UN Charter.

114 Certain situations envisaged in A/RES/3314 (XXIX) of 14 December 1974 containing the Definition of Aggression could well cover cyber attacks as well. In any case, the list contained in the Definition is not exhaustive and is not binding on the Security Council.

115 I. Österdahl, *Threat to Peace*, 1998, 85.

116 It is well-known that the drafters of the Charter deliberately left the notion undefined, *United Nations Conference on International Organization, Documents*, Vol. XII, 1945, 505.

117 DoD, *An Assessment*, see note 27, 15.

major Western economic powers (perhaps in the form of economic espionage) that would clearly not threaten the peace if discovered."[118]

If the Security Council does qualify a cyber attack as a threat to the peace, it will be able to adopt recommendations under Article 39, measures to prevent the worsening of the crisis under Article 40 and measures involving or not involving the use of force under Arts 41 and 42. In particular, Article 41 lists, among the measures not involving the use of force, "complete or partial interruption of [...] telegraphic, radio, and other means of communication". The Security Council could thus impose a cyber blockade on the state responsible of the cyber attack in order to prevent its continuation or repetition.[119]

2. Resort to an International Court

The responsible state, if identified, might also be brought before an international tribunal (for instance, the ICJ) in order to obtain reparation for the violation of Article 2 para. 4 and the principle of non intervention. The amount of damage caused by a cyber attack might however be difficult to quantify: financial institutions might for instance be reluctant in providing the exact data and the damage occurred because of business confidentiality.[120] Furthermore, the ICJ, like any other international court, does not have compulsory jurisdiction and therefore both parties must agree to submit the case to adjudication.

Another option would be the request of an Advisory Opinion of the ICJ on the legality of cyber attacks in accordance with Article 96 of the UN Charter. Such opinions are optional and non-binding, although they might decisively contribute to the formation of a customary international law rule.[121]

Some commentators have also suggested that, apart from giving rise to state responsibility, cyber attacks amounting to aggression also entail the international criminal responsibility of the individuals being re-

---

118 Schmitt, see note 26, 928.

119 Schmitt suggests that cyber attacks as a means to enforce Security Council resolutions might be "an 'intermediate step' between Article 41 non-forceful measures and the outright use of force under Article 42", Schmitt, see note 103, 70.

120 CCDCOE Report, see note 22, 17.

121 B. Conforti, *The Law and Practice of the United Nations*, 2005, 276.

sponsible.[122] The 2010 Review Conference of the Statute of the International Criminal Court (ICC) eventually adopted a definition of aggression modeled on that contained in the 1974 General Assembly Resolution 3314 (XXIX) but, in order to be consistent with the principle of legality, without including article 4, which declares the non-exhaustive nature of the list of cases of aggression thereby contained.[123] In 2008, some delegations expressed their concern that this wording of the definition would exclude cyber attacks and supported a previous proposal that also included forms of attack other than the use of armed force affecting the political or economic stability or exercise of the right to self-determination or violating the security, defense or territorial integrity of one or more states.[124] While it is true that some of the cases listed in article 8 *bis* (2) of the ICC Statute could also cover certain cyber attacks by invoking analogy with kinetic attacks,[125] it is doubtful whether such broad interpretative approach would be consistent with article 22 of the Statute, which prohibits extension by analogy.[126] On the other hand, the "leadership clause", that limits liability to persons "in a position ef-

---

122 Weisbord, see note 72, 39; Ophardt, see note 62, para. 75. The individuals accused of the crime of aggression could of course also be brought before a domestic court. Another problem, which is beyond the scope of this article, is whether genocide, war crimes and crimes against humanity (over which the ICC has jurisdiction according to arts 6, 7 and 8 of its Statute) could also be committed through cyber means, D. Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", *Harv. Int'l L. J.* 47 (2006), 179 et seq. (212-213).

123 <www.mediafire.com/?jjnmvmhwnzo>, Resolution RC/Res. 4, of 11 June 2010. The new article 8 *bis* (1) of the ICC Statute defines the "crime of aggression" as "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations". An "act of aggression" is "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations" (article 8 *bis* (2)).

124 Assembly of States Parties to the Rome Statute of the International Criminal Court, Resumed 6th Sess., 2-6 June 2008 (ICC-ASP/6/20/Add. 1), para. 35.

125 The Estonian Defense Minister, for instance, equated cyber attacks to the blockade of a country's ports two hundred years ago, *NATO and Cyber Defense*, see note 112, para. 59.

126 Ophardt, see note 62, para. 64.

fectively to exercise control over or to direct the political or military action of a State", would probably not exclude prosecution of hackers that take over the missile operational system of a state and use it to launch an aggression against another state.[127] The equalizing effect of cyber technologies, thus, could broaden the otherwise limited spectrum of individuals that might commit the crime of aggression.

3. Retortions and Countermeasures

The state victim of a cyber attack could also adopt retortions and non-military countermeasures against the attacker.[128] If the former, being unfriendly acts but not involving any breach of international law, can be adopted at any time, countermeasures consist of conduct inconsistent with a state's international obligations in response to a prior violation of international law by another state. The injured state could adopt them only when the cyber operation is illegal under international law, which is not the case, for instance, of cyber espionage. Cyber attacks as defined above and cyber propaganda with the purpose of causing civil strife in the target state would, however, be both unlawful, as in contrast with the prohibition of the use of force and of intervention in the domestic affairs of another state, respectively, and would entitle the injured state to adopt proportionate countermeasures consistently with the limitations and conditions spelt out in arts 50, 51 and 52 of the ILC Articles on State Responsibility.

Can the state victim of a cyber attack also adopt countermeasures involving the use of force against the attacker? As such measures are considered unlawful in contemporary international law,[129] the answer would be affirmative only if one should conclude that a cyber attack triggers the right to self-defense under Article 51 of the UN Charter or under customary international law. This will be discussed below. It is worth noting that, if cyber force falls within the scope of Article 2 para. 4 and therefore of article 50 para. 1 of the ILC Articles on State Responsibility, a state victim of a cyber attack could not react in kind unless the cyber attack entitles it to invoke Article 51 of the UN Charter. Nevertheless, the situation the ILC had in mind is that of a state us-

---

127 Ibid., para. 47.

128 See article 49 of the ILC Articles on State Responsibility, see note 52.

129 Article 50 para. 1 of the ILC Articles on State Responsibility, see note 52. See also ICJ Reports 1996, see note 86, 246 para. 46.

ing armed force against the previous violation of, for instance, a commercial treaty by the other party. It would indeed seem unreasonable to argue that the state victim of a cyber attack could not retaliate by sending a malicious code unless the cyber attack reaches the threshold of an armed attack. Of course, the expected consequences of the counter cyber attack will have to be proportionate to those of the attack. This might be difficult to achieve because, like biological weapons, malware sent through the cyberspace might spread uncontrollably.[130] Another problem lies in the fact that, in case of a DDoS attack carried out by millions of hijacked computers, the risk of a counter cyber attack for the actual attacker would be negligible, because the counter attack will be directed towards the hijacked computers (which could be located even in the victim state).

4. Use of Armed Force in Self-Defense under Article 51 of the UN Charter

a. When does a Use of Cyber Force amount to an "Armed Attack"?

Article 51 of the UN Charter provides that, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." The state victim of a use of cyber force will thus be entitled to react in self-defense only to the extent that such use of cyber force can be qualified as an "armed attack". In the Nicaragua case, the ICJ acknowledged that a definition of "armed attack" does not exist in the Charter and is not part of treaty law.[131] The ICJ, however, made clear that Article 51 does not refer to specific weapons and that it applies to "any use of force, regardless of the weapons employed."[132] As seen above in the context of Article 2 para. 4,[133] the fact that cyber attacks do not employ traditional kinetic weapons does not necessarily mean they cannot be "armed". As Zemanek notes, "it is neither the designation of a device, nor its normal use, which make it a weapon but the intent with which it is used and its ef-

130 Delibasis, see note 45, 364.
131 ICJ Reports 1986, see note 64, 94 para. 176.
132 ICJ Reports 1996, see note 86, 244 para. 39.
133 Above, Part IV.

fect. The use of any device, or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the conditions of an 'armed' attack."[134] This conclusion is supported by the Security Council's reaffirmation of the right to self-defense in response to the 11 September 2001 attacks on the United States, where the "weapons" employed were hijacked airplanes.[135]

But are all uses of cyber force "armed attacks"? It is well-known that the ICJ identified "the most grave forms of the use of force", i.e. armed attacks, and less grave forms and adopted the "scale and effects" criterion in order to distinguish them.[136] A commentator has tried to specify this criterion by arguing that an armed attack is, "an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (i.e. scale) which have as their consequence (i.e. effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, i.e. its political independence, as well as damage to or deprivation of its physical element namely, its territory", and the "use of force which is aimed at a State's main industrial and economic resource and which results in the substantial impairment of its economy."[137] Dinstein suggests some examples of cyber attacks amounting to armed attacks: "[f]atalities caused by the loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers)" and "the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated."[138] On the other hand, disruption of communications caused by a temporary DoS attack which does not result in sig-

---

134 K. Zemanek, "Armed attack", *Max Planck Encyclopedia of Public International Law*, 2010, para. 21.

135 See S/RES/1368 (2001) of 12 September 2001 and S/RES/1373 (2001) of 28 September 2001.

136 ICJ Reports 1986, see note 64, 101 para. 191, 103 para. 195.

137 A. Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter*, 2000, 63-64.

138 Dinstein, see note 31, 105.

nificant human losses or property damage would not amount to an armed attack, although it might be a use of force.[139]

It is not clear against whose computers and computer networks the cyber attack should be directed in order to be considered an attack on the state. In a traditional attack, the fact that the target is military or civilian does not make any difference. The state where the target is located would be entitled to self-defense because its territorial integrity has been violated. Hence, Dinstein correctly argues that, if a conventional armed attack against a civilian facility on the territory of the target state would amount to an armed attack even if no member of the armed forces is injured or military property damaged, there is no reason to come to a different conclusion with regard to cyber attacks against civilian systems: "[e]ven if the CNA impinges upon a civilian computer system which has no nexus to the military establishment (like a private hospital installation), a devastating impact would vouchsafe the classification of the act as an armed attack."[140] The fact that the computer network is run by a corporation possessing the nationality of a third state or that the computer system operated by the victim state is located outside its borders (for instance, in a military base abroad) does not change the situation.[141] When the damage caused to a certain state or its nationals is however not intended (e.g., because the cyber attack was an accident or the real target was another state),[142] it is doubtful that self-defense can be invoked by the casual victim: according to the ICJ, an armed attack must be carried out "with the specific intention of harming."[143]

---

139 Ibid. The view according to which stealing or compromising sensitive military information could also qualify as an armed attack "even though no immediate loss of life or destruction results" occur (C.C. Joyner/ C. Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", *EJIL* 12 (2001), 825 et seq. (855)) cannot thus be shared.

140 Dinstein, see note 31, 106.

141 Ibid., 106-107.

142 As Schmitt notes, "the attacker, because of automatic routing mechanisms, may not be able to control, or even accurately predict, the cyber pathway to the target", which increases the risk of unintended consequences, Schmitt, see note 103, 56.

143 Case concerning Oil Platforms (Iran v. United States), ICJ Reports 2003, 161 et seq. (191 para. 64). It is not however clear whether the Court wanted to emphasize a general requirement for self-defense or it only intended to limit the requirement to that specific case, C. Gray, *International Law and the Use of Force*, 2008, 146.

Nonetheless, the problem is whether a cyber attack on the computer network of *any* civilian infrastructure could potentially amount to an armed attack (providing it satisfies the scale and effects criterion). It has been claimed, for instance, that, as Google is the most powerful presence on the Internet, an attack on it would be an attack on the United States critical infrastructure.[144] There is no agreement, though, on what "critical infrastructures" are. The UN General Assembly recognized that "each country will determine its own critical information infrastructures."[145] The 1999 DoD's Assessment of International Legal Issues in Information Operations, for instance, refers to a nation's air traffic control system, its banking and financial system and public utilities and dams as examples of targets that, if shut down by a coordinated computer network attack, might entitle the victim state to self-defense.[146] The 2001 PATRIOT Act defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[147] The 2003 United States National Strategy to Secure Cyberspace describes critical infrastructures as "the physical and cyber assets of public and private institutions in [...] agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping."[148] The United Kingdom Cyber Security Strategy refers to nine sectors that deliver essential services: energy, food, water, transport, communications, government and public services, emergency services, health and finance.[149] The Australian government defines critical infrastructures as "those physical facilities, supply chains, information technologies and

---

144 M. Glenny, "In America's new cyber war Google is on the front line", *The Guardian*, 19 January 2010, 32.

145 See, e.g., A/RES/58/199 of 23 December 2003.

146 DoD, *An Assessment*, see note 27, 16.

147 Public Law 107-56, 26 October 2001, Section 1016 (e). The text can be read at <http://fl1.findlaw.com/news.findlaw.com/cnn/docs/terrorism/hr3162.pdf>.

148 United States National Strategy to Secure Cyberspace, see note 3, 1. See also *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, 35 <www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

149 United Kingdom Cyber Security Strategy, see note 59, 9.

communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security", in particular in the following sectors: "banking and finance, communications, emergency services, energy, food chain, health (private), water services, mass gatherings, and transport (aviation, maritime and surface)."[150] Australia's Cyber Security Strategy, however, also points out that systems of national interest "go beyond traditional notions of critical infrastructure" and include "systems which, if rendered unavailable or otherwise compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security."[151] Finally, the Commission of the European Union defines critical infrastructures as "those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments."[152]

The problem of the identification of national critical infrastructures is further complicated by the fact that, in most countries, the majority of such infrastructures are owned by the private sector. At the end of the day, the notion of "critical infrastructure" is linked to that of "national security", which is equally difficult to define, both in domestic and international law.[153] International tribunals recognize a broad mar-

---

150 Australia's Cyber Security Strategy, see note 4, 20.

151 Ibid., 12. The Strategy acknowledges that "[t]he identification of systems of national interest is not a static process and [...] must be informed by an ongoing assessment of risk" (ibid.).

152 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF> EU Commission, *Green Paper on a European Programme on Critical Infrastructure Protection*, COM (2005) 576 final, 17 November 2005, 20. Critical information infrastructures are defined as those information and communication technologies "that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)" (ibid., 19). An indicative list of critical infrastructure sectors includes energy, information and communication technologies, water, food, health, financial, public and legal order and safety, civil administration, transport, chemical and nuclear industry, and space and research (ibid., 24).

153 Th. Christakis, "L'Etat avant le droit? L'exception de 'sécurité nationale' en droit international", *RGDIP* 112 (2008), 5 et seq. (8-16).

gin of appreciation to states when it comes to determine what amounts to a threat to their national security, which "rend, en fin de compte, quelque peu vaine la recherche d'une définition objective et immutable du concept de «sécurité nationale»."[154]

b. The Legal Requirements of the Reaction in Self-Defense against a Cyber Attack

The reaction in self-defense against cyber attacks amounting to armed attacks must meet the requirements of necessity, proportionality and immediacy.[155] Necessity means that the use of force is a means of last resort and that all other available means have failed or are likely to fail. As a minimum, it implies an obligation to identify the author, verify that the cyber attack is not an accident and that the matter cannot be settled by less intrusive means (for instance, by preventing the hackers from accessing the networks and websites under attack through the use of cyber defenses). The major problem with using self-defense to react against a cyber attack is the identification of the aggressor.[156] Aware of this difficulty, certain commentators have suggested that responses in self-defense to a cyber attack against national critical infrastructures should be allowed even without first attributing and characterizing the attack. According to this view, "the law should permit an active response based on the target of the attack, regardless of the attacker's identity."[157] This position, however, cannot be accepted. Apart from being at odds with the law of state responsibility, it is inherently illogical. If it has not yet been established where the attack comes from and to whom it is attributable, against whom and where will the reaction be directed? Furthermore, as seen above, there is no generally accepted definition of "critical infrastructure". Finally, if one accepts "active self-defense" with regard to cyber attacks, why should it not also apply to terrorist attacks by traditional weapons, when no final evidence of state support has been found? Indeed, the United States DoD correctly rejects this view and argues that "the international law of self-defense would not generally justify acts of 'active defense' across international

---

154 Ibid., 15.

155 Y. Dinstein, *War, Aggression and Self-Defence*, 2005, 208-211.

156 See above, Part III.

157 Jensen, see note 53, 234-235. See also M. Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review* 32 (2009), 439 et seq. (453); Condron, see note 53, 415-416.

boundaries unless the provocation could be attributed to an agent of the nation concerned, or until the sanctuary nation has been put on notice and given the opportunity to put a stop to such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile."[158]

As to proportionality, a response in kind might not be possible, either because the victim state does not have the technology to conduct a cyber attack or because the aggressor does not have a sufficiently developed computer network to hit.[159] It is also doubtful whether a series of small-scale cyber attacks can be considered cumulatively when assessing the proportionality of the reaction. The doctrine of the accumulation of events, often invoked by Israel and the United States against terrorist attacks, is controversial.[160] In the Oil Platforms case, the ICJ did not expressly reject it, although the Court found it not applicable in the case before it.[161]

Finally, the requirement of immediacy reflects the fact that the ultimate purpose of self-defense is not punishing the attacker, but rather repelling the armed attack. This requirement must be applied flexibly, especially in the case of cyber attacks. If a state's military computer network has been incapacitated by the cyber attack, it might take some time for it to be able to react in self-defense. Furthermore, if the aggressor uses logic or time bombs, the actual damage could occur well after the cyber attack, which might delay the reaction.

c. Anticipatory Self-Defense against a Conventional Attack Preceded by a Cyber Attack

Even when the use of cyber force does not reach the threshold of an "armed attack", the victim state might still be in a position to invoke anticipatory self-defense against an imminent attack through conventional means that the cyber operation aims to prepare.[162] As mentioned above, for instance, right before the 2008 Russian invasion several Georgian governmental websites had already been the target of brief but debilitating cyber attacks that continued throughout the conflict. The shutting down of crucial websites in particular severed communi-

---

158 DoD, *An Assessment*, see note 27, 21.

159 Greenberg/ Goodman/ Soo Hoo, see note 112, 32.

160 Zemanek, see note 134, para. 7; Dinstein, see note 31, 109.

161 ICJ Reports 2003, see note 143, 191 para. 64.

162 Robertson, Jr., see note 89, 139.

cation from the Georgian government in the initial phase of the conflict.[163] It also appears that the 2007 bombing by Israel of a nuclear facility in Syria was preceded by a cyber attack that neutralized ground radars and anti-aircraft batteries.[164]

In the Nicaragua case, the ICJ did not take position on the problem of anticipatory self-defense, since "the issue of the lawfulness of a response to the imminent threat of armed attack" was not raised.[165] Similarly, in the case concerning Armed Activities on the Territory of the Congo the Court expressed no view, as Uganda eventually claimed that its actions were in response to armed attacks that had already occurred.[166] However, the Court was aware that the security needs that Uganda aimed to protect were "essentially preventative"[167] and held that "Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters."[168]

The crucial question is how imminent the armed attack is, which determines whether the reaction is anticipatory or preventive.[169] It appears that a right to anticipatory self-defense against an imminent

---

163 CCDCOE Report, see note 22, 4-5, 15.

164 M. Glenny, "Cyber armies are gearing up in the cold war of the web", *The Guardian*, 25 June 2009, <www.guardian.co.uk/commentisfree/2009/jun/25/cybercrime-nato-cold-war>.

165 ICJ Reports 1986, see note 64, 103 (para. 194).

166 Armed Activities on the Territory of the Congo (DRC v. Uganda), ICJ Reports 2005, 168 et seq. (222 para. 143).

167 Ibid.

168 Ibid., 223 (para. 148).

169 Although the terminology is controversial, the present author will refer to self-defense against imminent attacks as "anticipatory" and to self-defense against non-imminent attacks as "preventive". The doctrine of preventive self-defense was contained in the 2002 United States National Security Strategy (reaffirmed in 2006), that tried to expand the definition of "imminence" of armed attack to cover cases where "uncertainty remains as to the time and place of the enemy's attack", *The National Security Strategy of the United States of America*, 20 September 2002, <http://www.whitehouse.gov/nsc/nss.pdf>, 15; the 2006 version is available at <http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf>, 23. However, the doctrine of preventive self-defense has no basis in international law, either customary or conventional, A. Cassese, *International Law*, 2005, 361; Gray, see note 143, 213.

armed attack is consistent not only with customary international law,[170] but also with Article 51 of the UN Charter.[171] It is true that, under a literal reading of this provision, the armed attack must "occur", but, according to article 32 of the 1969 Vienna Convention on the Law of Treaties, the application of the article 31 criteria should not lead to an interpretation which is "manifestly absurd or unreasonable". It is unrealistic to expect that states will in all circumstances await an attack before reacting. The rationale of self-defense is to avert an armed attack. If the danger is "instant, overwhelming, leaving no choice of means, and no moment for deliberation",[172] if, in other words, it is necessary to react in that very moment because otherwise it would be too late, the victim state should be entitled to invoke self-defense.[173] According to Schmitt, three factors must be taken into account when establishing the right to respond in (anticipatory) self-defense against a cyber attack that does not amount in itself to an armed attack under Article 51 of the UN Charter: "1) The CNA is part of an overall operation culminating in armed attack; 2) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and 3) The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack."[174] This appears to be a reasonable application of the *Caroline* criteria. The imminence of the attack must be assessed not only against the time factor but also on the basis of the circumstances of each specific case. In the case of cyber attacks, the imminent character "depends on the intensity of the attack, the target of the attack, the reaction time required in order to successfully pre-empt the attack, and the speed with which the damage may move throughout the computer networks."[175] The defensive reaction

---

170 "A More Secure World: Our Shared Responsibility", Report of the High-level Panel on Threats, Challenges and Change, Doc. A/59/565, 63.

171 "In Larger Freedom: Towards Development, Security and Human Rights for All", Report of the Secretary-General, Doc. A/59/2005, 33.

172 Note from Daniel Webster on the *Caroline* incident to Henry S. Fox of 24 April 1841, in: *British and Foreign State Papers* 29 (1857), 1137-1138.

173 Classic examples of imminent attacks are an advancing army or ships on the horizon or a large scale mobilization of troops by an unfriendly neighboring state on its frontiers, W.H. Taft, IV, *The Legal Basis for Preemption*, 18 November 2002, <http://www.cfr.org/publication.php?id=5250>).

174 Schmitt, see note 26, 932-933.

175 Joyner/ Lotrionte, see note 139, 860.

should also be proportionate not to the cyber attack, but rather to the overall attack of which the cyber attack is a preliminary part.[176]

5. Does Customary International Law Permit Self-Defense against a Cyber Attack?

In addition to whether Article 51 of the UN Charter can be interpreted as allowing a reaction in self-defense against a cyber attack, one has also to investigate if any customary international law rule has already developed on the matter. In the Nicaragua case, the ICJ famously acknowledged that there is no complete identity between the customary international law rules on the use of force and the relevant provisions of the UN Charter and that "customary international law continues to exist and to apply, separately from international treaty law, even where the two categories of law have an identical content."[177] About ten years ago, D'Amato predicted that "computer network attack will soon be the subject of an outright prohibition under customary international law."[178] Other commentators, however, have argued that no customary international law has yet developed because the phenomenon is still too recent and there is no state practice yet.[179] This reasoning is, however, flawed. Apart from the fact that cyber attacks are as old as computer networks and are thus not such a recent phenomenon, "the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law."[180] Therefore, "[s]ome customary rules have sprung up quite quickly: for instance, sovereignty over air space, and the regime of the continental shelf, because a substantial and representative quantity of State practice grew up rather rapidly in response to a new situation."[181] With regard to the alleged absence of state practice, it is indeed difficult, if not impossible, to

---

176 Schmitt, see note 26, 933.

177 ICJ Reports 1986, see note 64, 96 para. 179.

178 A. D'Amato, "International Law, Cybernetics, and Cyberspace", in: Schmitt/ O'Donnell, see note 11, 69.

179 Schmitt, see note 26, 921, who concludes that "[a] customary norm may develop over time, but it does not exist at present" as "[n]either practice, nor *opinio juris*, is in evidence"; Shackelford, see note 12, 219.

180 North Sea Continental Shelf, ICJ Reports 1969, 3 et seq. (43 para. 74).

181 Statement of Principles Applicable to the Formation of General Customary International Law, in: International Law Association (ILA), *Report of the Sixty-Ninth Conference*, 2000, 731.

find cyber attacks clearly imputable to states. *Usus* as an element of custom, however, also includes "[v]erbal acts, and not only physical acts, of States", e.g. "[d]iplomatic statements (including protests), policy statements, press releases, official manuals (e.g., on military law), instructions to armed forces, comments by governments on draft treaties, legislation, decisions of national courts and executive authorities, pleadings before international tribunals, statements in international organizations and the resolutions those bodies adopt."[182] In fact, several states have expressed their views with regard to the issue of self-defense in response to a cyber attack. This practice, which also reveals *opinio juris*,[183] should be "extensive and virtually uniform."[184] True, statements and

---

182 Ibid., 725. As Gray states, interpreting state practice means looking at what states say, not necessarily at what they do, Gray, see note 143, 418. According to the ICTY, "[w]hen attempting to ascertain State practice with a view to establishing the existence of a customary rule or a general principle, it is difficult, if not impossible, to pinpoint the actual behaviour of the troops in the field for the purpose of establishing whether they in fact comply with, or disregard, certain standards of behaviour. This examination is rendered extremely difficult by the fact that not only is access to the theatre of military operations normally refused to independent observers (often even to the ICRC) but information on the actual conduct of hostilities is withheld by the parties to the conflict; what is worse, often recourse is had to misinformation with a view to misleading the enemy as well as public opinion and foreign Governments. In appraising the formation of customary rules or general principles one should therefore be aware that, on account of the inherent nature of this subject-matter, reliance must primarily be placed on such elements as official pronouncements of States, military manuals and judicial decisions" (Tadić, see note 66, para. 99). Although the ICTY refers to *jus in bello*, it seems that the same rationale would apply to *jus ad bellum* too.

183 Indeed, "the role of usage in the establishment of rules of international customary law is purely evidentiary: it provides evidence on the one hand of the contents of the rule in question and on the other hand of the *opinio juris* of the States concerned. Not only is it unnecessary that the usage should be prolonged, but there need also be no usage at all in the sense of repeated practice, provided that the *opinio juris* of the States concerned can be clearly established", B. Cheng, "United Nations Resolutions on Outer Space: 'Instant International Customary Law'?", *IJIL* 5 (1965), 23 et seq. (36).

184 The ICJ held that "an indispensable requirement would be that within the period in question, short though it may be, State practice […] should have been both extensive and virtually uniform in the sense of the provision invoked; - and should moreover have occurred in such a way as to show a

declarations on the issue under examination come from a limited number of states, but this is not an insurmountable obstacle to the formation of a custom. As Guzman observes, "[f]or many rules of CIL [customary international law], powerful states dominate the question of state practice. The group may grow still smaller once it is recognized that only states with a stake in the issue must be considered."[185] The ILA Report on the formation of customary international law also points out that the extensive character of state practice is more a qualitative than a quantitative criterion: "if all major interests ('specially affected States') are represented, it is not essential for a majority of States to have participated (still less a great majority, or all of them)."[186] Cassese makes the example of outer space: as only two states had the technology to exploit it, their convergence facilitated the fast creation of a customary international law rule.[187] The same applies to cyber attacks - it is those states that have developed military cyber technologies that one has to mainly look at in order to establish whether a "general practice accepted as law" has evolved in the field.[188]

The United States has repeatedly taken a stance in favor of the right to self-defense against cyber attacks. According to the 1999 DoD's Assessment of International Legal Issues in Information Operations, "[s]tate-sponsored [cyber] attacks may well generate the right of self-defence."[189] The document goes on to say, that "if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack."[190] The 2003 United States National Strategy to Secure Cyberspace states that "an investigation, arrest, and prosecution of the perpetrators, or a diplomatic or *military response* in the case of a state spon-

---

general recognition that a rule of law or legal obligation is involved", ICJ Reports 1969, see note 180, 43 para. 74.

185 A.T. Guzman, "Saving Customary International Law", *Mich. J. Int'l L. 27* (2005-2006), 115 et seq. (151).

186 ILA Report, see note 181, 737.

187 Cassese, see note 169, 158.

188 Article 38 para. 1 lit. b of the ICJ Statute.

189 DoD, *An Assessment*, see note 27, 21.

190 Ibid., 18.

sored action" will follow large cyber incidents.[191] More ambiguously, the 2006 National Security Strategy affirms that the United States is "pursuing a future force that will provide tailored deterrence of both state and non-state threats (including WMD [weapons of mass destruction] employment, terrorist attacks in the physical *and information domains*, and opportunistic aggression) while assuring allies and dissuading potential competitors."[192] In a United States Senate questionnaire in preparation for a hearing on his nomination to head of the new Cyber Command, Lt. Gen. Alexander made clear that, while the right to self-defense "has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with the law of war principles [...] would be lawful."[193] Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counterterrorism, stated that "an attack on American cyberspace is an attack on the United States that should trigger a military response."[194] The Head of the United States Strategic Command said that the White House retains the option to respond with physical force (including nuclear weapons) in case of a disabling cyber attack against United States computer networks.[195] Another Pentagon official recently stated that the United

---

191 United States National Strategy to Secure Cyberspace, see note 3, 28 (emphasis added). This is subsequently reaffirmed in the document: "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner", ibid., 50.

192 2006 United States National Security Strategy, see note 169, 43 (emphasis added).

193 L.C. Baldor, "Military asserts right to return cyber attacks", *Associated Press*, 14 April 2010, <www.google.com/hostednews/ap/article/ALeqM5jATLd9Qzrn-ioGcLQ4oDf99TgscAD9F2T3GO0>. A separate classified document discusses whether the United States should first ask the government from which the cyber attack originates to deal with it.

194 N.C. Cabana, "Cyber Attack Response: The Military in a Support Role", *Chronicles On Line Journal*, 4 April 2000, <www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html>.

195 <http://gsn.nti.org/gsn/nw_20090512_4977.php>, E.M. Grossman, "U.S. General Reserves the Right to Use Force, Even Nuclear, in Response to Cyber Attack", *Global Security Newswire*, 12 May 2009.

States is considering the possibility of using military force in response to a cyber attack.[196]

As to other states, the 2009 United Kingdom Cyber Security Strategy leaves open every option by saying that "[w]e recognize the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against [cyber] attack, and take steps against adversaries where necessary."[197] A senior Russian military officer is reported to have said that "considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces [...] Russia retains the right to use nuclear weapons first against means and forces of information warfare, and then against the aggressor state itself."[198] It also appears that a proposed new law would allow Russian authorities to treat a cyber attack of whatever kind as an act of war if established that it originates from another state.[199]

The practice of relevant international organizations is another form of "state practice" to be considered when assessing the existence of a rule of customary international law.[200] Although recognizing that "[t]he next significant attack on the Alliance may well come down a fibre optic cable",[201] the position of NATO and its Member States on the applicability of the duty of assistance in collective self-defense under article 5 of the North Atlantic Treaty in case of a cyber attack is not clear. In January 2008, NATO adopted a Policy on Cyber Defense that was endorsed by the Heads of State and Government at the Bucharest Summit in April of the same year.[202] Paragraph 47 of the Summit's Final Declaration emphasizes "the need for NATO and nations to protect key information systems in accordance with their respective responsibilities;

---

196 "Pentagon: Military Response to Cyber Attack Possible", 12 May 2010 <www.defensenews.com/story.php?c=AME&i=4623599&s=TOP >.

197 United Kingdom Cyber Security Strategy, see note 59, 14.

198 Quoted in Antolin-Jenkins, see note 110, 166.

199 McAfee Report, see note 5, 30.

200 ILA Report, see note 181, 730.

201 <www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf> *NATO 2020: Assured Security; Dynamic Engagement*, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17 May 2010, 45. NATO's new strategic concept should be adopted in November 2010 in Lisbon.

202 The exact details of the Policy remain classified.

share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack."[203] It appears, however, that NATO responses to cyber attacks were not placed under article 5, but rather under article 4 of the North Atlantic Treaty, that calls upon the Member States to "consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."[204] On 23 April 2010, Estonia concluded a memorandum of understanding (MoU) with NATO to facilitate exchange of information and to create a mechanism of assistance in case of cyber attack.[205] Although the MoU is not for public release, in response to a question from this author an Estonian official from the Ministry of Defense answered that the MoU sets up a framework of support, information exchange and consultations in case of cyber attacks against Estonia and does not consider cyber attacks as armed attacks against NATO.[206] The Organization's position with regard to the applicability of article 5 to cyber attacks is, however, still (perhaps intentionally) ambiguous. If a NATO official is reported to have "completely excluded" any military reaction under article 5 in a case of cyber attack against a Member State, another official did not rule out such option.[207] The 2010 Report of the Group of Experts on the New Strategic Concept for NATO maintains this ambiguity where it refers to "less conventional threats to the Alliance", such as cyber assaults, "which may or may not reach the level of an Article 5 attack."[208] The document further points out that large-scale cyber attacks against NATO's command and control systems or energy grids "could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5"[209] and that "whether an unconventional danger – such as a

---

203 Read the text of the Final Declaration <www.summitbucharest.ro/en/doc_201.html>.

204 R.B. Hughes, "NATO and Global Cyber Defense", in: R. Sheperd (ed.), *The Bucharest Conference Papers*, 2008, 48, <www.chathamhouse.org.uk/files/11276_bucharest08.pdf>).

205 See <www.nato.int/cps/en/natolive/news_62894.htm>. Similar agreements have also been signed with Slovakia, Turkey, the United Kingdom and the United States.

206 E-mail on file with the author.

207 "NATO agrees common approach to cyber defence", 4 April 2008, <www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377>.

208 NATO 2020, see note 201, 9.

209 Ibid., 45.

cyber attack [...] – triggers the collective defence mechanisms of Article 5 [...] will have to be determined by the NAC [North Atlantic Council] based on the nature, source, scope, and other aspects of the particular security challenge."[210] NATO Member States' position is also kept vague. The United Kingdom National Security Strategy (2009 Update), for instance, refers to the fact that "some allies of the UK, to which we have an obligation *under Article V* of the NATO Charter, could be threatened from other states, through military *or other means*."[211] With regard to the 2007 cyber attack on Estonia, a German official is claimed to have stated that, while such attack did not activate article 5 of the North Atlantic Treaty, this could change in the future if the attacks become more sophisticated.[212] The Estonian President and Defense Minister were also said to consider the invocation of article 5.[213]

VI. Concluding Remarks

The current debate on the need for an international treaty prohibiting the use of cyber force among states brings to mind the situation in Constantinople in 1453, where the doctors of faith were debating the issue of whether angels have a gender at the very moment the Ottoman army was at the gates.[214] Indeed, cyber warfare is already a reality and, in the

---

210 Ibid., 20.

211 United Kingdom National Security Strategy, see note 30, 41 (emphasis added). The Strategy points out that security threats "go beyond the traditional domains of land, sea and air, to include weapons of mass destruction, and the increasing importance of cyberspace" (ibid., 7).

212 Quoted in Lewis, see note 24, 3.

213 Shackelford, see note 12, 194; "NATO agrees common approach to cyber defence", see note 207. The fact that Estonia did not eventually invoke article 5 of the North Atlantic Treaty does not necessarily mean that the government of the Baltic state did not believe that collective self-defense could be invoked, but it could rather be an indication that the cyber attack was not regarded as reaching the threshold of an armed attack, as it did not cause physical damage or human losses.

214 The Russian Federation has supported the conclusion of a treaty to regulate the offensive use of cyber technologies by states and to ban attacks on computer networks, but the United States appears to prefer a law enforcement approach and improve cooperation in the context of cyber crime and cyber terrorism, Markoff, see note 108. On why new rules on cyber warfare are needed, see Hollis, see note 13, 1053-1057. See also Johnson, see note 109, 442-453.

current absence of specific *jus ad bellum* rules, we are left with the provisions contained in the UN Charter and in customary international law. These rules seem to be flexible enough to be extended to warfare that did not exist when they were conceived: after all, this already happened in the past with regard to nuclear weapons.

It has been seen that the main question is whether a cyber attack is an action below the threshold of the use of force, or a use of force, or a use of force amounting to an armed attack. This article has concluded that cyber force, unlike CNE operations, can be qualified as a use of "armed" force in the sense of Article 2 para. 4. On the other hand, only large scale cyber attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self-defense under Article 51 of the UN Charter. Self-defense would also be possible against a cyber attack that does not reach the threshold of an armed attack but which prepares an imminent armed attack with conventional weapons (although only if the *Caroline* requirements are met). The absence of frontiers in cyberspace and the possibility for the perpetrators to hide behind botnets or IP spoofing, however, could hamper the identification of the origin of the cyber attack and the application of the law of state responsibility.

This article has also suggested that customary international law could play a role in this area, as there is already some relevant state practice and *opinio juris*, in particular with regard to the right to self-defense against cyber attacks. Although this might lead to the formation of a customary rule in the forthcoming years, the process is on-going and, considering the ambiguity of the positions of certain states and international organizations, it is still difficult to predict its outcome.