Forum of EthnoGeoPolitics

Main Article

Non-proliferation of cyber weapons with a CBRN consequence

An exploratory analysis from an international-judicial perspective on cyber weapons with chemical, biological, radiological or nuclear consequences

Bas Wallage LL.B, Jeroen Slobbe M.Sc, and Stas Verberkt M.Sc

Introduction

Driven by the high dependence on digital networks, the threat of cyber weapons for society is serious. The Dutch government asked the Advisory Council on International Affairs (Adviesraad Internationale Vraagstukken, AIV) and the Advisory Committee on Issues of Public International Law (*Commissie van Advies inzake Volkenrechtelijke Vraagstukken*, CAVV) in 2010 to conduct research on this threat.[1] Meanwhile, among others, the United States[2] and South Korea[3] have declared their intention to actively develop cyber weapons.

Since the Stuxnet-virus in 2010 destroyed Iranian nuclear centrifuges, it has become clear that a cyber weapon is not just capable of shutting down a system or causing an explosion[4], but potentially can have the effects of a weapon with a chemical, biological, radiological or nuclear (CBRN) consequence.

The public debate on cyber weapons and how these should be curbed politically has not yet come up with a broadly shared consensus, partly because the Internet is seen as *terra nullius* —a no man's land[5]—and because of the attribution problem.[6] In this article the authors will describe the need for international agreements concerning cyber weapons with a CBRN consequence. The attribution problem is not further discussed in this article due to constraints in time and space and the overall goal of starting the discussion rather than solving the problem directly.

In this article, we define cyber weapons with a CBRN consequence as: cyber weapons capable of modifying the equipment or installation of a CBRN weapon or a CBRN installation, such that the control comes to lie partially or completely in the hands of the attacking state. This may for example concern a cyber weapon that disables the safety switch on storage tanks containing toxic materials for the production of CBRN weapons or gives an unauthorized instruction to attack the equipment of such materials.[7] The article will further discuss and focus on cyber weapons with a CBRN consequence that are in the possession of a nation state.

The Digital Threat

The Dutch government acknowledges the threat of cyber weapons, but also indicates that the extent of the threat and the impact this may have on Dutch society remains yet unknown.[8] Thus further research is of crucial importance, according to the Dutch government in 2011. After the Stuxnet-attack in 2010 against Iran's nuclear centrifuges with as result the destruction of these centrifuges and therefore a significant delay in the Uranium enrichment program, it has become obvious to many that the impact of cyber weapons can be considerable.

At this time, the digital domain is heavily affected by offensive dominance.[9] It is almost impossible to fully secure a digital or any other electronic network. For this reason, states may choose to develop possibilities of (counter-)attack. It is easier, faster and cheaper to attack a system than to protect it.[10] This is partly, amongst other things, caused by the anonymity in which the attacker can prepare, who then can count on the advantage of surprise. Moreover, the monitoring on the use of cyber weapons is difficult, again due to the anonymity of the attacker and thus the lack of a clearly identifiable aggressor.

Cyber weapons are comparatively easy to hide, in sharp contrast to traditional weapons with a CBRN consequence. For example, interballistic missiles with a nuclear consequence are large physical devices that emit radiation. Because some states focus on cyber counter-attacks, and an international monitoring system of cyber weapons with a potential CBRN consequence is gravely lacking, it is vital that states start to form agreements regarding the use of and non-use of i.e. prohibitions against this type of cyber weapons.

The Stuxnet-attack

One of the most famous cyber weapons with a potential CBRN consequence is Stuxnet. One of the two variants of this virus was spread through a USB-stick and targeted industrial systems in Iran.[11] After three years of investigation it became clear that this cyber weapon had had huge consequences. Given the scale and complexity of the attack, one suspects and expects a nation state as being responsible for the virus. The virus is in fact so complex that it must have been created by a group of consisting of multiple, various computer engineers over a number of years.[12] Although unproven, researchers suspect the United States and Israel of developing the Stuxnet virus.[13]

Ralph Langner describes two Stuxnet attacks in his research on this virus. The first version of Stuxnet originates from 2007 and can be seen as one of the most aggressive known cyber weapon in history.[14] This virus was used to disrupt Iran's nuclear program. The first version of Stuxnet tried to take over the security system of the Natanz uranium reactor.[15]

These reactors are operated primarily by Siemens S7-417 controllers, which control a group of 164 centrifuges.[16] The purpose of the virus was to cause irreparable damage to these centrifuges.[17] The virus made the end users believe that the system was functioning properly[18]. While the impact of this first attack is formally unknown, Iran's former President Ahmadinejad of Iran has admitted that the reactors in Natanz were indeed been attacked by the Stuxnet virus.[19]

The second version of Stuxnet made sure that the systems of the Iran's nuclear centrifuges were damaged by alternately shutting down and increasing the speed of rotation. Due to these differences in speed within a relatively short time period, the centrifuge can break down.[20] This version also simultaneously sent false data to the control systems and displays. The virus probably has shut down the nuclear centrifuges in Iran for a period of time, thus stagnating the uranium enrichment production during that time.[21]

Langner said after his investigation that there has never been such a complex and precise cyber weapon developed and deployed before: "A computer virus that can cause damage in the physical world without any casualties. It's like turning up with a JSF jet fighter on a battlefield during the First World War." [22] Langner is also of the opinion that the virus has not been created by private individuals.

Destroying the centrifuges has been a financial and political blow to Iran, but it has not resulted in an explosion. In 1982 a Trojan Horse virus in the Trans-Siberian gas pipeline resulted in a huge gas explosion.[23] The consequences of such viruses (with a cyber to physical effect) can be immense. For this reason it is urgent that international agreements are made on the none-use of such cyber weapons.

Cyber Weapons with CBRN-consequence and Humanitarian Law

The reports of the Advisory Council (AIV) and Advisory Committee (CAVV) contain the proposal to consider the digital domain as the fifth dimension for military action, in addition to the traditional four dimensions—land, sea, air and space.[24] Article 36 of the Additional Protocol (I) to the Geneva Conventions[25] provides that when studying, developing, buying or commissioning a new weapon or way to conduct warfare, it must be determined whether the new weapon is in breach of any agreement under international law.

Arguably, the said Article 36 already partially limits the use of new cyber weapons with a CBRN consequence under existing agreements via its requirement to review the legality of such new weapons.[26] Nuclear cyber weapons—e.g. cyber weapons that make use of nuclear installations or nuclear missiles to generate a nuclear consequence—could be governed under the Non-Proliferation Treaty[27], which states that the signatory member states should not directly or indirectly transfer nuclear weapons or control over nuclear weapons to other states that at the time of the Convention's ratification, January 1, 1967, were not in possession of nuclear weapons. However, explicit agreements on cyber weapons with a CBRN consequence do not currently exist.[28]

The Necessity of International Agreements

Since many countries have an offensive strategy for the use of cyber weapons, it is important to make international agreements on the (non-)use of these weapons. At the G8 Summit in May 2011, the member states present expressed the belief that the Internet should be free as well as safe and secure.[29] The question remains how one can guarantee this safety, given the choice for an offensive strategy by many countries and the lack of international regulation.

At present, there are almost no international standards of conduct on the use of cyber weapons. Still, the United Nations General Assembly (UNGA) has stressed the importance of countries enhancing the protection of their systems in its Resolution 58/199.[30] The provision in this UNGA resolution, however, do not supervise or tackle the use of cyber weapons with CBRN consequence by nation states.

Possession of cyber weapons with CBRN consequence will be hard to prove in practice. However, this also applies to the possession of traditional weapons with such a consequence. Surprise-site inspections would be feasible. Through increasing the right of inspection[31] enforced by the requirement to conclude Comprehensive Safeguards Agreements with the International Atomic Energy Agency (IAEA) on the peaceful, safe and secure use of expanding nuclear technology with the ability to provide assurance about not developing cyber weapons with a nuclear consequence, one would have a crucial means to monitor the development of this type of weapons.

The advantage of this preventive agreement with respect to physical retaliation afterwards, is that the attribution problem becomes less relevant to international agreements to be made to govern the use and development of cyber weapons with a CBRN consequence.[32]

Nevertheless, the practical objections (for example the attribution problem) by the Dutch AIV and CAVV were sufficiently grave to advice that a treaty comparable to the non-proliferation treaty would have no added value.[33] On the other hand, one could argue that the use or at least development of traditional ´physical´ weapons by other countries can be equally hard to prove. Thus, a coalition of countries, including the Netherlands, intervened militarily in 2003 in Iraq because weapons of mass destruction supposedly were produced there. These weapons were never found and after subsequent investigation turned out to have never been present.[34]

The making of international agreements and the establishment of rules should ensure that countries agree on moral standards of behavior with each other on the use of cyber weapons. The implementation of these rules is then enforced by the international community. After drafting these rules, States Signatory Parties may seek affiliation to the International Court of

Justice or the Permanent Court of Arbitration so that disputes can be settled. This should create next to cyber regulation cyber law as well.

Conclusion

Given the developments in the digital domain, it is quite conceivable that states will wage war partially through the digital domain in the foreseeable future. In 2010 Iran suffered from the Stuxnet virus, which was able to destroy or at least severely damage or hamper its nuclear reactors. It was also found that some cyber weapons were and are able to cause an explosion in the physical world.

International agreements on traditional, physical weapons do exist, such as the Non-Proliferation Treaty. Despite the encouraging example of Article 36 of the Additional Protocol (I) to the Geneva Conventions, there are still no international rules on the (non-)use of cyber weapons with plural CBRN consequences.

Although the enforcement of such rules would be challenging in practice, just like the enforcement of rules on the (non-)use of traditional weapons with a CBRN consequence, such international agreements are absolutely necessary. For if there are no such rules, standards, supervisions and laws, it remains unclear to nation-states whether and when the use of cyber weapons with a potential CBRN consequence is unacceptable.

Jeroen Slobbe (jeroen.slobbe@gmail.com) and Stas Verberkt (stas@verberkt.net) are information security consultants. Bas Wallage (baswallage@hotmail.com) is a master student of Law at the University of Leiden, the Netherlands. *The authors thank Prof. Dr. L. van den Herik, Prof. mr. dr. M. Hildebrandt, Prof. Dr. Ph. Wallage and mr A. Altena for their advice and suggestions.*

Endnotes

1. AIV, CAVV, *Digitale Oorlogvoering* (Digital Warfare), No 77, AIV/no22, CAVV December 2011.
2. *The New York Times*, "U.S. Steps Up Effort on Digital Defenses", 27 April 2009.
3. *BBC News*, "South Korea to develop Stuxnet-like cyberweapons", 21 February 2014.
4. Frank Dickman, 'Hacking the industrial SCADA network', *Pipeline & Gas journal* Vol.236 No.11, November 2009.
5. Chatham House, *On Cyber Warfare*, November 2010.
6. Franklin D. Kramers *et al.*, "Cyberpower and National Security", Center for Technology and National Security Policy—National Defense University, 2009, pp.15-16.
7. Eric Byres, "Making the Control System Intrinsically Secure", Process Control Systems Forum, 2007, https://ics-cert.us-cert.gov/sites/default/files/pcsf-arc/making_cs_intrinsically_secure-byres.pdf.
8. Cybersecuritybeeld Nederland, December 2011, GOVCERT.NL, p.12, https://www.nctv.nl/Images/cybersecuritybeeld-nederland_tcm126-444006.pdf.

9. Report of a general consultation, established on 2014 the Defense Cyber Strategy, Dutch Ministery of Defense. 33-321 nr 4, 21 May 2014.

10. AIV, CAVV, *Digitale Oorlogvoering* (Digital Warfare), No 77, AIV/no22, CAVV December 2011, p.13.

11. A.R. Lodder and L.J.M Boer, 'Cyberwar? What war? *Justitiële verkenningen* (Judicial explorations) vol.38, no.1, 2012, p.52. *Veiligheid in cyberspace* (Security in cyberspace).

12. Ibid.

13. A prominent researcher of the Stuxnet virus, Ralph Langer, has given a lecture on "decoding Stuxnet", explaining exactly how the code has been deciphered and what could have been the possible consequences if the virus had not been detected and defused in time: see Cracking Stuxnet, a 21st-century cyber weapon, TED2011: www.ted.com/talks/lang/eng/ralph_langer_cracking_stuxnet_a_21st_century_cyberweapon.html (January 2012).

14. Ralph Langner, 'Stuxnet's Secret Twin', *Foreign policy*, 19 November 2011, p.2.

15. Ibid.

16. Ibid, p.4.

17. Ibid, p.5.

18. Ibid, p.6.

19. Ibid, p.4.

20. Ralph Langner, 'Stuxnet's Secret Twin', *Foreign policy*, 19 November 2011, p.8.

21. A.R. Lodder and L.J.M Boer, 'Cyberwar? What war?' *Justitiële verkenningen* (Judicial explorations) vol.38, no.1, 2012, p.52. *Veiligheid in cyberspace* (Security in cyberspace).

22. Iris Ludeker, "Virus als ultiem wapen (Virus as the ultimate weapon)", *Trouw* (a Dutch quality newspaper), 6 January 2011; quote translated from Dutch.

23. Frank Dickman, 'Hacking the industrial SCADA network', *Pipeline & Gas journal* Vol.236 No.11, November 2009.

24. AIV, CAVV, *Digitale Oorlogvoering* (Digital Warfare), No 77, AIV/no22, CAVV December 2011, p.10.

25. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

26. Ibid.

27. The Nuclear Non-Proliferation Treaty of May 25, 1970, United Nations Treaty Series (UNTS), 729, 169.

28. Editor, 'Do We Need Cyber Warfare Treaties? Study Looks at Legacy of Stuxnet', *Journal of law & cyber warfare*, 15 January 2014, http://www.jlcw.org/need-cyber-warfare-treaties-study-looks-legacy-stuxnet/.

29. G8 Declaration, Renewed Commitment for Freedom and Democracy, Deauville, 26-27 May 2011, http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf.

30. UNGA Resolution 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 23 December 2003.

31. International Atomic Energy Agency, "Model protocol additional to the agreement(s) between state (s) and the International Atomic Energy Agency for the application of safeguards", 1997, http://www.iaea.org/sites/default/files/publications/documents/infcircs/1997/infcirc540.pdf.

32. The attribution of an actual attack, regardless whether with traditional or cyber weapons, will always remain an issue. See for example the case of the shooting of flight MH17 in 2014.

33. AIV, CAVV, *Digitale Oorlogvoering* (Digital Warfare), No 77, AIV/no22, CAVV December 2011, p.30.

34. Parliamentary Report by the Commission of Inquiry about the Dutch decisionmaking on Iraq, the so-called Davids Commission, 2010, http://www.rijksoverheid.nl/bestanden/documenten-en-

publicaties/rapporten/2010/01/12/rapport-commissie-davids/rapport-commissie-irak.pdf. See also: Joost Oranje, "Acht vragen over onderzoek naar steun Irak-oorlog (Eight questions about inquiry into support for the Iraq war)", *NRC Handelsblad* (New Rotterdam Courier Trades′ Paper, a Dutch quality newspaper), 3 February 2009.

NB: do you have any comments on Bas Wallage *et al.*'s article? Please send these to info@ethnogeopolitics.org, or through the contact form at http://www.ethnogeopolitics.org.

Criticism of the paper's definition and framework of 'digital weapons of mass destruction'

(Critical Response to Bas Wallage *et al.*'s "Non-proliferation of cyber weapons with a CBRN consequence")

My first and foremost concern is the use of the term "cyber weapons of mass destruction". It would be more logical to address cyber weapons as such; and in this specific case, to address the use of cyber weapons against CBRN weapons/systems/facilities/etcetera, rather than to address "cyber weapons of mass destruction". The latter term does not exist in international law and other international sources; and I believe it is the result of a confusion in the article about the various ways to categorise weapons.

The two main approaches to categorise weapons are: the intended use (purpose) of a weapon; and the effects of a weapon. The approaches are, however, not mutually exclusive. For certain weapons the differences between their intended use (purpose) and effects remain ambiguous and contextual—for example white phosphor, which can be used legally for the purpose of creating a smokescreen as an operational cover for combatants; but it can also be used illegally as an incendiary weapon against non-combatants and other persons.

Such dilemmas, however, do not yet arise with cyber weapons. Here the questions are much more basic, and thereby, also more fundamental. What characterises cyber weapons is that they operate within the cyber environment and they can produce effects in the (i) digital and (ii) physical world.

(i) With respect to effects in the digital world, there is a legal/philosophical discussion about what amounts to an attack, within the legal meaning, if this takes place entirely within the digital environment.

(ii) With respect to effects in the physical world, there are many discussions, and one of them concerns the use of such tools to disrupt our environment.

In the latter hypothetical situation, these cyber weapons are sometimes called weapons of mass *disruption* and it is in that situation that there is serious concern about the implications