CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Stuxnet – Legal Considerations

Dr. iur. Katharina Ziolkowski, LL.M. (UNSW)

Tallinn 2012

Disclaimer

This publication is a draft product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre) and it represents the views and interpretations of the Centre. It is produced for the purpose of providing a background of the incident to the NATO community in terms of applicable international law. This publication does not represent the opinions or policies of NATO and is designed to provide an independent position.

Third-party sources are quoted as appropriate and the Centre is not responsible for the content of the external sources referenced in this publication. The Centre assumes no responsibility for any loss or harm arising from the use of information contained in this publication. Copies of this publication may be distributed for non-profit and non-commercial purpose only.

Contact

NATO Cooperative Cyber Defence Centre of Excellence
Filtri tee 12, Tallinn 10132, Estonia
publications@ccdcoe.org
www.ccdcoe.org

Table of Contents

Introduction 3
Legal Considerations According to Public International Law 6
Use of Force Short of Armed Attack 7
Pre-Emptive Self-Defence 12
Countermeasure Short of Use of Force 15
Armed Conflict 17
Territorial Sovereignty 19
Customary International Environmental Law 20
Economic Coercion 21
Principle of Non-Intervention in Internal Affairs 22
Conclusion 25

Introduction

Stuxnet, a malicious form of software also known as *W32.Stuxnet worm*[1], was first reported on 17 June 2010 under the name *Rootkit.TmpHider*.[2] Subsequently, information on and samples of the malicious code were released to individual IT security companies which undertook immense endeavours to monitor the data traffic between the worm and its command-and-control servers, as well as to understand the design, functionality and aim of this highly sophisticated computer program.[3]

Stuxnet targeted the computer systems of five facilities (according to recorded WAN IP addresses / computer domain names) located in Iran, between June 2009 and May 2010.[4] By February 2010 the IT security company *Symantec* had gathered 3.280 unique samples representing three different variants of *Stuxnet*.[5] The worm affected specific industrial control systems which use a type of software for management of large-scale industrial systems (Supervisory Control and Data Acquisition (SCADA) systems) developed by the company *Siemens* and showing specific configuration requirements.[6] The spread of *Stuxnet* beyond the initially targeted computer systems is likely to be considered an unintentional side-effect.[7] According to *Stuxnet´*s architecture, the worm was created to amend the code of Programmable Logic Controllers (PLCs) of industrial control systems in order to amend the plant's operations by manipulating frequency converter control systems and thus slowing

---

[1] *See* Symantec, W32.Stuxnet *available at* http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99 (last visited 5 November 2011).

[2] O. Kupreev, S. Ulasen, Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review, VirusBlokAda Publication *available at* http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf (last visited 5 November 2011); N. Falliere, L.O. Murchu & E. Chien, W32.Stuxnet Dossier (Symantec Publication, Version 1.4, February 2011), at p. 4 *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (last visited 25 June 2011).

[3] *See* information at http://www.langner.com/en/ and Falliere / Murchu / Chien, *supra* note 2, at p. 5.

[4] Falliere / Murchu / Chien, *supra* note 2, at pp. 7-11.

[5] *Ibid*, at p. 7.

[6] *Ibid*, at pp. 2, 4-6.

[7] *Ibid*, at p. 7.

down or speeding up a motor, as well as hiding such changes from the operator of the respective equipment.[8] Although the names of the five targeted Iranian facilities were not officially disclosed, a myriad of media reports soon identified nuclear infrastructures in Iran as the targets of *Stuxnet*, namely the uranium enrichment plant at *Natanz* and/or the nuclear power plant at *Bushehr*, suspecting that the speed of the IR-1 centrifuges´ rotors was being amended in order to negatively affect Iran´s nuclear programme.[9]

Legally assessing the implications of the creation, installation and control of the *Stuxnet* worm is especially challenging because of the lack of detailed and reliable information relating to its origin and the physical effects it caused outside the targeted SCADA systems.

The media reported that *Stuxnet* was the first "cyber-weapon"[10] used and were speculating that intelligence operatives from certain States[11] might have been the creators of the

[8] *Ibid*, at pp. 39-43 and 1-2.

[9] *See* e.g. R. McMillan, Was Stuxnet Build to Attack Iran´s Nuclear Program?, in: *pcworld* online of 21 September 2010 *available at* http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html (last visited 8 November 2011); Stuxnet may turn Busher into a new Chernobyl, in: *Homeland Security News Wire* online of 1 February 2011 *available at* http://www.homelandsecuritynewswire.com/stuxnet-may-turn-bushehr-new-chernobyl (last visited 8 November 2011); D. Albright, P. Brannan & Ch. Walrond, Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, ISIS Report of 15 February 2011 *available at* http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf (last visited 8 November 2011).

[10] *See* e.g. E. Nakashima, Stuxnet malware is blueprint for computer attacks on U.S., in: *The Washington Post* online of 2 October 2010 *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/10/01/AR2010100106981.html (last visited 21 June 2011); The Stuxnet outbreak. A worm in the centrifuge. An unusually sophisticated cyber-weapon is mysterious but important, in: *The Economist* online of 30 September 2010 *available at* http://www.economist.com/node/17147818 (last visited 5 November 2011); A. Klimburg, H. Tirmaa-Klaar, Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action Within the EU, Study of 15 April 2011 conducted for the European Parliament, Directorate-General for External Policies, Policy Department, executive summary, at p. 7.

[11] *See* e.g. US and Israel were behind Stuxnet claims researcher, in: *BBC News* online of 4 March 2011 *available at* http://www.bbc.co.uk/news/technology-12633240 (last visited 21 June 2011); Th. Erdbrink, E. Nakashima, Iran struggling to contain 'foreign-made' computer worm, in: *The Washington Post* online of 28 September 2010 *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706606.html (last visited 21 June 2011); S. Kamali Dehghan, Iran accuses Siemens of helping launch Stuxnet cyber-attack - Senior official says German engineering giant supplied US and Israel with details of control system used by Tehran, in: *The Guardian* online of 17 April 2011 *available at* http://www.guardian.co.uk/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (last visited 21 June 2011); J. Warrick, Iran's Natanz nuclear facility

malware. Although a *cui bono* analysis can perfectly well point in the direction of entities that might have an interest in affecting Iran´s nuclear programme, it does not provide sufficient indices in legal terms to attribute the malicious cyber-activity to an individual, to a group of individuals or even to a State.

Further impeding the legal analysis, it remains unclear whether *Stuxnet* did indeed cause damage of a physical nature outside the targeted SCADA systems. Despite respective assertions by media reports[12] and scientific analyses[13] based on information available in media, it is not known whether *Stuxnet* did affect the physical integrity of IR-1 centrifuges or other components in Iran´s uranium enrichment plant at *Natanz*, the nuclear power plant at *Bushehr* or in other nuclear facilities. Iranian officials did not confirm any actual damage of a physical nature which had been caused by *Stuxnet*.[14] Reports of the replacement[15] of a remarkable number of centrifuges in the nuclear enrichment facility at *Natanz* do not provide evidence, in legal terms, of physical damage indirectly caused by *Stuxnet* either, as it was equally reported that Iran has faced numerous technical problems in recent years because of the poor quality of equipment used, especially in regard to an old centrifuge model which has been troubled by breakdowns for years.[16]

---

recovered quickly from Stuxnet cyberattack, in: *The Washington Post* online of 16 February 2011 *available at* http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html (last visited 21 June 2011).

[12] See e.g. Warrick, *supra* note 11; Y. Katz, Stuxnet may have destroyed 1,000 centrifuges at Natanz, in: *The Jerusalem Post* online of 24 December 2010 *available at* http://www.jpost.com/Defense/Article.aspx?id=200843 (last visited 8 November 2011).

[13] *See* e.g. Albright / Brannan / Walrond, *supra* note 9, at p. 3.

[14] A denial of any physical damage by Iranian officials was reported by: Reuters, After Stuxnet: Iran says it's discovered 2nd cyber attack, in: *The Jerusalem Post* online *available at* http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795 (last visited 8 November 2011).

[15] *See* Albright / Brannan / Walrond, *supra* note 9, at p. 3; Katz, *supra* note 12.

[16] See D.E. Sanger, W.J. Broad, Iran Has New Equipment to Speed the Production of Nuclear Fuel, Panel Is Told, in: *The New York Times* online of 2 September 2011 *available at* http://www.nytimes.com/2011/09/03/us/03nuke.html (last visited 8 November 2011), („[T]he IR-1s were so notoriously unreliable that they broke down even when they were not the target of cyberattacks."); G. Thielmann, P. Crail, Chief obstacle to Iran's nuclear effort: its own bad technology, in: *The Christian Science Montior* online of 8 December 2010 *available at* http://www.csmonitor.com/Commentary/Opinion/2010/1208/Chief-obstacle-to-Iran-s-nuclear-effort-its-own-bad-technology (last visited 8 November 2011); Iranian Nuclear Program Plagued by Technical Difficulties, in: *Global Security Newswire* online of 23 November 2010 *available at*

Therefore, the legal analysis of the creation, installation, control and effects of *Stuxnet* can only be based on assumptions, and can only touch upon its *potential* national or international law implications.

Legal Considerations According to Public International Law

If non-state actors did create, install and control *Stuxnet*, according to private[17] international law, different domestic laws could apply. This could involve (1) the laws of the States of where the actors were citizens, (2) the laws of the States on whose sovereign territory *Stuxnet* was created, installed or controlled[18] from, and (3) the national laws of Iran, the State on whose territory *Stuxnet* revealed its alleged effects. First of all, the criminal[19] and civil law liability of the individuals involved would depend on whether the respective national laws penalize or otherwise prohibit actions such as the unauthorized and intentional access to a computer system, alteration of computer data, or hindering of the functioning of a computer system, or prohibit, for instance, the partial damaging of or interference with the operations of critical infrastructure systems (even if located on the territory of another State). Of course, the personal liability of a non-state actor would be further conditioned by a sound legal examination of the facts in each individual case.

If one or more States were to be held responsible[20] for the creation, installation and control of the *Stuxnet* worm, the following aspects of public international law could be of relevance:

---

http://www.globalsecuritynewswire.org/gsn/nw_20101123_2990.php (last visited 5 November 2011); F. Dahl, S. Westall, Technical woes halt some Iran nuclear machines: diplomats, in: *reuters.com* (US edition) of 23 November 2010 *available at* http://www.reuters.com/article/2010/11/23/us-nuclear-iran-problems-idUSTRE6AM1L520101123 (last visited 5 November 2011).

[17] Private international law decides which law to apply when a case shows linkage to domestic laws of different States.

[18] It was reported that Stuxnet command and control servers were located in Denmark and Malaysia, *see* Falliere / Murchu / Chien, *supra* note 2, at p. 21.

[19] *See* Articles 2-6 of the *Convention on Cybercrime* of 23 November 2001 *available at* http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm (last visited 21 June 2011).

[20] In regard to the attribution of individual conduct to a State *see*: Articles 4-11 of the ILC-*Draft Articles on Responsibility of States for Internationally Wrongful Acts* of 2001, UN GA Res. 56/83 of 12 December 2001, Annex *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/477/97/PDF/N0147797.pdf?OpenElement (last visited 21 June 2011), and the commentary ILC-*Draft Articles on Responsibility of States for Internationally Wrongful*

Use of Force Short of Armed Attack

As indicated by media contributions[21], it is worth considering whether the installation and the alleged effects of the *Stuxnet* worm could be deemed "use of force" according to Article 2(4) of the *Charter of the United Nations* (hereafter referred to as the UN Charter).

According to the prevailing opinion within scholarly writing, the prohibition of threat or use of force, as endorsed in the UN Charter, is also reckoned as a peremptory[22] norm of international customary law.[23] However, this finding can refer only to the core meaning of the prohibition, as there is little agreement within the international community as to the interpretation[24] of the term "force".[25] Indeed, "force" can include a variety of actions,

---

Acts, with commentaries of 2001 *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (last visited 22 June 2011).

[21] *See* e.g. A. Sternstein, Experts Recommend an International Code of Conduct for Cyberwar, in: *National Journal* online of 10 June 2011 *available at* http://www.nationaljournal.com/nationalsecurity/experts-recommend-an-international-code-of-conduct-for-cyberwar-20110610 (last visited 24 June 2011); C. Walsh, US Prepares for Cyber Threats in the Wake of Suspected "Stuxnet" Attack in Iran, in: *Harvard National Security Journal* online of 7 October 2010 *available at* http://harvardnsj.com/2010/10/us-prepares-for-cyber-threats-in-the-wake-of-suspected-%E2%80%9Cstuxnet%E2%80%9D-attack-in-iran/ (last visited 24 June 2011).

[22] *See* Article 53 of the *Vienna Convention on the Law of Treaties* of 1969: "[…] a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."

[23] A. Randelzhofer, Art. 2(4), in: B. Simma (ed.), The Charter of the United Nations. A Commentary (Oxford University Press, Oxford et al., Vol. I., 2nd ed. 2002), at para. 61 *et seq.*; K. Doehring, Collective Security, in: R. Wolfrum / Ch. Philipp (ed.), United Nations: Law, Policies and Practice (Vol. I., Munich 1995), p. 110 *et seq*., at para. 9; A. Randelzhofer, Use of Force, in: R. Bernhardt (ed.), Encyclopedia of Public International Law, (Vol. IV, 2000), p. 1246 *et seq.*, at p. 1255; I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 98-101 para. 187-190. It shall be only mentioned that some scholars, given the violent State practice since 1945, doubt the authority of the prohibition of threat or use of force, *see* M.J. Glennon, Why the Security Council Failed, in: Vol. 82 No. 3 *Foreign Affairs* 2003, p. 16-35, at p. 22 *et seq.*; Th. M. Franck, What Happens Now? The United Nations after Iraq, in: Vol. 97 *American Journal of International Law* 2003, p. 607-620, at p. 610; Th. M. Franck, When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?, in: Vol. 4 *Singapore Journal of International and Comparative Law* 2000, p. 362-376, at p. 362; W. M. Reisman, Assessing Claims to Revise the Law of War, in: Vol. 97 *American Journal of International Law* 2003, p. 82-90, at p. 83.

[24] *See* Article 31(1) and (4) of the *Vienna Convention on the Law of Treaties* of 1969. Despite being a highly political document, the UN Charter is subject to the rules of interpretation of international treaties. Although, according to its Article 4, the Convention does not apply retroactively (to the UN Charter of 1945), the provisions on interpretation of treaties are a valuable reference as they reflect

including measures of political and economic coercion, as asserted[26] by socialist and developing countries in the past. All in all, a closer examination of the norm in reference to its context within the UN Charter, to its spirit and purpose as well as to its drafting history, leads to the conclusion that "force" in the meaning of Article 2(4) of the UN Charter means "armed force" only.[27] This finding is supported by the resolutions of the UN General Assembly, which do not depict political and economic coercion as an aspect of use of "force", but rather of the principle of non-intervention in domestic affairs of another State.[28] Although they are non-binding documents (see Article 10 of the UN Charter), the resolutions can be seen as relevant to the interpretation of Article 2(4) of the UN Charter as "subsequent practice"[29] of the UN Member States. Further, the above finding is supported by the jurisdiction of the International Court of Justice (ICJ). In its *Nicaragua Case* of 1986, the Court did not address economic coercion measures undertaken by the USA against Nicaragua as a "use of force", but discussed it in relation to the principle of "non-intervention".[30]

---

international customary law. *See*: G. Ress, The Interpretation of the Charter, in: Simma (*supra* note 23), at para. 2 *et seq.*

[25] *See* Randelzhofer, Art. 2(4), *supra* note 23, at para. 65 *et seq.*

[26] B.E. Carter, Economic Coercion, in: Encyclopedia of Public International Law (September 2009, electronic version, free sample article), at para. 6 *available at* http://www.mpepil.com/sample_article?id=/epil/entries/law-9780199231690-e1518&recno=7& (last visited 22 June 2011); Randelzhofer, Art. 2(4), *supra* note 23, at para. 21.

[27] A sound interpretation of Article 2(4) of the UN Charter including aspects of its context, spirit and purpose as well as the drafting history would exceed the scope of the present analysis; *see* representatively: Randelzhofer, Art. 2(4), *supra* note 23, at para. 16-27.

[28] E.g. *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* [in the following referred to as *Friendly Relations Declaration*], UN GA Res. 2625 [XXV] of 24 October 1970, Annex, Principle 1; *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*, UN GA Res. 2131 [XX] of 21 December 1965, para. 2; *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, UN GA Res. 36/103 of 9 December 1981, para. 2, principle I(b) and II (a); *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, UN GA Res. 42/22 of 18 November 1987, Annex, para. 8.

[29] *See* Article 31 (3)(b) of the *Vienna Convention on the Law of Treaties* of 1969: "There shall be taken into account, together with the context: […] any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation". *See* also *supra* note 24.

[30] I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 126 para. 245.

Thus, assuming that the effects of *Stuxnet* did negatively affect the quality of a uranium enriched end product of a presumably high economic value at the facility in *Natanz*, and did have a negative impact on Iran´s nuclear programme, which is a part of the State´s economy, such effects would not be considered with regard to Article 2(4) of the UN Charter.

However, as of today, there is no agreement as to which actions would constitute "armed force". The UN General Assembly's *Definition of Aggression*[31] of 1974, which partly[32] reflects international customary law and defines the broader term of "aggression" (Article 39 of the UN Charter), is often referred to by scholars and practitioners when defining "armed force". Analysis of the examples stated in Article 3 of the document leads one to the conclusion that use of "armed force" means use of conventional physical force by military or paramilitary forces of one State against the forces of another State (including acts of individuals or groups, if attributable[33] to a State).

According to the traditional understanding, the use of military force requires the employment of kinetic weaponry. A weapon is a tool designed to cause kinetic effects of a physical nature on a body or on an object. *Stuxnet* was allegedly designed to amend, suppress, delete or send data, but not to directly cause kinetic effects. However, some means, like biological or chemical agents, are reckoned to be weapons, although they do not set free any kinetic energy.[34] Their use is deemed to be one of "armed force" because, although they do not cause physical destruction, they aim to cause death or injury.[35] This approach, focusing on the effects rather than the means, perfectly corresponds with the

[31] UN GA Res. 3314 (XXIX) of 14 December 1974, Annex.

[32] In regard to Article 3(g) of the resolution: I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 103 para. 195.

[33] As of today, there is no internationally agreed set of criteria for attribution of actions of non-state actors to a State, although indications can be found in scholar writings and international jurisdiction, the ILC-*Draft Articles on Responsibility of States for Internationally Wrongful Acts* of 2001, *supra* note 20, being also a supporting reference.

[34] J. Barkham, Information Warfare and International Law on the Use of Force, in: Vol. 34 *New York University Journal of International Law & Politics* 2001, p. 57 *et seq.*, at p. 72; T. Morth, Considering Our Position. Viewing Information Warfare as Use of Force Prohibited by Article 2(4) of the U.N. Charter, in: Vol. 30 *Case Western Reserve Journal of International Law* 1998, p. 576 *et seq.*, at p. 590.

[35] I. Brownlie, International Law and the Use of Force by States (Oxford, Clarendon Press, 1963), at p. 362.

effects-based approach inherent to public international law. Thus, the majority of scholars judge malicious cyber-activities to be a use of "armed force" if they show effects comparable to those of kinetic, biological or chemical weapons, i.e. those which directly or indirectly result in death, physical injury or the destruction of property.[36] Additionally, some scholars demand that further criteria should be met in order to classify malicious cyber-activities as uses of "armed force", one of which is the severity of the effects.[37]

Thus, the assessment of the installation, control and alleged effects of *Stuxnet* as constituting use of "armed force" pursuant to Article 2(4) of the UN Charter depends on whether the worm indirectly caused a non-trivial destruction of property. It remains unclear whether the worm (indirectly) destroyed or affected the physical integrity of (a considerable number of) IR-1 centrifuges at the nuclear enrichment plant at *Natanz* or at other nuclear facilities in Iran.

However, even if "physical" effects outside the targeted SCADA systems were not detectable, the installation, control and presumed effects of *Stuxnet* could be deemed to be a use of "armed force" if they substantially disrupted Iranian critical infrastructure systems.

---

[36] Y. Dinstein, Computer Network Attack and Self-Defense, in: M.N. Schmitt & B.T. O'Donnell (eds.), Computer Network Attack and International Law (Newport / Rhode Island, US Naval War College, 2002), p. 99-119, at p. 103; D.B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter', in Schmitt & O'Donnell (eds.), p. 73-97, at p. 85; J. Barkham, *supra* note 34, at p. 80; T. Morth, *supra* note 34, at p. 591; C.C. Joyner & C. Lotriont̩e, Information Warfare as International Coercion: Elements of a Legal Framework, in: Vol. 12 No. 5 *European Journal of International Law* 2001, p. 825-865, at p. 846 and 850; M.N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, in: Vol. 37 No. 3 *Columbia Journal of Transnational Law* 1999, p. 885-937, at p. 914; W.G. Sharp, Cyberspace and the Use of Force (Aegis Research Cooperation, Falls Church 1999), at p. 102; L.T. Greenberg, S.E. Goodman & K.J. Soo Hoo, Information Warfare and International Law (National Defence University, Washington 1998), at p. 19 and 32.

[37] *See* M.N. Schmitt, Computer Network Attacks: The Normative Software, in: Vol. 4 *Yearbook of International Humanitarian Law* 2001, p. 53-85, at p. 65 *et seq.* Schmitt proposes a catalogue of criteria indicating that a malicious cyber-activity constitutes "use of force": (1) severity of the effects, i.e. threat of physical injury or destruction of property, (2) immediacy of the occurrence of the negative consequences, (3) direct nexus between the CNO and the negative consequences caused, (4) invasiveness of the consequences on foreign territory, (5) measurability of the consequences, (6) pre-assumption of illegitimacy of the CNO according to national rules and to the International Public Law, based on the prima facie illegitimacy of the use of force in international relations. It shall be only mentioned that some of those criteria determine the conditions of attribution of the damage to a certain action rather than specify the term "use of armed force". Further, it is debatable, whether a particular act is to be deemed as illegal by the assertion of its prima facie legitimacy.

Article 41 of the UN Charter, which describes the complete or partial interruption of critical infrastructure systems as measures employed by the UN Security Council "not involving the use of armed force", would not contradict such an inference.[38] The disruption of critical infrastructure systems can equally be caused by UN Security Council measures which would involve the use of "armed force", finding then their legal basis in Article 42 of the UN Charter instead of Article 41. However, it is agreed amongst the majority of scholars that the disruption of computer networks supporting critical infrastructure systems can only be considered a use of "armed force" if its effects can be equated to physical destruction.[39] Thus, the installation, control and alleged effects of the *Stuxnet* worm could only be deemed a use of "armed force" if they were significantly disruptive to one or more critical infrastructure systems (e.g. the energy supply infrastructure as such) of Iran in a way comparable to the physical destruction of the facilities and systems involved. As of today, such serious effects have not been reported.

Further, according to a minority view, the mere destruction of data which is of substantial importance or of significant economic value is to be considered a use of "armed force".[40] This view reflects the fact that nowadays data sets can be deemed to have a value and importance comparable to those physical assets enjoy. Consequently, it appears compelling, even in the context of Article 2(4) of the UN Charter, to apply the same criteria and consequences to the deletion of data of significant economic value or importance as to the physical destruction of objects. However, it could be questioned whether the mere deletion of data without further physical effects outside the targeted computer system would be comparable to the employment of kinetic, biological or chemical weaponry. Further, it would be most difficult to determine in each individual case of malicious cyber-activities whether the data deleted were indeed of "substantial importance" or of a rather trivial nature. The *Stuxnet* worm was reported to have been aimed at the amendment of data in SCADA systems of one or more Iranian nuclear facilities. Deletion of data is an inherent part of data

[38] *See* also Schmitt, *supra* note 36, at p. 912.

[39] J.P. Terry, Responding to Attacks on Critical Computer Infrastructure. What Targets? What Rules of Engagement?, in: Schmitt & O'Donnell, *supra* note 36, p. 421-437, at p. 428 *et seq.*; Morth, *supra* note 34, at p. 599. *See* also Sharp, *supra* note 36, at p. 129 *et seq.* Contra: Dinstein, *supra* note 36, at p. 105.

[40] *See* Barkham, *supra* note 34, at p. 88.

amendment, as the latter constitutes a process of data overwriting. Thus, according to the minority view presented, it would depend on the substantial economic value or importance of the deleted or overwritten data within the SCADA systems as to whether the installation of the *Stuxnet* worm was to be considered a use of "armed force".

Pre-Emptive Self-Defence

Only if the installation, the control and the alleged effects of the *Stuxnet* worm were deemed equivalent to the use of force pursuant to the general prohibition of Article 2(4) of the UN Charter, could it be considered whether the malicious cyber-activities were justified as measures of self-defence.

Pursuant to Article 51 of the UN Charter (and the corresponding international customary law)[41], the right to self-defence comprises the use of defensive military force against an "armed attack" launched by another State (or possibly by non-state actors)[42]. Even though there is a degree of uncertainty[43] as to which actions would actually constitute an "armed attack", in general terms, it would require direct or indirect use of "armed force" of significant scale and effects.[44] Additionally, a customary right to "anticipatory" ("preventive" or "interceptive") self-defence in situations "in which the necessity of self-defence is instant,

[41] Y. Dinstein, War, Agression ans Self-Defence (Cambridge University Press, Cambridge, 3rd ed. 2001), at p. 165; I. Brownlie, International Law and the Use of Force by States Revised, in: Vol. 21 *Australian Yearbook of International Law* 2000, p. 21-37, at p. 26; Brownlie, *supra* note 35, at p. 272-275. *See* also references at A. Randelzhofer, Art. 51, in: Simma, *supra* note 23, at para. 10, footnote 25.

[42] *See* detailed discussion at M.N. Schmitt, "Change Direction" 2006: Israeli Operations in Lebanon and the International Law of Self-Defense, in: Vol. 29 *Michigan Journal of International Law* 2008, p. 127-164.

[43] *See* discussion at Randelzhofer, *supra* note 41.

[44] *See* I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 101 and 103 para. 191 and 195 („the most grave forms", „[…] of significant scale […]", „[…] because of its scale and effects, would have been classified as an armed attack rather than a mere frontier incident […]"); I.C.J., *Oil Platforms (Islamic Republic of Iran v. United States of America), Merits*, I.C.J. Reports 1996, p. 803 *et seq.*, at p. 830 para. 51. In regard to the lawfulness of the use of armed force in cases of "low intensity conflicts" *see* Randelzhofer, *supra* note 41, at para. 6-8.

overwhelming, leaving no choice of means, and no moment for deliberation"[45] (*Caroline* or *Webster* formula)[46], is affirmed in academic writings.[47]

As there are no indications of an "armed attack" or imminent "armed attack" by Iran against any State, only the concept of so-called pre-emptive self-defence could be thought of in the context of a justification of the malicious cyber-activities directed against Iran´s nuclear facilities.

The concept of pre-emptive self-defence does not require an armed attack to have occurred or to be imminent. According to the doctrine, the right to self-defence is triggered when the threat of an armed attack is emerging, means short of use of force are not deemed sufficient to eliminate the threat, and measures of the UN Security Council are either not expected or not expected to be effective.[48] Scholars who support[49] the concept emphasize the need to effectively defend against attacks by terrorists and "rogue states" possessing weapons of mass destruction. It is especially stressed that the criterion of "immediacy" of an attack is

---

[45] *See* quote at Brownlie, *supra* note 35, at p. 43. *See* also Article 25 of the ILC-*Draft Articles on State Responsibility of States for Internationally Wrongful Acts* of 2001 (*supra* note 20), according to which the wrongfulness of an act is precluded if that act (1) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (2) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

[46] In 1837, settlers in Canada rebelled against the British colonial government. American sympathizers assisted the rebels with men and supplies, transported by the steamboat *The Caroline*. In response, British forces entered United States territory at night (from Canada), seized *The Caroline*, set the ship on fire, and sent it over the Niagara Falls. The British government claimed that the attack was an act of self-defence. In a letter to the British Ambassador, US Secretary of State *Daniel Webster* argued that a self-defence claimant would have to show the criteria as quoted above. *See* details at W. Meng, The Caroline, in: R. Bernhardt (ed.), Encyclopedia of Public International Law (Vol. I., 1992), p. 537 *et seq.*

[47] Dinstein, *supra* note 41, at p. 182 and 244; Meng, *supra* note 46; *see* also discussion and references at Randelzhofer, *supra* note 41, at para. 10, 35, 39.

[48] M.N. Schmitt, Preemptive Strategies in International Law, in: Vol. 24 *Michigan Journal of International Law* 2003, p. 513-548, at p. 530 *et seq.*; Dinstein, *supra* note 41, at p. 220.

[49] O. Corten, The Controversies Over the Customary Prohibition on the Use of Force. A Methological Debate, in: Vol. 16 *European Journal of International Law* 2005, p. 802-822, at p. 807 *et seq.*; Reisman, *supra* note 23, at p. 87 *et seq.*; Schmitt, *supra* note 48, at p. 534; A.D. Sofaer, On the Necessity of Pre-emption, in: Vol. 15 *European Journal of International Law* 2003, p. 209-226, at p. 210 and 214; M.J. Glennon, The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter, in: Vol. 25 *Harvard Journal of Law and Public Policy* 2002, p. 539-558, at p. 552 *et seq.*; Dinstein, *supra* note 41, at p. 220.

primarily suitable in the context of visible mobilization of armed forces, and would impede effective defence against an attack launched by weapons of mass destruction. Others[50] reject the concept, asserting that the speculative concerns of a State about another State's possible future actions cannot be equated with an "armed attack". Those scholars also refer to Article 39 of the UN Charter, which authorizes the UN Security Council alone to take measures against latent threats to international peace and security, a finding supported by the report of the UN *High-level Panel on Threats, Challenges and Change*[51] of 2004 as well as by the ICJ in the case *Congo v. Uganda*[52] of 2005.

Although there are some individual cases of State practice[53] that could be considered examples of pre-emptive self-defence, partly accompanied by respective *opinio juris*[54], today it is rather doubtful whether the concept reflects public international law. It shall only be mentioned that, according to the ICJ´s findings in the *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* of 1996, the mere possession of nuclear weapons is not illegal under customary international law[55]. Therefore, the development or possession of weapons of mass destruction can only comprise a violation of treaty obligations, such as the violation of the *Treaty on the Non-Proliferation of Nuclear Weapons* ratified[56] by Iran in

[50] *See* also Randelzhofer, *supra* note 41, at para. 39 *et seq*.

[51] Report of the Secretary-General's High-level Panel on Threats, Challenges and Change. UN (2004), at p. 55 para. 190-194.

[52] I.C.J., *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo* v. *Uganda), Judgment,* I.C.J. Reports 2005, p. 168 *et seq.*, at p. 223 *et seq.* para. 148.

[53] *See* examples at Ch. Gray, The US National Security Strategy and the New "Bush Doctrine" on Preemptive Self-defense, in: Vol. 1 *Chinese Journal of International Law* 2002, p. 437-447, at p. 440 *et seq.*; M.E. O´Connell, Pre-Emption and Exception. The U.S. Moves Beyond Unilaterism, in: D.S. Lutz, H.J. Gießmann (eds.), Die Stärke des Rechts gegen das Recht des Stärkeren. Politische und rechtliche Einwände gegen eine Rückkehr des Faustrechts in die internationalen Beziehungen (Nomos, Baden-Baden 2003), p. 148-159, at p. 154.

[54] *Opinio juris* refers to the belief of States that a certain State practice is in conformity with international law. *Opinio juris* is an aspect necessary for the development of international customary law, *see* M.N. Shaw, International Law (Cambridge University Press, Cambridge et al., 6th ed. 2008), at p.84 *et seq*.

[55] I.C.J., *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* I.C.J. Reports 1996, p. 226 *et seq*., at p. 277-267.

[56] *See* UN website, Disarmament Affairs, Weapons of Mass Destruction, Nuclear Weapons, Nuclear Non-Proliferation Treaty, Status of the Treaty *available at* http://unhq-appspub-

1970. It is rather questionable whether such a violation alone, without further acts, could comprise an emerging threat of an "armed attack" in the meaning of the concept of pre-emptive self-defence.

Countermeasure Short of Use of Force

Furthermore, the installation, control and alleged effects of the *Stuxnet* worm could be discussed as a countermeasure. A countermeasure is an act which is otherwise illegal under public international law, but justified if taken in response to a previous intentional wrongful act of another State.[57] It aims to induce the State which has committed the wrongdoing to comply with its international obligations.[58]

Considering the prohibition of threat or use of force in international relations (Article 2(4) of the UN Charter) and the obligation of States to settle their international disputes by peaceful means (see Article 2(3) of the UN Charter and diverse conventions[59]), only countermeasures short of "use of force" are legal.[60] This finding is supported by Articles 49 and 50(1)(a) of the ILC-*Draft Articles on Responsibility of States for Internationally Wrongful Acts* of 2001, by several resolutions of the UN Security Council[61] and UN General Assembly[62] as well as by the

---

01.un.org/UNODA/TreatyStatus.nsf/NPT%20(in%20alphabetical%20order)?OpenView&Start=1.58 (last visited 22 June 2011).

[57] *See* e.g. Brownlie, *supra* note 35, p. 281 *et seq.*

[58] *Id*.

[59] *See* e.g. *Convention on Pacific Settlement of International Disputes* (Hague I) of 18 October 1907, Article 12 of the *Charter of the League of Nations* of 28 June 1919, Article II of the *Briand-Kellogg-Pact* of 27 August 1928, *General Convention of Inter-American Conciliation* (Montevideo-Convention) of 5 January 1929; Article I of the *American Treaty on Pacific Settlement* (Bogota-Pact) of 30 April 1948.

[60] B. Simma, NATO, the UN and the Use of Force: Legal Aspects, in: Vol. 10 *European Journal of International Law* 1999, p. 1-22, at p. 2; Brownlie, *supra* note 35, p. 281 *et seq*.

[61] *See* e.g.: SC Res. 101 (1953) of 24 November 1953, para. 1 (Israel v. Jordan): „retaliatory action"; SC Res. 111 (1956) of 19 January 1956, para. 2 (Israel v. Syria): „whether or not undertaken by way of retaliation"; SC Res. 171 (1962) of 9 April 1962, para. 2 (Israel v. Syria): „The Security Council, [...] [r]eaffirms its resolution 111 (1956) [...] which condemned Israel military action [...] whether or not undertaken by way of retaliation"; SC Res. 188 (1964) of 9 April 1964, para. 1 (Great Britain v. Yemen): „The Security Council, [...] [c]ondemns reprisals"; SC Res. 228 (1966) of 25 November 1966, para. 4 of the preamble and para. 3 (Israel v. Jordan): „condemning past incidents of reprisal", „actions of military reprisals cannot be tolerated"; SC Res. 270 (1969) of 26 August 1969, para. 4 (Israel v. Lebanon): „actions of military reprisal […] cannot be tolerated."

jurisdiction of the ICJ[63]. Therefore, the installation, control and alleged effects of *Stuxnet* could only be considered a legal countermeasure if they are short of "use of force" in the meaning of Article 2(4) of the UN Charter (see discussion above).

In order to be justifiable, several other conditions must also be met by a countermeasure.[64] In the context of *Stuxnet*, two of those conditions merit closer examination: First, a legal countermeasure can be taken in response to a previous intentionally wrongful act of the State the countermeasure is directed against. Second, the State conducting the countermeasure must be injured by the wrongful act in question.

Whether those requirements are met depends upon whether Iran did commit an illegal act under international law against one or more States which installed and controlled the *Stuxnet* worm. It shall be only mentioned that Iran´s international obligations deriving from the *Treaty on the Non-Proliferation of Nuclear Weapons* apply only towards the community of States Party to the treaty as a whole; the international obligations in respect to inspections of the International Atomic Energy Agency (IAEA) apply towards the IAEA only. Thus, if *Stuxnet* was installed and controlled by one or more States, it will be difficult to argue that Iran injured that State or these States through alleged violations of its obligations deriving from the above mentioned international treaty.

Bearing in mind that a countermeasure aims to induce the culpable State to comply with its international obligations, one could imagine a concept of pre-emptive countermeasures. Such a concept would, in a way, reflect aspects of the concept of pre-emptive self-defence (see discussion above), but with a major difference: while the concept of pre-emptive self-defence depicts a "use of force" aimed at preventing an "armed attack" expected in the future, a pre-emptive countermeasure would be short of use of force and would aim to

---

[62] *See* e.g. *Friendly Relations Declaration* which states that "States have a duty to refrain from acts of reprisal involving the use of force", UN GA Res. 2625 [XXV] of 24 October 1970, Annex, Principle 1, para. 6.

[63] *See* I.C.J. *Corfu Channel (United Kingdom v. Albania*), *Merits,* I.C.J. Reports 1949, p. 4 *et seq*., at p. 35; *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p.127 para. 249; *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* I.C.J. Reports 1996, p. 226 *et seq*., at p. 246 para. 46.

[64] *See* the enumeration of the conditions by the I.C.J. in *Gabčikovo-Nagymaros Project (Hungary v. Slovakia)*, I.C.J. Rep. 1997, p. 7 *et seq*., at p. 55-57 para. 83-87.

prevent any expected future illegal behaviour that did not constitute an "armed attack". Only if those purely theoretical deliberations were found to be conceivable could it be considered whether the installation and control of *Stuxnet* could be deemed a pre-emptive countermeasure undertaken against Iran, aiming to prevent future violations of the *Treaty on the Non-Proliferation of Nuclear Weapons*, i.e. by the development of nuclear weapons. However, today, the existence of such a concept of a pre-emptive countermeasure has neither been claimed by States nor asserted in scholars' writings.

Armed Conflict

Further, legal considerations could involve the question of whether the installation and control of the *Stuxnet* worm, as well as the effects it allegedly caused, could have incited an international armed conflict between Iran and the State or States responsible for the installation and control of the worm.

The question is of relevance since a situation of international armed conflict would invoke the applicability of the laws of armed conflict (LOAC), also referred to as humanitarian law, between the States Party to the conflict (see common Article 2 of the *Geneva Conventions* of 1949[65]), as well as the rules of neutrality.

According to the prevailing opinion, an international armed conflict occurs when one or more States have recourse to "armed force" against another State, regardless of the legality, reasons or even the intensity of this confrontation.[66] This opinion is confirmed by the Commentary on the *Geneva Conventions* of 1952 which states that "any difference arising between two States and leading to the intervention of armed forces is an armed conflict

[65] These are: *Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* of 12 August 1949 (I); *Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* of 12 August 1949 (II); *Convention Relative to the Treatment of Prisoners of War* of 12 August 1949 (III); *Convention Relative to the Protection of Civilian Persons in Time of War* of 12 August 1949 (IV).

[66] *See* D. Fleck (ed.), The Handbook of International Humanitarian Law (Oxford University Press, Oxford et al., 2nd ed. 2008), para. 202 and 210; *see* also a compendium of scholar opinions in: International Committee of the Red Cross (ICRC), How is the Term "Armed Conflict" Defined in International Humanitarian Law?, Opinion Paper (March 2008), at p. 1 *et seq. available at* http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (last visited 23 June 2011).

within the meaning of Article 2."[67] Thus, the situation of international armed conflict, and consequently the application of LOAC, is given when States use "armed force" against each another.

The notion of "use of armed force", which implies an international armed conflict, is to be distinguished from the term "use of (armed) force" in the meaning of Article 2(4) of the UN Charter. The former expression belongs to the body of law referred to as *ius in bello* which regulates the conduct of already ongoing hostilities, the latter being an aspect of the area of law called *ius ad / contra bellum* and dealing with the legality or illegality of the use of force between States. However, the two terms are closely related. Whenever a State carries out actions considered to be a "use of armed force" in the meaning of *ius ad bellum* against another State, this indicates the outbreak of hostilities reaching the level of "use of force" in the meaning of *ius in bello* and thus the threshold of an armed conflict. However, it could be asserted that this finding does not apply to quick, discrete and only "surgical" use of armed force by a State without further response by the victim (e.g. the reported[68] bombardment of the nuclear reactor in *Osirak* / Iraq in 1981 or in *Dair Alzour* / Syria in 2007 by Israel´s Air Force).

As *Stuxnet* reportedly affected components in Iran's nuclear installations between June 2009 and April 2010 – a considerable amount of time – its installation and remote control cannot be described as a quick and surgical action. Therefore, the question of whether the installation of *Stuxnet* and its control and alleged effect, led to a situation of international armed conflict between Iran and one or more States responsible for the installation and control of the worm, depends upon whether those actions are considered "use of force" within the meaning of Article 2(4) of the UN Charter (see discussion above).

---

[67] J. Pictet, Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (ICRC, Geneva 1952), at p. 32.

[68] *See* e.g. U. Mahnaimi, S. Baxter & M. Sheridan, Israelis 'blew apart Syrian nuclear cache', in: *The Sunday Times* online of 16 September 2007 *available at* http://www.timesonline.co.uk/tol/news/world/middle_east/article2461421.ece (last visited 23 June 2011); S. M. Hersh, A Strike in the Dark, in: *The New Yorker* online of 11 February 2008 *available at* http://www.newyorker.com/reporting/2008/02/11/080211fa_fact_hersh (last visited 23 June 2011).

Territorial Sovereignty

Further, it is worth contemplating whether the installation, control and the alleged effects of the *Stuxnet* worm could be deemed a violation of the territorial sovereignty of Iran.

The principle of territorial sovereignty is to be distinguished from the principle of sovereign integrity, the latter of which is violated in the case of the (illegal) use of force by one State on the territory of another State (see discussion above).[69] Territorial sovereignty describes the exclusive authority of a State over its territory and is violated in cases of, for example, unauthorized entrance into the territory by foreign government agents or individuals on orders from another State or in cases of the unauthorized exercise of State authority on the territory of another State.[70] In order to violate the principle of territorial sovereignty, the effects caused by a State on the territory of another State, notwithstanding their scale or intensity, must be of either a physical nature or perceptible as the exercise of a foreign State´s authority. Bearing this in mind, it could be argued that, nowadays, a significant impairment or manipulation of the operations of a computer system by foreign governments' agents could constitute "causing perceptible effects" in relation to exercising a foreign State's authority.

It remains unclear whether the *Stuxnet* worm caused physical or perceptible effects outside the targeted SCADA system, for example by damaging the IR-1 centrifuges in the uranium enrichment plant at *Natanz*. It is not known whether the manipulation of the computer-controlled operation of the IR-1 centrifuges, and their speed in particular, was indeed significant. Very probably, the alleged alteration to the uranium enrichment of the end product at the *Natanz* facility cannot be considered to be a physical effect or a perceptible effect of exercising a foreign State's authority.

[69] *See* Shaw, *supra* note 54, at p. 522.

[70] *See* B. Fassbender & A. Bleckmann, Art. 2(1), in: Simma, *supra* note 23, at para. 10; Greenberg, Goodman & Soo Hoo, *supra* note 36, at p. 24; similar: Joyner & Lotriionte, *supra* note 36, at. p. 842 *et seq*.

Customary International Environmental Law

Although international environmental protection is provided for mainly under treaty law, there are a few environmental-related rules which are acknowledged to be part of customary international law. One of those fundamental rules of customary international law is the obligation of States not to significantly damage the natural environment beyond their national jurisdiction.[71] This obligation is based on the general postulation that the territorial sovereignty of the State inflicting environmental damage on its own territory is limited by the territorial integrity of the State affected.[72] The prohibition of causing trans-boundary environmental damage is expressed in numerous international treaty provisions[73], in various States´ declarations[74] and is endorsed by the jurisdiction of the ICJ[75].

There are currently no reports of any environmental damage on Iranian territory which could have been caused by the effects of the installation and control of the *Stuxnet* worm.

However, it could be considered whether the installation of *Stuxnet* in the operating systems of Iranian nuclear facilities could be deemed to have inflicted significant environmental danger.[76] Although the ILC-*Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*[77] of 2001 states that there is an obligation only to "minimize" the risk of

---

[71] *See* L. Gründling, Environment, International Protection, in: R. Bernhardt (ed.), Encyclopedia of Public International Law (Vol. II., 1995), p. 96 *et seq.*, at p. 101; I.C.J., *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226 *et seq.*, at p. 241 *et seq.* para. 29.

[72] Gründling, *supra* note 71, at p. 101.

[73] *See* an overview of treaties on international environment protection which are deposited with the UN at the UN Treaty Collection Website *available at* http://treaties.un.org/Pages/Treaties.aspx?id=27&subid=A&lang=en (last visited 23 June 2011). It shall be mentioned that the overview does not contain (numerous) regional treaties, especially the ones on international regimes for the use of rivers, lakes and other territorial waters.

[74] Gründling, *supra* note 71, at p. 101.

[75] *See* I.C.J., *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports 1996, p. 226 *et seq.*, at p. 241 *et seq.* para. 29; *Gabčikovo-Nagymaros Project (Hungary v. Slovakia)*, I.C.J. Reports 1997, p. 7 *et seq.*, at p. 41 para. 53.

[76] *See* e.g. Reuters, Russia's NATO envoy: Iran-bound Stuxnet worm could have caused new Chernobyl, in: *Haaretz* online of 26 January 2011 *available at* http://www.haaretz.com/news/international/russia-s-nato-envoy-iran-bound-stuxnet-worm-could-have-caused-new-chernobyl-1.339376 (last visited 24 June 2011).

[77] ILC-*Draft Articles on Prevention of Transboundary Harm from Hazardous Activities with commentaries* of 2001 *available at*

trans-boundary harm (Article 3), it is widely accepted within scholarly writing that causing significant trans-boundary risk or danger to the natural environment (either where this is highly probable or there is a risk of extremely serious consequences) is also prohibited by international custom.[78]

However, the assessment of the possible danger of environmental damage is impossible without detailed technical expertise and information on the potential negative impact *Stuxnet* could have had on the operating systems of Iran´s nuclear facilities and the potential danger which it may have posed to the natural environment.

Economic Coercion

Economic coercion is defined as any economic measure taken by a State during peace time in order to induce another State to change its policy or practices.[79] The term "economic coercion" is to be distinguished from the expression "economic warfare", as the latter describes the endeavours of Parties to an already ongoing armed conflict or war to weaken the enemy's ability to supply its military forces or population.[80] It shall only be mentioned, that – as stated above – measures of economic coercion do not constitute illegal use of force within the meaning of Article 2(4) of the UN Charter.

Assuming that *Stuxnet* did negatively affect the uranium enrichment process at Iran´s facility at *Natanz* and thus the quality and usability of an end product of a significant economic value, it could be questioned whether the actions presumably undertaken by one or more States should be judged to be a form of economic coercion. This deliberation is pertinent provided that the installation and alleged effects of *Stuxnet* did indeed change Iran's State

---

http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf (last visited 23 June 2011).

[78] G. Händl, Transboundary Impact, in: D. Bodansky, J. Brunnée & E. Hey (eds.), The Oxford Handbook of International Environmental Law (Oxford University Press, Oxford / New York 2007), p. 531-549, at p. 538 *et seq.*; Gründling, *supra* note 71, at p. 101.

[79] Carter, *supra* note 26.

[80] K. Zemanek, Economic Warfare, in: Bernhardt, *supra* note 71, p. 38.

practice, namely by delaying or otherwise amending Iran's course of action with regard to its nuclear programme, as repeatedly reported in the media[81].

The practice of States, condemning economic coercion in several regional treaties (e.g. Article 19 of the *Charter of the Organization of American States*), as well as the practice of the UN General Assembly[82] in adopting several resolutions and declarations condemning the use of economic coercion in order to influence the internal affairs of another State, indicate that economic coercion becomes legally relevant only if it reaches the threshold of a forbidden "intervention in internal affairs" of a State.[83] This finding is supported by the jurisdiction of the ICJ. In its *Nicaragua Case*, the Court did address economic coercion measures undertaken by the USA against Nicaragua in the context of the principle of "non-intervention" only.[84]

Principle of Non-Intervention in Internal Affairs

Assuming that *Stuxnet* was created, installed and controlled by one or more States, the customary rule of non-intervention in internal affairs of another State, a corollary of the principle of sovereign equality of States, could be relevant. The principle is endorsed in some regional conventions (e.g. Articles 16-19 of the *Charter of the Organization of American States*, Article 3 of the *Charter of the Organisation of African Unity*) as well as in Article 2(7) of the UN Charter in regard to UN organs. Further, it is reflected in declarations of certain States (e.g. Principle VI of the *Helsinki Final Act* of 1975[85]) and in resolutions of the UN

[81] *See* e.g. W.J. Broad, J. Markoff & D.E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, in: *The New York Times* online of 15 January 2011 *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1 (last visited 24 June 2011).

[82] *See supra* note 28.

[83] Carter, *supra* note 26, at para. 5, 11.

[84] I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.* at p. 126 para. 244 and 245.

[85] *(Helsinki) Final Act of the Conference on Security and Co-operation in Europe* of 1 August 1975 *available at* http://www.hri.org/docs/Helsinki75.html#H4.6 (last visited 22 June 2011).

General Assembly[86]. Also, it is confirmed to be part of international customary law by the ICJ.[87]

An illegal intervention occurs when a State interferes with the internal or external affairs of another State considered by the latter as "internal" or "domestic" (domestic jurisdiction, *domaine réservé*), in order to coerce the other into certain behaviour. [88]

In general terms, it can be asserted that the "internal" or "domestic" affairs of a State are all those affairs not regulated by international norms.[89] It is debatable whether the installation and control of *Stuxnet* and the subsequent influence on Iran's nuclear programme would affect an "internal" or "domestic" affair. Since 1958 Iran has been a Member of the IAEA. As of November 2010[90] the IAEA has 151 Members, representing approximately 80% of the international community. In 1970 Iran ratified[91] the *Treaty on the Non-Proliferation of Nuclear Weapons*, making Iran's nuclear programme subject to IAEA´s verification. As of today, 190 States are Parties to the – consequently almost universal – treaty.[92] In consequence, it can be disputed whether Iran´s nuclear program is a matter of "internal" or "domestic" affairs, or rather a matter of an "internationalized" nature not falling under Iran´s *domain réservé*.

Additionally, it is questionable whether *Stuxnet*'s installation, control and effects as reported in the media can be deemed a mode of "coercion". It will always be a challenging undertaking to distinguish between the employment of illegal coercion and the perfectly

---

[86] *See supra* note 28.

[87] I.C.J., *Corfu Channel (United Kingdom v. Albania*), *Merits,* I.C.J. Reports 1949, p. 4 *et seq.*, at p. 35; *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 106 para. 202.

[88] Th. Oppermann, Intervention, in: Bernhardt, *supra* note 71, p. 1436; I.C.J., *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.* at p. 106 *et seq.* para. 202-203.

[89] U. Beyerlin, Intervention, in: Wolfrum / Philipp, *supra* note 23, p. 378 *et seq.*, at para. 7.

[90] *See* IAEA website, Member States of the IAEA *available at* http://www.iaea.org/About/Policy/MemberStates/ (last visited 22 June 2011).

[91] *See supra* note 56.

[92] Information *available at* http://unhq-appspub-01.un.org/UNODA/TreatyStatus.nsf (last visited 26 June 2011).

legal employment of (political, economic etc.) influence.[93] Indeed, neither State practice nor academic writings provide useful criteria for such a distinction.[94] However, scholarly writing asserts that illegal coercion is the employment of massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not envision as a free and sovereign State.[95] Some additional indications as to the meaning of the term "coercion" can be derived from the *Friendly Relations Declaration*[96] unanimously adopted by the UN General Assembly in 1970. Although it is a non-binding document (see Article 10 of the UN Charter), it was stated by the ICJ in the *Nicaragua Case*[97] of 1986 that it represented the *opinio juris* of the international community (see also Article 31(3)(b) of the *Vienna Convention on the Law of Treaties* of 1969). Thus, the declaration can be deemed to be a valuable reference. In its Principle 3, the declaration describes armed intervention, obtaining subordination of the exercise of a State's sovereign rights, and actions directed towards the violent overthrow of a regime of another State, as being a forbidden intervention in the internal affairs of a State. It further affirms that every State is free to choose its political, economic and cultural system. All in all, scholarly writing as well as the examples given by the *Friendly Relations Declaration* indicate that "coercion" occurs only in drastic cases of overwhelming – direct or indirect – force being put upon a State's free and sovereign decision-making process.

The effects of the installation and control of *Stuxnet* were reported to have had a delaying effect on Iran's nuclear programme by a few years. It is rather questionable whether this presumed outcome is comparable with the above mentioned threshold of an overwhelming force put upon a State and its decision-making processes. Consequently, it can be doubted whether the installation and the alleged effects of *Stuxnet* can be considered coercion and thus forbidden intervention in internal affairs with regard to the alleged delay of Iran's nuclear programme.

---

[93] *See* discussion at Oppermann, *supra* note 88, at p. 1436.

[94] *Id*.

[95] Beyerlin, *supra* note 89, at p. 809.

[96] *See supra* note 28.

[97] I.C.J., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits*, I.C.J. Reports 1986, p. 14 *et seq.*, at p. 106 para. 202.

However, it is worth considering whether the negative effects *Stuxnet* might have had on Iran's economy could be considered "coercion". Acknowledging Iran´s nuclear programme as part of the State economy, and the uranium enriched end product (whose quality or enrichment percentage is affirmed to be diminished by the effects of *Stuxnet*) as a material of high economic value, a forbidden intervention in regard to the State's economy seems at first sight to be a valuable consideration. However, it must be taken into account that the *Friendly Relations Declaration* assumes that a "forbidden intervention" occurs in cases of interference with the choice of the economic system as such, but not in cases of causing selective economic damage. This statement correlates with the findings of the ICJ, which rejected, in its *Nicaragua* judgment, even more drastic economic measures undertaken by the USA against Nicaragua as being a forbidden intervention in domestic affairs (these included the cessation of economic aid in April 1981, the reduction of the sugar quota for imports from Nicaragua by 90%, and a trade embargo adopted on 1 May 1985).[98] Thus, the assumption of a forbidden intervention in internal affairs based on the possible negative effects the installation and control of the *Stuxnet* worm could have had on Iran's economy, is questionable.

Conclusion

As the facts concerning *Stuxnet* partly remain unclear, the legal analysis of the creation, installation, control and effects of the computer program can be based on assumptions only. Under the supposition that the malicious software has been created, installed and controlled by one or more States and indeed did not cause any damage of physical nature, it appears not to reach the threshold of illegality pursuant to public international law and thus to be a "legal masterpiece".

[98] *Ibid.*, at para. 244 and 245.