Cyber operations as nuclear counterproliferation measures

Marco Roscini

School of Law

Cyber Operations as Nuclear Counterproliferation Measures

Marco Roscini[1]

This is an unproofed version
(final version in 19(1) *Journal of Conflict and Security Law* (2014), pp. 133-157)

Abstract

Focusing on recent malware that allegedly targeted Iran's nuclear programme, this article discusses the legality of inter-state cyber operations as measures to prevent the proliferation of nuclear weapons approaching the topic from the perspective of the law of State responsibility, in particular the circumstances precluding wrongfulness. After examining the role that cyber attacks and cyber exploitation can play in preventing nuclear proliferation, the article explores whether cyber operations can be justified as countermeasures in response to a possible breach by Iran of its non-proliferation obligations. It then discusses whether counterproliferation cyber operations amounting

[1] Reader in International Law, School of Law, University of Westminster. I am grateful to Pierre-Emmanuel Dupont, Dieter Fleck and Daniel Joyner for their helpful comments on previous versions of this article. All errors and omissions remain mine. The author gratefully acknowledges the financial support received from the Leverhulme Trust in order to conduct the research of which this article is one of the outputs. This article is based on developments as of November 2013 and all websites were also last visited on that date.

to a use of force are submitted to a more lenient legal regime than other forms of the use of force in international relations. Finally, the article explores the legality of counterproliferation cyber operations from the perspective of Chapter VII of the UN Charter, and in particular of the resolutions adopted against Iran by the Security Council. The article concludes that the legality of counterproliferation cyber operations must be assessed in the light of the general primary and secondary rules of international law: neither the means used (cyber instead of kinetic) nor the aim pursued (the non-proliferation of nuclear weapons) justify a special legal regime.

Keywords

Cyber operations, nuclear proliferation, Iran, Stuxnet, circumstances precluding wrongfulness, countermeasures.

1. Introduction

In September 2010, it was reported that a computer worm, named Stuxnet, had attacked Iran's industrial infrastructure with the alleged ultimate purpose of sabotaging the gas centrifuges at the Natanz uranium enrichment facility, where the Islamic Republic is suspected of conducting a military nuclear programme that may lead to a violation of its obligations under Article II of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT).[2] Even though an earlier version had already been released as early as

[2] According to Art II of the NPT, '[e]ach non-nuclear-weapon State Party to the Treaty undertakes not to receive the transfer from any transferor whatsoever of nuclear weapons or other nuclear explosive devices

2007,[3] the worm mainly operated in three waves between June 2009 and May 2010. It was also reported that, in December 2012, the worm reappeared and targeted companies in southern Iran.[4] In October 2011, other malware, dubbed DuQu, was discovered: its code had striking similarities with Stuxnet although its payload was not designed to cause physical damage but to obtain information that could be used to attack industrial control systems.[5] Malware, dubbed Flame, was also found in May 2012 to have penetrated the computers of senior Iranian officials with the alleged purpose of stealing sensitive data. Disguised as a routine Microsoft update, Flame collected intelligence from a variety of sources and sent it back to its controllers, but, unlike Stuxnet, did not cause material damage.[6] Although the evidence is at best circumstantial,[7] the

---

or of control over such weapons or explosive devices directly, or indirectly; not to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices; and not to seek or receive any assistance in the manufacture of nuclear weapons or other nuclear explosive devices'. Iran ratified the NPT in 1970. For a comprehensive technical analysis of Stuxnet, see Symantec's N Falliere, L O Murchu and E Chien, 'W32. Stuxnet Dossier', Version 1.4, February 2011 <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Iran claims that its uranium enrichment programme is for purely civilian purposes.

[3] I Barzashka, 'Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme' (2013) 158(2) RUSI Journal 50, 55.

[4] 'US general warns over Iranian cyber-soldiers', BBC News Technology, 18 January 2013, <www.bbc.co.uk/news/technology-21075781>.

[5] Symantec, 'W32. DuQu – The Precursor to the Next Stuxnet', 23 November 2011 <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>.

[6] E Nakashima, G Miller and J Tate, 'U.S., Israel developed Flame computer virus to slow down Iranian nuclear efforts, officials say', The Washington Post, 19 June 2012 <http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware>.

sophistication of Flame and DuQu and, in the case of Stuxnet, also its consequences on the Natanz facility have raised claims that States could be behind the incidents, in particular Israel and the United States: it has been reported that cyber efforts to disrupt the Iranian nuclear programme, code-named 'Operation Olympic Games', started in 2006 during the Bush Administration with Israel's cooperation and were expanded by President Obama.[8]

Using the above cyber operations as a case-study, and assuming that States were indeed responsible for them, this article discusses if and when States can engage in cyber operations against other States in order to prevent the proliferation of nuclear weapons.[9] This article, then, does not deal with remedies *against* cyber operations, but focuses on the use *of* cyber operations against violations of non-proliferation agreements, in particular the NPT. Furthermore, this article does not aim to establish what primary rules were breached by the above cyber operations – a question that will be dealt with only incidentally - but rather approaches the matter from a secondary rules perspective and discusses whether their illegality may be excluded on the basis of the

[7] On the standard of evidence required for attribution of cyber operations, in particular with regard to the exercise of self-defence against such operations, see M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) XXX; N Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 Journal of Conflict and Security Law 235.

[8] DE Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', The New York Times, 1 June 2012 <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0)>.

[9] The present article, then, only focuses on cyber operations conducted by States, and does not deal with cyber crime or cyber terrorism.

relevant circumstances precluding wrongfulness.[10] The article starts by distinguishing between cyber attacks and cyber exploitation and by discussing their respective possible role as counterproliferation measures.[11] It subsequently analyses whether and under what conditions counterproliferation cyber operations can be justified as countermeasures. Section 4 investigates whether counterproliferation cyber operations amounting to a use of force are submitted to a more lenient legal regime than other forms of the use of force in international relations and whether Stuxnet could be qualified as a self-defence measure. Finally, Section 5 examines the legality of counterproliferation cyber operations from the perspective of Chapter VII of the UN Charter, and in particular of the resolutions adopted against Iran by the Security Council.

2. Cyber Attacks, Cyber Exploitation and the Proliferation of Nuclear Weapons

[10] While primary rules provide for substantive rights and obligations, secondary rules determine the consequences of the violation of primary rules. See R Ago, Second Report on State Responsibility - The Origin of International Responsibility, Yearbook of the International Law Commission, 1970, Vol II, 179. This article will not deal with consent, force majeure, distress and necessity as circumstances precluding wrongfulness as they are not relevant in the present context.

[11] 'Counterproliferation' consists of 'efforts either to preclude specific actors from obtaining WMD [weapons of mass destruction]-related material and technologies or to degrade and destroy an actor's existing WMD capability' (DH Joyner, *International Law and the Proliferation of Weapons of Mass Destruction* (OUP 2009) 250).

Cyber operations conducted by States include both cyber attacks and cyber exploitation.[12] Cyber attacks could be standalone operations or be used in conjunction with a subsequent kinetic or cyber attack, and could occur in peacetime as well as in time of armed conflict.[13] A cyber attack may go from relatively innocuous operations such as website defacement to acts that cause havoc in military campaigns by generating misinformation, or acts resulting in major disruption of services and even physical damage to property, loss of lives and bodily injury. In all cases, a cyber attack involves an action, either in offence or in defence, delivered in or through cyberspace, that targets either an information system or an infrastructure control system.[14] The former contains information but do not operate physical infrastructures, hence an attack on them causes loss, alteration or corruption of data but does not directly result in loss of functionality or material damage. The latter, of which a common type is Supervisory Control and Data Acquisition (SCADA) systems, operate infrastructures: if corrupted, the consequence may be malfunction or even physical damage.[15] For security reasons, SCADAs, including that used at Natanz, are normally 'air gapped' from the internet and the attack can only be delivered from within the closed network or through local installation of malware by agents that have close access to the system, for instance through flash drives.

[12] On the taxonomy and classification of cyber operations, see Roscini (n 7) XXX.

[13] Even though a 'cyber attack' might be an 'armed attack' in the sense of Art 51 of the UN Charter or an 'attack' under Art 49(1) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War, care should be taken not to see these expressions as coterminous.

[14] J Ricou Heaton, 'Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces' (2005) 57 Air Force Law Review 161.

[15] Ricou Heaton (n 14) 161.

Cyber exploitation is hereby intended as the unauthorized access to computers, computer systems or networks in order to exfiltrate information, but without affecting the functionality of the accessed system or altering, deleting or corrupting the data or software resident therein.[16] As has been observed, '[t]he primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed – a cyber attack payload is destructive whereas a cyberexploitation payload acquires information nondestructively.'[17] Although they are often labeled in the press as 'cyber attacks', then, cyber exploitation operations are different in that they do not affect the system's operation. They focus on intelligence collection, surveillance and reconnaissance rather than on disruption and can be preliminary to a kinetic or cyber attack that they aim to enable, for instance by collecting information about the architecture of the attacked network (network mapping) or operating system (footprinting) or by identifying previously unknown vulnerabilities.[18] Stealing security

[16] Roscini (n 7) XXX.

[17] HS Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 Journal of National Security Law and Policy 64.

[18] Intelligence is 'any information concerning enemy forces and activities, as well as information necessary to facilitate one's own operations'. Surveillance is 'the systematic observation of areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.' Reconnaissance is 'a single mission undertaken to obtain – by visual observation or other detection methods – specific information about the activities and resources of an enemy' (Harvard Program on Humanitarian Policy and Conflict Research (HPCR), *Manual on International Law Applicable to Air and Missile Warfare* (CUP 2013) 320-321).

data or intellectual property from governments and corporations could also be an aim in itself and is a major threat to national security and commerce.[19]

Both cyber attacks and cyber exploitation could be employed as counterproliferation tools in alternative to, or together with, more traditional means. Cyber attacks, for instance, could be used to incapacitate the air defence networks of the proliferator in support of aerial monitoring of compliance with non-proliferation agreements.[20] Cyber attacks could also be used to enable a subsequent kinetic attack for counterproliferation purposes, as in the case of Israel's bombing of a Syrian nuclear facility in 2007, which was preceded by a cyber attack that neutralized ground radars and anti-aircraft batteries.[21] Finally, States could conduct cyber attacks to directly damage or disrupt the facilities where nuclear weapons are being manufactured or, if the State in question has already acquired nuclear weapons, to attack other national critical infrastructure (NCI) in order to persuade it to disarm. Stuxnet was allegedly designed to

[19] As has been noted, 'the cyber context changes the scale and consequences of theft and espionage to a degree that can result in harm to the country at least as severe as a physical attack.'(J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 EJIL 133). As a consequence of the cyber intrusions allegedly originating from China, the US government adopted a new strategy to combat intellectual property theft (White House, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, February 2013, <www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>, on which see DP Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies', *ASIL Insights*, vol 17, issue 10 (20 March 2013).

[20] JK Kleffner and HA Harrison Dinniss, 'Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations' (2013) 89 International Law Studies 532.

[21] H Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 7.

slow down Iran's nuclear programme by affecting the gas centrifuges at the Natanz uranium enrichment facility. Unlike other malware, the worm did not limit itself to self-replicate, but also contained a 'weaponised' payload designed to give instructions to other programs[22] and is, in fact, the first known use of malicious software designed to produce material damage by attacking the SCADA system of a NCI.[23] Stuxnet presumably infiltrated the Natanz system through laptops and USB drives as, for security reasons, the system is not usually connected to the internet, and had two components: one designed to force a change in the centrifuges' rotor speed, inducing excessive vibrations or distortions that would destroy the centrifuges, and one that recorded the normal operations of the plant and then sent them back to plant operators so to make it look as everything was functioning normally.[24] Although the exact consequences of the incident are still the object of debate, the International Atomic Energy Agency (IAEA) reported that, in the period when Stuxnet was active, Iran stopped feeding uranium into a significant number of gas centrifuges at Natanz.[25] It is

[22] J Richmond, 'Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?' (2011-2012) 35 Fordham International Law Journal 849.

[23] See T Rid, 'Cyber War Will Not Take Place' (2012) 35 Journal of Strategic Studies 17-20.

[24] WJ Broad, J Markoff and DE Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', The New York Times, 15 January 2011 <www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850>.

[25] WJ Broad, 'Report Suggests Problems with Iran's Nuclear Effort', The New York Times, 23 November 2010 <www.nytimes.com/2010/11/24/world/middleeast/24nuke.html>.

still unclear, however, whether this was due to Stuxnet or to technical malfunctions inherent to the equipment used.[26]

Cyber exploitation may also be employed as a counterproliferation tool in at least two ways: to verify compliance with non-proliferation agreements and to enable a counterproliferation kinetic or cyber attack. As to the latter, cyber exploitation could for instance be used for target acquisition, network mapping, footprinting and to identify the defences of the proliferator State. It appears, for instance, that Flame and DuQu were designed to obtain information that could be used to attack industrial control systems. Flame, in particular, collected information about the infected system and network, recording network connections, searching and exporting files, capturing screenshots and key strokes, scanning for locally available Bluetooth devices and even recording environment audio.[27] It is entirely possible that Flame and DuQu worked together with Stuxnet for the same goal: slowing down Iran's nuclear programme.

Cyber exploitation may also be used to collect information about the nuclear programme of the suspected proliferator.[28] The US Foreign Intelligence Surveillance (FISA) Amendments Act of 2008, for instance, allows the FISA Court to authorize 'the targeting of persons reasonably believed to be located outside the United States to

[26] K Ziolkowski, 'Stuxnet – Legal Considerations', NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2012, 5; Barzashka (n 3) 52.

[27] 'FAQ on Flame', International Telecommunication Union Articles, 18 June 2012, <www.itu.int/cybersecurity/Articles/FAQs_on_FLAME.pdf>.

[28] The problem of collecting intelligence with regard to WMD proliferation has been highlighted by MC Waxman 'The Use of Force Against States That *Might* Have Weapons of Mass Destruction' (2009-2010) 31 Michigan Journal of International Law 15-21.

acquire foreign intelligence information',[29] where 'foreign intelligence' includes 'information that relates to […] the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power'.[30] As has been observed, 'software agents can be introduced into a collection target's computer system that can scan all accessible files for certain keywords (e.g., "nuclear" in the appropriate local language) and e-mail those files in encrypted form to an address controlled by U.S. intelligence services'.[31]

While cyber attacks like Stuxnet are, as a minimum, a violation of the sovereignty of the target State and, when accompanied by a coercive intent, also an intervention in its internal affairs,[32] the legality of intelligence gathering is a matter of debate. While it is true, for instance, that espionage is not prohibited *per se* by international law although it is usually criminalised at domestic level,[33] it may be an internationally wrongful act when it entails the unauthorized presence of a foreign organ or agent in the territory of

[29] Section 702, 50 USC § 1881a(a).

[30] 50 USC § 1801(e)(1). See E Lichtblau, 'In Secret, Court Vastly Broadens Powers of N.S.A.', The New York Times, 6 July 2013, <www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?_r=0>.

[31] WA Owens, KW Dam, and HS Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press 2009), 190.

[32] Roscini (n 7) XXX. On Stuxnet as a use of force, see below, Section 4.

[33] Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 International Law Studies 101; RW Aldrich, 'How Do You Know You Are at War in the Information Age?' (1999-2000) 22 Houston Journal of International Law 252; DP Fidler, 'Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think' (2012) 5 International Journal of Critical Infrastructure Protection 28; D Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 688.

another State and, therefore, a violation of its sovereignty.[34] The Group of Experts that drafted the *Tallinn Manual on the International Law Applicable to Cyber Warfare* could not achieve consensus on 'whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty'.[35] One of the experts, however, has suggested that it may be a violation of the sovereignty of the targeted State when the cyber operation entails an unauthorized intrusion into cyber infrastructure located in another State (be it governmental or private).[36] If this conclusion is correct, DuQu and Flame (if attributed to a State) would also be internationally wrongful acts.

---

[34] Q Wright, 'Legal Aspects of the U-2 Incident' (1960) 54 AJIL 844; Fleck (n 33) 707. In *Nicaragua*, the ICJ found that the US reconnaissance flights breached Nicaragua's sovereignty as a result of their trespass into Nicaraguan airspace (*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States),* Judgment, Merits, 27 June 1986, ICJ Reports 1986, para 91). Certain intelligence gathering may also be inconsistent with international human rights law, such as Art 12 of the 1948 UN Universal Declaration of Human Rights and Art 17 of the 1966 UN International Covenant on Civil and Political Rights.

[35] *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 16.

[36] W Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Law Studies 129. More cautiously, an early study of the US Department of Defense concluded that '[a]n unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community. […] If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community' (US Department of Defense, *An Assessment of International Legal Issues in Information Operations*, May 1999, <www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>). On the other

It should be recalled that several nuclear arms control and non-proliferation agreements provide for 'national technical means of verification' of compliance.[37] Indeed, '[i]n the absence of any multilateral capacity to evaluate threats from and calibrate responses to the dangers of weapons of mass destruction and terrorism, international organizations will be forced to rely on intelligence their member states provide'.[38] By ratifying the relevant treaties, the States Parties accept not to interfere with such activities by other Parties.[39] It is difficult, however, to qualify cyber exploitation, and in particular Flame and DuQu, as a lawful national technical means of verification, for two reasons. Firstly, the NPT does not provide for such mechanisms. Secondly, as Article IV(A)(5) of the CTBT makes clear, national means of verification must be used 'in a manner consistent with generally recognized principles of international law, including that of respect for the sovereignty of States'.[40] They therefore essentially include remote sensing, for instance through satellite reconnaissance, but not territorially intrusive activities.[41]

---

hand, Doswald-Beck argues that, when the individual conducts intelligence gathering from outside the adversary's territory through cyber exploitation, 'the situation should be no different from someone gathering data from a spy satellite' (L Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' (2002) 76 International Law Studies 172).

[37] See, eg, Art IV(A)(5) of the Comprehensive Nuclear Test Ban Treaty (CTBT). On national technical means of verification, see S Chesterman 'The Spy Who Came from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law 1090-1093.

[38] Chesterman (n 37) 1129.

[39] See Art IV(A)(6) of the CTBT.

[40] See also, inter alia, Art XII(1) of the 1972 Anti-Ballistic Missile (ABM) Treaty.

[41] M Bothe, 'Verification of Facts', *Max Planck Encyclopedia of Public International Law* (OUP 2012), vol X, 654.

3. Cyber Operations as Countermeasures Against the Proliferation of Nuclear Weapons

Even when inconsistent with certain primary norms, the illegality of the counterproliferation cyber operations might be precluded if they amount to countermeasures aimed to stop the continuation of the wrongful act and to provide reparation (Article 22 of the Articles on the Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission (ILC) in 2001 and endorsed by the UN General Assembly (hereinafter 'ILC Articles')).[42] If acts of retorsion, i.e. unfriendly acts not involving any breach of international law, can be adopted at any time, countermeasures are 'measures that would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation'.[43]

It does not seem that Article 55 of the ILC Articles, according to which the Articles apply only if special rules do not exist, plays a significant role in the present context: the non-compulsory character of the NPT's institutional framework for compliance does not deprive the injured States (if there are any) of their right to adopt

[42] Text in *Yearbook of the International Law Commission*, 2001, vol II, Part Two, 16ff. See also Rule 9, *Tallinn Manual* (n 35) 36.

[43] ILC, Responsibility of States for Internationally Wrongful Acts – General Commentary ('ILC Commentary'), *Yearbook of the International Law Commission*, 2001, vol II, Part Two, 128.

countermeasures under general international law.[44] The invocation of countermeasures as a circumstance precluding wrongfulness, however, is subordinated to the presence of certain requirements that will be examined in the following pages.

A. The Previous Commission of an Internationally Wrongful Act by the Targeted State

To be lawful, countermeasures can only be undertaken by the injured State(s) in reaction to a previous internationally wrongful act attributable to the targeted State.[45] Counterproliferation cyber countermeasures, therefore, presuppose that the conduct of the targeted State amounts to a violation of its non-proliferation obligations under a treaty or customary international law.[46] The development, manufacture or acquisition of nuclear weapons is not prohibited by customary international law. Indeed, the ICJ found that '[t]he emergence, as *lex lata,* of a customary rule specifically prohibiting the use of nuclear weapons as such is hampered by the continuing tensions between the nascent *opinio juris* on the one hand, and the still strong adherence to the practice of deterrence

[44] M Happold, 'The "Injured State" in Case of Breach of a Non-proliferation Treaty and the Legal Consequences of Such Breach', in DH Joyner and M Roscini (eds), *Non-proliferation Law as a Special Regime* (CUP 2012) 192-194; S Singh, 'Non-proliferation Law and Countermeasures', ibid, 223-224.

[45] *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, Judgment, 25 September 1997, ICJ Reports 1997, para 83.

[46] In *Nicaragua*, the ICJ found that 'in international law there are no rules, other than such rules as may be accepted by the State concerned, by treaty or otherwise, whereby the level of armaments of a sovereign State can be limited, and this principle is valid for all States without exception' (*Nicaragua* (n 34) para 269).

on the other'.[47] If this is correct for the use of nuclear weapons, the conclusion must hold even truer for the mere development and possession of such weapons. Indications of the non-customary status of the NPT are North Korea's withdrawal from the treaty, the UN Security Council's demands that it retracts its withdrawal[48] and the non-ratification of India, Pakistan and Israel.

The possession and acquisition of nuclear weapons, however, are prohibited by the NPT (for certain States) and by the treaties establishing nuclear weapon-free zones (NWFZs) in some regions of the world.[49] In the case of Iran (a State Party to the NPT), it has not yet been conclusively established that the Islamic Republic is engaging in activities in breach of Article II of the NPT. In fact, if one interprets the term 'manufacture' not as including any activity that might lead to proliferation but only design and construction of warheads, there is no evidence in support of such conclusion.[50] Iran's past conduct in not fulfilling its obligations under the safeguards agreement with the IAEA may have constituted non-compliance with that agreement:[51]

---

[47] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996, para 73.

[48] SC Res 1874 (2009).

[49] Five treaties establishing NWFZs have been concluded so far: the 1967 Treaty of Tlatelolco with regard to Latin America and the Caribbean, the 1985 Treaty of Rarotonga on the South Pacific Ocean, the 1995 Bangkok Treaty with respect to South-East Asia, the 1996 Pelindaba Treaty in relation to Africa and the 2006 Semipalatinsk Treaty on Central Asia. All five treaties have now entered into force. The text of the treaties can be found at <www.opanal.org>.

[50] Joyner (n 11) 16-17.

[51] INFCIRC/214, 13 December 1974, <www.iaea.org/Publications/Documents/Infcircs/Others/infcirc214.pdf>. Para 5 of SC Res 1929 (2010) also '*calls upon* Iran to act strictly in accordance with the provisions of the Additional Protocol to its

this non-compliance, however, is limited to the safeguards agreement and does not automatically constitute a breach of Article III of the NPT, which merely requires States Parties to *enter* into a safeguards agreement with the IAEA.[52] On the other hand, it is not controversial that Iran has breached Security Council resolutions requiring it to suspend all uranium enrichment-related activities.[53] Whether the Security Council can deprive a State of an 'inalienable' right like that to the peaceful uses of nuclear energy is a complicated issue that is outside the scope of this article.[54]

B. The State 'Injured' by the Wrongful Act

Assuming, for the sake of argument, that Iran did (or will) commit an internationally wrongful act by breaching its nuclear non-proliferation obligations, it is only the 'injured States' that are entitled to claim the full spectrum of the consequences of State

---

IAEA Safeguards Agreement that it signed on 18 December 2003'. As Iran has not ratified the Protocol, its binding effects on the Islamic Republic rest on Art 25 of the UN Charter. On 11 November 2013, Iran signed a Joint Statement on Framework for Cooperation with the IAEA (<www.iaea.org/newscenter/pressreleases/2013/prn201321.html>). See also the measures of cooperation agreed in the Joint Plan of Action signed by the P5+1 and Iran on 24 November 2013 (text at <www.theguardian.com/world/interactive/2013/nov/24/iran-nuclear-deal-joint-plan-action?CMP=twt_gu>).

[52] DH Joyner, *Interpreting the Nuclear Non-Proliferation Treaty* (OUP 2011) 88-89.

[53] See, in particular, SC Res 1696 (2006) and 1737 (2006).

[54] The Joint Plan of Action signed by the P5+1 and Iran on 24 November 2013 (above (n 51)) recognizes Iran's right to enrich uranium, which raises the question whether such agreement is in breach of SC Res 1696 (2006) and 1737 (2006) and, if so, with what consequences.

responsibility, including the right to adopt countermeasures. According to Article 42 of the ILC Articles,

> [a] State is entitled as an injured State to invoke the responsibility of another State if the obligation breached is owed to:
>
> (*a*) that State individually; or
>
> (*b*) a group of States including that State, or the international community as a whole, and the breach of the obligation:
>
> (i) specially affects that State; or
>
> (ii) is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.

NPT obligations are obviously of a collective character. As there is no 'specially affected State' in case of their breach, States Parties would be injured only if NPT obligations qualify as 'integral' (or 'interdependent') obligations according to Article 42(b)(ii) of the ILC Articles. Integral obligations operate 'in an all-or-nothing fashion':[55] even though they pursue a collective interest of the group, 'each parties' performance is effectively conditioned upon and requires the performance of the

[55] J Crawford, Fourth Report on State Responsibility, Yearbook of the International Law Commission, 2001, Vol II, Part One, 10.

other'.[56] As Sir Gerald Fitzmaurice put it, 'the obligation of each party to disarm, or not to exceed a certain level of armaments, or not to manufacture or possess certain types of weapons, is necessarily dependent on a corresponding performance of the same thing by all the other parties, since it is the essence of such a treaty that the undertaking of each party is given in return for a similar undertaking by the others'.[57]

Due to the peculiar asymmetric character of the NPT regime, which distinguishes between nuclear weapon States and non-nuclear weapon States, it may however be difficult to argue that its non-proliferation obligations are integral under the law of State responsibility. Indeed, if one interprets Article 42(b)(ii) as referring only to 'a modification which affects the future performance of the *specific* obligations in question' by *all* the other Parties,[58] it can be doubted that the obligations not to manufacture or otherwise acquire nuclear weapons under Article II of the NPT are of an integral character: as has been suggested, their breach by a State Party 'would not undermine or modify the position of *all other States* to which the obligation is owed, with respect to the *future performance of that same specific obligation*', because such obligations do not apply to the nuclear weapon States Parties to the NPT.[59] Note the

[56] Report of the International Law Commission on the work of its fifty-third session, Yearbook of the International Law Commission, 2001, Vol II, Part Two, 119. The Commission included disarmament and nuclear free zone treaties among the examples of this type of obligations.

[57] G Fitzmaurice, Second Report on the Law of Treaties, Yearbook of the International Law Commission, 1957, Vol II, 54.

[58] G Gaja, 'The Concept of an Injured State' in J Crawford, A Pellet and S Olleson (eds) *The Law of International Responsibility* (OUP 2010) 946 (emphasis added).

[59] S Singh, 'Iran, the Nuclear Issue and Countermeasures', 4 <www.dipublico.com.ar/english/iran-the-nuclear-issue-countermeasures/> (emphasis in the original, underlining and bold omitted). Of course,

difference with Article 60(2)(c) of the 1969 Vienna Convention on the Law of Treaties. Under this provision, States may suspend in whole or in part the operation of a treaty with respect to themselves in case of a material breach by a State Party 'if the treaty is of such a character that a material breach of its provisions by one party radically changes the position of every party with respect to the further performance of its obligations under the treaty'. This provision refers to a modification 'which affects the *totality* of obligations deriving from the treaty',[60] not only the performance of the same specific obligation as in Article 42(b)(ii) of the ILC Articles, and would therefore apply to material breaches of the NPT. Under Article 60, however, a State could only suspend the same treaty in reaction to a material breach of its provisions, and not commit other violations of international law, such as unlawful cyber operations.

If one accepts the interpretation according to which it is only the obligation to *conclude* a safeguards agreement with the IAEA, and not also that to comply with it, which has been collectivized through Article III of the NPT, the obligation to fully apply safeguards is of a bilateral character. In such case, the only party injured by its violation would be the IAEA, with which the agreement was concluded. As has been observed, 'just as for States, whether an organization is an injured subject depends on the participation of the organization in a primary legal relationship', which is certainly the case 'where the breached obligation results from a bilateral treaty to which the

---

when it is obligations contained in other non-proliferation treaties that are allegedly breached, the conclusion may be different. For instance, the main provisions contained in NWFZ treaties are of an integral character (M Roscini, 'Something Old, Something New: The 2006 Semipalatinsk Treaty on a Nuclear Weapon-Free Zone in Central Asia' (2008) 7 Chinese Journal of International Law 611).

[60] Gaja (n 58) 946 (emphasis added).

organization is a party'.[61] But even if non-compliance with IAEA safeguards was considered also a breach of Article III(1), this would still not entitle the NPT States Parties to adopt countermeasures as injured States, for the same reasons explained above with regard to Article II, ie because its breach would not affect the position of *all* other Parties with respect to the performance of the *same* obligation.[62]

Finally, the violation of the Security Council resolutions requiring Iran to stop all uranium enrichment activities translates into a breach of Article 25 of the UN Charter, according to which '[t]he Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter'. Strictly speaking, this is a breach of a provision contained in a treaty establishing an international organization which, in the present case, indirectly imposes an obligation, that of suspending uranium enrichment, related to non-proliferation. It is doubtful that UN Member States may adopt unilateral countermeasures against a State that is the object of mandatory sanctions decided by the Security Council. But even be that as it may, the NPT States Parties would still not be entitled to adopt countermeasures in reaction to the violation of the Security Council resolutions on Iran under the law of State responsibility. Indeed, Article 25 of the UN Charter is an *erga omnes partes* obligation owed to all other UN Member States:[63] for this type of obligations, Article 42(b)(i) of the ILC Articles prescribes that, although all Member States have a legal interest in the fulfilment of the obligation, only those 'specially affected' by the breach

[61] Eglantine Cujo, 'Invocation of Responsibility by International Organizations', in Crawford, Pellet and Olleson (n 58) 970-971.

[62] See, for an alternative view, Happold (n 44) 184-185.

[63] See *Prosecutor v Blaskić*, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, ICTY, Appeals Chamber, 28 October 1997, para 26.

are injured States and are thus entitled to adopt countermeasures under Article 49.[64] In the present case, there are no States 'specially affected' by the breach of Article 25 of the UN Charter as a consequence of the continuation of the Iranian uranium enrichment programme.

If the NPT States Parties were not 'injured' by Iran's conduct, then, it should be demonstrated that they can otherwise invoke the responsibility of the author of the breach, including the right to adopt countermeasures. Article 54 of the ILC Articles notoriously leaves the problem unresolved and provides that, in case of obligations of a collective character, any States 'other than the injured States', to which the collective obligation is owed, can take 'lawful measures' against the wrongdoing State 'to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached', but without specifying whether 'lawful measures' include countermeasures.[65] Assuming *arguendo* that this is the case, and if compliance with IAEA safeguards agreements is indeed a bilateral obligation, Article 54 would not apply, as, by referring to Article 48(1) of the ILC Articles, this provision only becomes relevant in case of collective obligations.[66] If, however, one considers the obligation to comply with IAEA safeguards agreements collectivized through Article III of the NPT, the IAEA would be the international organization in the interest of which to

[64] This conclusion would not change should one consider Art 25 as an *erga omnes* obligation due to the universal character of the UN Charter and its membership.

[65] The ILC Commentary explains that Art 54 'reserves the position and leaves the resolution of the matter to the further development of international law' (ILC Commentary (n 43) 139).

[66] Art 48 (1) of the ILC Articles applies when '(*a*) the obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or (*b*) the obligation breached is owed to the international community as a whole'.

adopt 'lawful measures', but arguably a precondition should be that non-compliance with the safeguards agreement has been established by the Agency, something which has not occurred with regard to Iran. As to breaches of Article II of the NPT, Article 54 is difficult to apply as there would be no injured States in the interest of which other affected States could adopt countermeasures and it is difficult to see who the 'beneficiaries' of the breached obligation could be. Finally, at least in case of breaches of Security Council resolutions, there is a strong argument in favour of suspending the right of non-injured States to take unilateral countermeasures when the Security Council has imposed mandatory sanctions against the wrongdoer. As Sicilianos explains, 'the triggering of Chapter VII ends the power of States not individually injured to react as they please at the individual level'.[67] 'Collective countermeasures', i.e. measures adopted by non-injured States in response to violations of *erga omnes* obligations, can exclusively be adopted if the Security Council fails to act. If that is not the case, non-injured States can only adopt those measures 'which are necessary and sufficient for the execution of those mandatory sanctions'.[68]

In light of the above, it is not possible to conclude that the United States (assuming that it was responsible for Stuxnet, Flame and DuQu) was 'injured' by Iran's

[67] L-A Sicilianos, 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community' in Crawford, Pellet and Olleson (n 58) 1142. See also the comments by A Pellet on the Fourth Report of the Special Rapporteur on State Responsibility, *Yearbook of the International Law Commission*, 1992, Vol I, 144; and P-E Dupont, 'Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran' (2012) 17 Journal of Conflict and Security Law 333. *Contra*, see NJ Calamita, 'Sanctions, Countermeasures, and the Iranian Nuclear Issue' (2009) 42 Vanderbilt Journal of Transnational Law 1438-1440.

[68] Sicilianos (n 67) 1142.

non-compliance with IAEA safeguards or Security Council resolutions, or that it was entitled to adopt countermeasures, including cyber operations, under Article 54. The result would not change in case of violation of Articles II or III(1) of the NPT by Iran. These conclusions apply even more strongly to Israel, which is not even a State Party to the NPT.

C. Conditions Related to the Adoption of Countermeasures

States adopting countermeasures also have to comply with the requirements provided in Part Three, Chapter II of the ILC Articles that reflect customary international law. In particular, the injured State must first call upon the responsible State to discontinue the internationally wrongful act or provide reparation[69] and, apart from the case of 'urgent countermeasures',[70] must notify it of the decision to take countermeasures and offer to negotiate.[71] This did not occur with regard to Stuxnet, DuQu and Flame. An obligation to notify cyber countermeasures, however, is probably unrealistic, as it deprives the operations of one of their main advantages, ie their anonymity and covert character. Also, if the injured State notifies its intention to adopt cyber countermeasures, the wrongdoing State may immunize itself by reinforcing its active and passive cyber defences. Having said that, '[t]he injured State need not specify the content or timing of

[69] Art 52(1)(a) of the ILC Articles on State Responsibility.

[70] Art 52(2) of the ILC Articles on State Responsibility.

[71] Art 52(1)(b) of the ILC Articles on State Responsibility.

the measures'.[72] Article 52(1)(b) of the ILC Articles, therefore, still leaves some room for covert countermeasures, including cyber ones.

The purpose of the countermeasure must be to ensure compliance with international law and the measure must be 'as far as possible' reversible, i.e. 'taken in such a way as to permit the resumption of performance of the obligations in question'.[73] Indeed, as the ILC Commentary explains, 'inflicting irreparable damage on the responsible State could amount to punishment or a sanction for non-compliance, not a countermeasure as conceived in the [ILC] Articles'.[74] Therefore, 'if the injured State has a choice between a number of lawful and effective countermeasures, it should select one which permits the resumption of the performance of the obligation suspended as a result of countermeasures'.[75] From this perspective, a Distributed Denial of Service (DDoS) campaign, which would only overload the targeted system with multiple requests, may be preferable, all being equal, to a cyber attack, like Stuxnet, that employs malware to modify, corrupt or alter data or software and that may spread to other systems.[76] DDoS attacks, however, are unlikely to be an option against nuclear facilities, which, like most NCIs, are usually not connected to the internet. In any case, 'the duty to choose

[72] Y Iwasawa and N Iwatsuki, 'Procedural Conditions', in Crawford, Olleson and Pellet (n 58) 1152.

[73] Art 49(3) of the ILC Articles on State Responsibility.

[74] ILC Commentary (n 43) 131.

[75] ILC Commentary (n 43) 131.

[76] '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. On botnets, see L Vihul, C Czosseck, K Ziolkowski, L Aasmann, IA Ivanov, and S Brüggemann, *Legal Implications of Countering Botnets*, CCDCOE, 2012

measures that are reversible is not absolute. It may not be possible in all cases to reverse all of the effects of countermeasures after the occasion for taking them has ceased'.[77]

Cyber countermeasures must be necessary to ensure the cessation of the wrongful act if it is continuing, its non-repetition or full reparation in its various forms.[78] A corollary of this is that countermeasures 'must be directed against' the State responsible for the internationally wrongful act.[79] In the case of cyber countermeasures, therefore, the malware must able to be directed with sufficient accuracy against the wrongdoing State.[80] Otherwise, the State acting in countermeasure may become itself the object of countermeasures if it breaches the rights of innocent States. Finally, the countermeasure must be proportionate, ie 'commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question'.[81] Although the ILC Commentary states that '[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or

[77] ILC Commentary (n 43) 131.

[78] Iwasawa and Iwatsuki (n 72) 1153.

[79] *Gabčíkovo-Nagymaros Project* (n 45) para 83.

[80] This does not mean that third States' rights cannot be incidentally affected (ILC Commentary (n 43) 130).

[81] Art 51 of the ILC Articles on State Responsibility. See also *Gabčíkovo-Nagymaros Project* (n 45), para 85. The UK Foreign Secretary, for instance, included the 'need for governments to act proportionately in cyberspace and in accordance with national and international law' in his seven principles for the international use of cyberspace (W Hague, Speech at the Munich Security Conference: Security and Freedom in the Cyber Age—Seeking the Rules of the Road, 11 February 2011, cited in DJ Ryan, M Dion, E Tikk, and JJCH Ryan, 'International Cyberlaw: A Normative Approach' (2011) 42 Georgetown Journal of International Law 1172).

a closely related obligation',[82] they do not necessarily have to be in kind. This is particularly important in the case of nuclear non-proliferation obligations, where the collective interest is to prevent the general collapse of the regime as a consequence of reciprocal violations. The 'rights in question' referred to in Article 51 of the ILC Articles are not only those of the injured and responsible States:[83] the possible spreading of the malware to third States, or the consequences on such States of disrupting the internet connection of the target State, should also be taken into account when assessing the proportionality of the cyber countermeasure.[84] Proportionality, however, may be difficult to calculate in advance in the cyber context because of the interconnectivity of information systems, which causes that malware sent through cyberspace might spread uncontrollably. As the ILC Commentary acknowledges, however, 'what is proportionate is not a matter which can be determined precisely'.[85] All in all, meeting the proportionality criterion is essentially a technical issue: customized cyber countermeasures are possible if the software is written with this purpose in mind. The code could, for instance, be designed in a way as to be activated only by the presence of certain characteristics. This requires a high degree of information on the targeted systems, which can be obtained through traditional intelligence collection and/or cyber

[82] ILC Commentary (n 43) 129.

[83] The Commentary states that 'the position of other States which may be affected [by the countermeasure] may also be taken into consideration' (ILC Commentary (n 43) 135).

[84] As the Commentary explains, however, '[i]n a situation where a third State is owed an international obligation by the State taking countermeasures and that obligation is breached by the countermeasure, the wrongfulness of the measure is not precluded as against the third State' (ILC Commentary (n 43) 130).

[85] ILC Commentary (n 43) 135.

exploitation.[86] Stuxnet is a good example of such customized cyber operations. Unlike most malware, Stuxnet did little harm to computers and networks that did not meet specific configuration requirements. While the worm was promiscuous, it made itself inert if the specific Siemens software used at Iran's Natanz enrichment plant was not found on infected computers, and contained safeguards to prevent each infected computer from spreading the worm to more than three others. The worm was also programmed to erase itself on 24 June 2012.[87]

Another limit to the adoption of countermeasures is Article 50(1) of the ILC Articles, which reflects customary international law and provides that countermeasures cannot affect 'the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations'.[88] This point will be explored in the next Section.

4. Counterproliferation Cyber Operations Amounting to a Use of Force

It is outside the scope of this study to engage in an in-depth discussion of when cyber operations amount to a use of force under Article 2(4) of the UN Charter, as this has

[86] Owens, Dam, and Lin (n 31) 123.

[87] Richmond (n 22) 856.

[88] Other obligations that cannot be affected by countermeasures are obligations for the protection of fundamental human rights, obligations of a humanitarian character prohibiting reprisals, obligations arising from peremptory norms of general international law, obligations under any dispute settlement procedure applicable between it and the responsible state and obligations related to the inviolability of diplomatic or consular agents, premises, archives and documents (Art 50 of the ILC Articles on State Responsibility).

been extensively done elsewhere.[89] In two articles published in a special issue on 'cyber war' of this Journal, Russell Buchan and Nicholas Tsagourias speak for numerous scholars when they argue that, if a cyber operation causes physical damage to property or persons, it would qualify as a use of force.[90] If it was proved that Stuxnet did cause physical damage to the gas centrifuges at Natanz and significantly disrupted the functioning of the facility, then, it could hardly be doubted that it qualified as a use of force under Article 2(4), although arguably not of a scale and effects to also be an 'armed attack' under Article 51.[91]

Having said that, one may wonder whether the cyber (instead of kinetic) character of the operation and its alleged purpose (nuclear counterproliferation) justify a more lenient legal regime than other forms of the use of force in international relations. In this regard, an analogy can be made with the threat of force as a policy instrument. In her 1988 article, Romana Sadurska argues that, although Article 2(4) of the UN Charter prohibits both, 'the threat of force is in actuality treated as a lesser international wrong, even if its consequences are comparable to the lasting effects of the use of force'.[92] She

[89] See, eg, Roscini (n 7) XXX.

[90] R Buchan, 'Cyber Attacks: Unlawful Use of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 219, 221; Tsagourias, (n 7) 231. See also *Tallinn Manual* (n 35) 48.

[91] ME O'Connell, 'Cyber Security without Cyber War' (2012) 17 Journal of Conflict and Security Law 201-202. On the scale and effects threshold of 'armed attack', see *Nicaragua* (n 34) paras 191, 195. On whether cyber operations disrupting the provision of services without causing physical damage also amount to a use of force, see Roscini (n 7) XXX. Cyber exploitation operations like Flame and DuQu can never qualify as a use of force, as they do not cause physical damage to property or persons or disruption of infrastructures (ibid, XXX).

[92] R Sadurska, 'Threats of Force' (1998) 82 AJIL 258.

opines that 'there is no reason to assume that the threat will always be unlawful if in the same circumstances the resort to force would be illicit'.[93] Taking State practice into account, in particular the lack of significant reactions to threats of force, she concludes that Article 2(4) is not the only parameter against which the legality of a threat of force is assessed by States, which consider threats lawful if: 1) they are made to protect the security of the State, providing that the internal self-determination of the target is not violated; 2) they are made to vindicate a denied right; 3) they are prudent and balance individual and community values.[94] If the main purpose of the Charter is the preservation of peace and security and not the freedom of States from external pressure and if '[t]he Charter prohibits the use of force in violation of the political independence and territorial integrity of a state *because* it may lead to international instability, breach of the peace and/or massive abuses of human rights', then there is no reason why the threat and the use of force should be treated equally.[95] The legal appraisal of the threat would be the same as that of the use of force only when they produce comparable results, which is not a likely case, as 'even an effective threat will not have the same destructive consequences as the use of force'.[96]

Many of Sadurska's arguments in relation to threats of force could be easily extended to cyber attacks when used to enforce international law, in particular non-proliferation obligations, because of their potentially less lethal character: even when they cause some material damage as in the case of Stuxnet, cyber attacks can cause

[93] Ibid, 250.

[94] Ibid, 260-266.

[95] Ibid, 250.

[96] Ibid.

fewer human casualties (if any) than a kinetic attack. It has been claimed, for instance, that the Stuxnet operation was a 'huge success' because it was 'nearly as effective as a military strike, but even better since there were no fatalities and no full-blown war'.[97] Cyber operations might then come to be seen as a more subtle approach to pursue community objectives such as nuclear weapons counterproliferation and a 'greater opportunity to achieve goals such as retarding the Iranian nuclear programme without causing the loss of life or injury to innocent civilians that air strikes would seem more likely to inflict'.[98]

This argument seems to find support in the fact that, even though Stuxnet has allegedly damaged a considerable number of centrifuges in the Natanz uranium enrichment plant, there was no significant reaction to it, by the victim State, by those suspected of having planned and executed the operation or by the international community in general. One commentator has maintained that this silence can be interpreted as acquiescence suggesting that 'states don't perceive this situation triggered the rules on the use of force, armed attack, and aggression' even though, had the attack been carried out by kinetic means, it would have probably been treated differently.[99] According to this view, 'states, particularly the big cyber-powers, are seeking to establish higher use-of-force and armed-attack thresholds for cyber-based actions to

[97] Y Katz, 'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years', Jerusalem Post, 15 December 2010, <www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years>.

[98] JP Farwell and R Rohozinski, 'Stuxnet and the Future of Cyber War' (2011) 53 Survival: Global Politics and Strategy 34.

[99] DP Fidler, 'Was Stuxnet an Act of War?' (2011) 9(4) IEEE Security & Privacy 74.

permit more room to explore and exploit cybertechnologies as instruments of foreign policy and national security'.[100]

De lege ferenda, it might well be that the law will develop in the sense of allowing cyber operations as a 'ritualized substitute for violence'[101] that States employ to restore a minimum legal order, especially when resort to the right of self-defence would be dubious. This conclusion, however, is still a speculative one and not consistent with the *lex lata*. At a closer look, the analogy with the threat of force is not helpful. Sadurska's view was disproved by the 1996 *Nuclear Weapons* Advisory Opinion: as the International Court of Justice (ICJ) held, '[t]he notions of "threat" and "use" of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal - for whatever reason - the threat to use such force will likewise be illegal. In short, if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter'.[102] There is also ample practice that proves that States consider the threat of force prohibited under the same circumstances as the use of force, even if they do not cause direct physical damage.[103]

It is also not correct that Stuxnet met with no reaction. Iran, in particular, qualified the cyber attack as 'nuclear terrorism' and as 'a grave violation of the principles of the UN Charter and international law', even though it refrained from using explicit *jus ad*

[100] Ibid, 74-75.

[101] Sadurska (n 92) 246.

[102] *Legality of the Threat or Use of Nuclear Weapons* (n 47) para 47.

[103] M Roscini, 'Threats of Armed Force and Contemporary International Law' (2007) 54 NILR 243-251.

bellum language.[104] It also encouraged the Security Council 'to act against those States undertaking cyber attacks and sabotage in the peaceful nuclear facilities'.[105] But even be that as it may, from a purely methodological perspective silence cannot be interpreted as acquiescence in the present case as no State openly acknowledged the responsibility of Stuxnet or offered legal justifications for it. It is more likely that the lack of significant reactions by the international community was due to non-legal factors. In particular, many regional States were certainly not unhappy that Iran's nuclear programme had been delayed. Silence might have also been due to the lack of reliable information about the incident and its actual consequences, as well as its uncertain attribution. States might have also preferred not to condemn the cyber operation as a 'use of force' because they are engaging or wish to engage in similar operations themselves. Finally, the absence of significant reactions could have been motivated by the fact that the attention of the international community was at the time focused on other events, in particular the 'Arab Spring'.

If Stuxnet did cause some physical damage and was therefore a use of force, it would fall under Article 50(1) of the ILC Articles and could not be justified as a lawful countermeasure, even if adopted for counterproliferation purposes. Article 21 of the ILC Articles, however, provides that '[t]he wrongfulness of an act of a State is precluded if

[104] Iranian Foreign Minister's address to the UN Security Council, 28 September 2012, <http://iran-un.org/en/2012/09/28/28-september-2012-2/>.

[105] Ibid. More explicit *jus ad bellum* language, including references to Article 2(4) of the UN Charter, has been used by members of Iran's mission to the United Nations (A Miryousefi and H Gharibi, 'View from Iran: World needs rules on cyberattacks', The Christian Science Monitor, 14 February 2013, <www.csmonitor.com/Commentary/Opinion/2013/0214/View-from-Iran-World-needs-rules-on-cyberattacks-video>).

the act constitutes a lawful measure of self-defence taken in conformity with the Charter of the United Nations'. Article 51 of the UN Charter constitutes an exception to the prohibition of the use of force contained in Article 2(4) and provides that the State victim of an armed attack or any other State in collective self-defence of the victim could use force against the attacker if the armed attack 'occurs'.[106] Any attempt to justify Stuxnet as a self-defence measure would run against the fact that, regardless of whether or not Iran has breached its non-proliferation obligations under the NPT or IAEA safeguards agreements, the acquisition and manufacture of nuclear weapons clearly do not amount, per se, to an 'armed attack' in the sense of Article 51. Only if Iran does acquire those weapons and actually uses them against another State, or – to use the *Caroline* incident's language - at least is about to do so and there is 'no choice of means, and no moment for deliberation',[107] can the right of self-defence be exercised by using force. The claim that self-defence can be invoked against an imminent *threat* of an armed attack, where the imminence is referred to the threat of an armed attack and not to the attack itself,[108] has no basis in international law.

5. Counterproliferation Cyber Operations and the UN Collective Security System

[106] See *Tallinn Manual* (n 35) 54.

[107] Letter from Daniel Webster to Henry S Fox (24 April 1841), 29 British and Foreign State Papers 1137-1138.

[108] H Koh, 'International Law in Cyberspace', Speech at the USCYBERCOM Inter-Agency Legal Conference, 18 September 2012, in CD Guymon (ed), *Digest of United States Practice in International Law*, 2012, 595, <www.state.gov/documents/organization/211955.pdf>.

According to Article 59 of the ILC Articles, the Articles are 'without prejudice to the Charter of the United Nations'. Article 103 of the Charter provides that '[i]n the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail'. Regardless of whether one prefers to consider Article 103 as a hierarchy rule and a circumstance precluding wrongfulness,[109] or as a mere conflict clause,[110] in both cases the illegality of Stuxnet, DuQu and Flame would be precluded, at least *vis-à-vis* other UN Member States to which the breached obligation is owed, if the operations had been authorized by the UN

[109] M Milanović, 'Norm Conflict in International Law: Whither Human Rights?' (2009-2010) 20 Duke Journal of Comparative and International Law 76-77 ('Article 103 is not a simple rule of priority - it also precludes or removes any wrongfulness due to the breach of the conflicting norm. In other words, a state cannot be called to account for complying with its obligations under the Charter, even if in doing so it must violate some other rule - any rule, that is, except a rule of *jus cogens*'); V Gowlland-Debbas, 'The Limits of Unilateral Enforcement of Community Objectives in the Framework of UN Peace Maintenance' (2000) 11 EJIL 365, 368; D Bowett, 'The Impact of Security Council Decisions on Dispute Settlement Procedures' (1994) 5 EJIL 89. Preclusion of responsibility on the basis of Art 103, at least between UN Member States, could also be explained as a situation of consent, which is an uncontroversial circumstance precluding wrongfulness (Art 20 of the ILC Articles; see A Tzanakopoulos, 'Collective Security and Human Rights' in E De Wet and J Vidmar (eds) *Hierarchy in International Law. The Place of Human Rights* (OUP 2012) 65).

[110] Tzanakopoulos (n 109) 63-66. This Author maintains that the inclusion in the ILC Articles of self-defence as a circumstance precluding wrongfulness despite this being already contained in Art 51 of the UN Charter demonstrates that Art 103 was not deemed to be sufficient to preclude the wrongfulness of State conduct (ibid, 65).

Security Council.[111] It is true that, according to the letter of Article 103, the Charter's obligations prevail only over 'international agreements', and not also customary international law norms, like the duty to respect another State's territorial sovereignty and the principle of non-intervention. As suggested in the Report of the ILC's Study Group on the Fragmentation of International Law, however, 'the practice of the Security Council has continuously been grounded on an understanding that Security Council resolutions override conflicting customary law. […] Therefore it seems sound to join the prevailing opinion that Article 103 should be read extensively - so as to affirm that charter obligations prevail also over United Nations Member States' customary law obligations'.[112]

---

[111] Art 103 only refers to '*obligations* of the Members of the United Nations under the present Charter' (emphasis added), and would thus seem to apply only to binding resolutions, i.e. decisions, of the Security Council, not mere authorizations. As has been observed, however, '[b]ecause authorizations by the Council to member states have effectively taken over the role of armed forces under UN command, as was originally envisaged in the Charter, and thus have a central place in the system of collective security, Article 103 has generally been interpreted to extend to Council authorizations as well as to its commands' (Milanović (n 109) 78). See also Gowlland-Debbas (n 109) 371; R Kolb, 'Does Article 103 of the Charter of the United Nations Apply only to Decisions or also to Authorizations Adopted by the Security Council?' (2004) 64 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 31-35. The point was also made by the UK House of Lords in the 2007 *Al-Jedda* Judgment (*R (Al-Jedda) v Secretary of State for Defence* [2007] UKHL 58, 12 December 2007, para 33 (Lord Bingham)).

[112] 'Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law', Report of the Study Group of the International Law Commission, A/CN.4/L.682, 13 April 2006, 176. See also M Zwanenburg, 'Existentialism in Iraq: Security Council Resolution 1483 and the Law of Occupation' (2004) 86 International Review of the Red Cross 761; B Fassbender, 'The United Nations Charter as Constitution of the International Community' (1998) 36 Columbia Journal of

It is well-known that, according to Article 24(1) of the UN Charter, the Security Council is the organ that has the primary responsibility for the maintenance of international peace and security. To this aim, the Charter confers broad powers upon the organ, in particular those provided in Chapter VII, that can be exercised whenever the Council determines the existence of a threat to the peace, a breach of the peace or an act of aggression.[113] Unlike the case of countermeasures and self-defence, a cyber operation under Chapter VII does not require that Iran has breached international law, as long as the Security Council has qualified the situation as a threat to the peace.[114] In such case, the Security Council could make recommendations under Article 39, adopt measures aimed at preventing the worsening of the crisis under Article 40 and, more importantly, adopt coercive measures under Articles 41 and 42. As to the former, Member States may be required to prohibit the provision to the targeted State of computer hardware and software that could be employed in the military nuclear activities of the proliferator. The non-exhaustive list of measures that the Council can recommend or decide under Article 41 also includes 'complete or partial interruption of . . . telegraphic, radio, and other means of communication': the Security Council could thus adopt targeted cyber sanctions or limit the access to the internet of the State responsible for nuclear

---

Transnational Law 586. *Contra*, see G Arangio-Ruiz, 'Article 39 of the ILC First-Reading Draft Articles on State Responsibility' (2000) 83 Rivista di diritto internazionale 752; K Zemanek, 'The Legal Foundations of the International System' (1997) 266 Recueil des cours 232; R Liivoja, 'The Scope of the Supremacy Clause of the United Nations Charter' (2008) 57 ICLQ 602-608; Tzanakopoulos (n 109) 66.

[113] Art 39 of the UN Charter.

[114] It is well-known that the Charter's drafters deliberately left the notion of 'threat to the peace' undefined (United Nations Conference on International Organization, Documents, Vol XII, 1945, 505).

proliferation.[115] Member States may be authorized or required to conduct monitoring activities or to hamper the internet access of the proliferator and to ensure that webpages are denied access from the domain name of the targeted State.[116] Security Council sanctions will have to be implemented at the domestic level through the adoption of legislation requiring national Internet Service Providers (ISPs) to adopt restrictive measures against the targeted State.

It is worth recalling that a Joint Declaration on Freedom of Expression and the Internet by the rapporteurs on freedom of expression of the United Nations, the Organization of American States and the African Commission on Human and Peoples' Rights and the Organization for Security and Cooperation in Europe's representative on freedom of the media provides that '[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds'.[117] The Declaration, however, is essentially addressed to governments and it may be argued that, if the cyber sanctions are decided by the Security Council, they would not be for

[115] B Brockman-Hawe, 'Using Internet "Borders" to Coerce or Punish: The DPRK as an Example of the Potential Utility of Internet Sanctions' (2007) 25 Boston University International Law Journal 187ff.

[116] An example of this scenario, although not against a State responsible for nuclear proliferation, is the unilateral sanctions imposed by the United States on Cuba, which also affect access to the internet and use of social networks (UN Doc A/67/167, 23 July 2012, 10–11).

[117] Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet (2011), para 6 (b), <www.osce.org/fom/78309>.

public order or 'national' security grounds, but to enforce an interest of the international community. In such case, 'restriction of certain content may be appropriate if authorized by the mandate, proportionate under international standards and necessary to protect a recognized interest'.[118]

'Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate',[119] it could authorize cyber attacks amounting to a use of force in order to react against nuclear proliferation qualified as a threat to the peace.[120] It is true that Article 42 only refers to enforcement action 'by air, sea, or land forces': a literal reading of the provision might lead to conclude that enforcement in cyberspace is precluded to the Council. The purpose of Article 42, however, was to extend the collective security machinery to all military domains available at the time the Charter was drafted.[121] An evolutive interpretation of the norm would then include any other military domain that becomes accessible through technological developments, such as outer space and cyberspace.

It is difficult, however, to invoke Chapter VII of the UN Charter in the case of the cyber operations against Iran. It is true that, on 4 February 2006, the IAEA Board of

[118] Kleffner and Harrison Dinniss (n 20) 532.

[119] Art 42 of the UN Charter.

[120] The proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, has been famously qualified as a threat to international peace and security in SC Res 1540 (2004). More recently, see SC Res. 2094 (2013) in relation to North Korea's nuclear tests.

[121] N Melzer, 'Cyber Warfare and International Law', UNIDIR, 2011, 19, <www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=134218>.

Governors referred the Iranian case to the Security Council[122] and that there are several resolutions that have set up a sanctions regime against Iran and Iranian individuals 'to constrain Iran's development of sensitive technologies in support of its nuclear and missile programmes',[123] but none of them expressly refers to cyber sanctions:[124] as has been argued, '[b]ecause the resolutions leave the power to expand the scope of the sanctions in the hands of the [Security] Council and the [Sanctions] Committee, states are not legally able to rely upon those resolutions and the Charter (particularly Articles 25 and 103) to shield themselves from any legal consequences which additional measures may have'.[125] If Stuxnet is qualified as a use of force as seems preferable, in particular, resolutions adopted by the Security Council under Article 41 would not be a proper legal basis and there is still no resolution authorizing UN Member States to use 'all necessary means' (i.e. including the use of kinetic or cyber force) to push Iran to comply with its obligations. In fact, in the debates at the Security Council several States have reaffirmed that the resolutions adopted so far do not permit the use of force.[126]

[122] Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran, IAEA Doc GOV/2006/14, 14 February 2006.

[123] Preamble of SC Res 1737 (2006), 1747 (2007), 1803 (2008), 1929 (2010).

[124] SC Resolution 1737 (2006), adopted under Art 41, requires Member States to block the import or export of sensitive nuclear materials and equipment and to freeze the financial assets of persons or entities supporting its proliferation sensitive nuclear activities or the development of nuclear-weapon delivery systems. The sanctions regime provided in Resolution 1737 has been integrated and extended in subsequent resolutions (SC Resolutions 1747 (2007), 1803 (2008), 1835 (2008), 1929 (2010)).

[125] Calamita (n 67) 1406.

[126] See the statements by the Russian Federation (UN Doc S/PV.5500, 31 July 2006, 5; S/PV.5612, 23 December 2006, 2; S/PV5647, 24 March 2007, 11; S/PV.5848, 3 March 2008, 21), Tanzania (S/PV.5500,

6. Conclusions

Recent cyber operations that allegedly targeted the Iranian nuclear programme epitomize the possible use of cyber measures for nuclear counterproliferation purposes. The legality of such operations must be assessed in the light of the general primary and secondary rules of international law: neither the means used (cyber instead of kinetic) nor the aim pursued (the non-proliferation of nuclear weapons) justify a special legal regime. While it may be uncertain that Flame and DuQu, that aimed at gathering intelligence and did not cause physical damage or disruption of services, were internationally wrongful act, the unlawful character of Stuxnet can hardly be questioned. The worm breached several primary rules of international law and could not be justified as a countermeasure: NPT States Parties (and, even less, non-Parties) were not 'injured' by Iran's non-compliance with IAEA safeguards agreements or relevant Security Council resolutions nor would they be injured if Iran breached Article II of the NPT, and it does not seem that they are entitled to adopt countermeasures under Article 54 of the ILC Articles. Furthermore, countermeasures cannot amount to a violation of the prohibition of the threat and use of force. If Stuxnet qualified as a use of force because of its physically destructive consequences, then, it would be lawful only if used in self-defence against an armed attack by Iran, but neither the acquisition nor the development of nuclear weapons (and even less uranium enrichment) constitute an armed attack in the sense of Article 51 of the UN Charter and customary international

31 July 2006, 6), Argentina (S/PV.5612, 23 December 2006, 8), Nigeria (S/PV.6335, 9 June 2010, 13) and Mexico (ibid, 14).

law. Finally, Chapter VII of the UN Charter cannot be invoked to justify the operation: none of the resolutions sanctioning Iran that have been adopted by the Security Council make any reference to cyber operations or authorize Member States to use 'all necessary means' to ensure compliance with the NPT and IAEA safeguards agreements.

Apart from any considerations on its legality, it seems that, all in all, Stuxnet was of limited use as counterproliferation measure, as it neither caused a significant shutdown of enrichment processes nor had a permanent impact on the centrifuges.[127] On the other hand, the operation might have hampered the negotiations for a diplomatic solution of the crisis that were under way at the time the worm was discovered.[128] In the long-term, Iran might have even taken advantage of the incident in order to improve its active and passive cyber defences and repel further cyber attacks on its critical infrastructures.[129]

[127] Barzashka (n 3) 52-54, who however concedes that Stuxnet 'might have temporarily slowed down Iran's *rate* of expansion' of its enrichment programme (ibid, 54; emphasis in the original).

[128] Ibid.

[129] 'US general warns over Iranian cyber-soldiers' (n 4).