doi:10.1017/aju.2021.6

SYMPOSIUM ON NEW CHALLENGES IN WEAPONS INSPECTION

AN INSPECTION REGIME FOR CYBER WEAPONS: A CHALLENGE TOO FAR?

*Przemysław Roguski**

Two of the most pressing questions concerning international peace and security today are how to avoid an escalation of conflicts in cyberspace and how to ensure responsible behavior and accountability of states in their use of information and communication technologies. With more than thirty states now possessing offensive cyber capabilities[1] and cybersecurity incidents such as Stuxnet, WannaCry, and NotPetya causing significant physical effects or financial damage, there is a clear need to find a better way to manage security risks connected with the use of increasingly sophisticated cyber means by states. At present, this issue is on the agenda of two United Nations groups[2] and is mainly addressed through a "framework for responsible behavior of states" consisting of international law, voluntary and non-binding norms, and confidence-building measures for states' use of information and communication technologies.[3] What the current discussions do not address, however, is whether the security risks could also be regulated through an arms control and inspection regime for cyber weapons. While such a regime has been proposed by scholars,[4] states remain skeptical or even actively opposed to efforts to impose traditional arms control measures on offensive cyber capabilities.[5] This essay examines why a cyber weapons inspection regime is so difficult to devise. It argues that due to their nature and mode of functioning, cyber weapons significantly differ from traditional nuclear, chemical, or biological weapons, such that mechanisms established by traditional arms control treaties either will not work or will not be agreed to by states. Instead, new regulatory approaches are necessary.

* *Lecturer, Chair for Public International Law, Jagiellonian University in Kraków, Poland.*

[1] William C. Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AJIL Unbound 191, 191 (2019).

[2] These are the Group of Governmental Experts, established by G.A. Res. 73/266 (Dec. 22, 2018), and the Open-Ended Working Group, established by G.A. Res. 73/27 (Dec. 5, 2018).

[3] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Transmitted by Note by the Secretary-General, UN Doc. A/70/174 (July 22, 2015) [hereinafter Report of the Group of Governmental Experts].

[4] Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, *in* 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings (Christian Czosseck et al. eds., 2012); Markus Maybaum & Jens Tölle, *Arms Control in Cyberspace – Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods*, *in* 8th International Conference on Cyber Conflict, CyCon 2016 - Proceedings 159-73 (Nikolaos Pissanidis et al. eds., 2016).

[5] Christopher A. Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Remarks at the Center for Strategic and International Studies: Responding to Modern Cyber Threats with Diplomacy and Deterrence (Oct. 19, 2020).

© Przemysław Roguski 2021. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2021.6 Published online by Cambridge University Press

What is a Cyber Weapon?

Officials and researchers give four main reasons for the absence of an arms control regime for cyber weapons: difficulties in defining the weapons due to their intangible character and pace of innovation, their dual-use character, the need for secrecy, and the resulting difficulties in verifying compliance.[6] These unique characteristics, it is argued, make a control regime based on existing models impractical or at least very hard to implement. Indeed, as far back as 2011 the U.S. Department of Defense acknowledged that "[t]he interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains" and that "[t]here is currently no international consensus regarding the definition of a 'cyber weapon.'"[7] No progress has been made in this regard since then, and some authors even propose to "stop using the hackneyed moniker 'cyber weapons' altogether."[8] In consequence, states and authors use broad functional descriptions which put emphasis on the digital nature of the employed means and their destructive or disruptive effects.[9] To understand the challenges posed by cyber weapons to any potential inspection regime, one must first have a sense for how these weapons function.

Cyber weapons consist of lines of code which affect the functioning of the target computer system. They can be conceptualized as essentially consisting of three elements: a propagation method, exploits, and a payload.[10] The propagation method is the means by which code is delivered to the target system. This delivery can be accomplished by remote access, such as by sending an email with an infected attachment; by compromising websites; or by connecting to the target's wi-fi router. It can also be accomplished by direct access, including by establishing a direct connection to the target system through mobile storage devices such as USB drives. Some pieces of malware (e.g., Stuxnet) use more than one propagation method to get to the target system.[11]

After an access route has been established, the next phase of a cyber operation consists of exploiting a vulnerability in the target system to install the payload. Most typically, vulnerabilities in computer systems occur due to unintentional or sometimes intentional flaws in the systems' software or hardware, system features (i.e., intended functionalities which can nevertheless be misused by an attacker), or user error.[12] The exploit itself consists of computer code which is specifically designed to take advantage of a vulnerability to enable the operation of other components of the malware, such as the payload or further propagation methods.

Finally, the payload denotes computer code which is executed on the target system to achieve the attacker's intended goal.[13] The effects of the payload depend on a range of factors: the nature of the target, the technical

[6] Erica Borghard & Shawn Lonergan, *Why Are There No Cyber Arms Control Agreements?*, Council on Foreign Relations (2018); Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Remarks at the European Union Conference on Nonproliferation: Rules, Norms, and Community: Arms Control Discourses in a Changing World (Dec. 13, 2019).

[7] U.S. Dep't of Defense, Department of Defense Cyber Policy Report 8 (2011).

[8] Thomas Rid, Cyber War Will Not Take Place 188 (2017).

[9] *See, e.g.*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 452 (Michael N. Schmitt & Liis Vihul eds., 2017) (stating that "cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects"); Ministère des Armées, International Law Applied to Operations in Cyberspace 18 (2019) (defining a "cyber weapon" as a "[d]igital capability(ies), including digital warfare weapons, resources and methods, used in a cyber-operation against the adversary in and in connection with an armed conflict situation").

[10] Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model*, 8 J. Nat'l Sec. L. & Pol'y 301, 303 (2016).

[11] Nicolas Falliere et al., W32.Stuxnet Dossier, Symantec-Security Response (2011).

[12] Nat'l Cyber Security Ctr., *Understanding Vulnerabilities* (Oct. 14, 2015).

[13] Australian Cyber Security Ctr., *Glossary – Payload*.

https://doi.org/10.1017/aju.2021.6 Published online by Cambridge University Press

skills and capabilities of the attacker, and the attacker's intentions. They can range from exfiltration of data for espionage purposes; to alteration, encryption, or destruction of data as in the cases of WannaCry and NotPetya; to alteration of the functioning of the attacked computer to cause secondary effects on systems or processes controlled by that computer, as in the case of Stuxnet.

Analogies to Established Arms Control Regimes Do Not Fit

With this short description, the difficulties in copying existing arms control regimes for use against cyber weapons become apparent. One issue is that there is no single cyber-weapon-specific propagation method which could be regulated through a limitation regime (such as the Strategic Arms Reduction Treaties). Propagation methods are often adjusted to the nature of the target and the identified vulnerability. For instance, in the case of the SolarWinds supply-chain attack, attackers gained access to the source code of a widely used network management system, and the infected software was distributed to the target via the software vendor's update servers.[14] But in the case of Stuxnet, the attackers first infected the private computer of a Natanz nuclear facility employee through phishing emails and then made sure that the malware was carried onto the target system by the unsuspecting employee on a USB drive.[15] Moreover, as becomes clear from these examples, most propagation methods are dual-use, so any limitation regime could also potentially affect non-military uses of information and communication technologies.

One conceivable angle for regulation could be the exploit element of a cyber weapon. Indeed, the Wassenaar Arrangement,[16] which is a multilateral export control regime, currently puts controls on exports of "intrusion software," which it defines as "'software' specially designed or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device" and performing either "extraction of data" or "modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions."[17] If "avoiding detection" and "defeating protective countermeasures" are sufficient descriptions of software for the purposes of export controls, one might argue that the Wassennaar Arrangement could serve as a model for a cyber-arms control regime. However, while states may want to control and limit the proliferation of intrusion software through an export control regime for security and human rights purposes, the same security needs are likely to reduce states' willingness to agree to a limitation and inspection regime for cyber weapons based on their intrusive properties. This is because states rely on exploiting vulnerabilities in computer systems to gain access for law enforcement or intelligence purposes.[18] Any control regime would therefore need to take account of the fact that the existence of a cyber weapon is not determined by the exploit used. The regime would also need to recognize that the stockpiling and use of vulnerabilities by governments may serve legitimate national security interests.

The tension between achieving greater security through a limitation of intrusion opportunities and the need to retain capabilities to exploit systems' vulnerabilities for national security purposes is best demonstrated by the discussion about vulnerability disclosure—i.e., the reporting of security flaws in computer software or hardware to vendors or developers. On the one hand, disclosing vulnerabilities increases cybersecurity because it reduces the

[14] Jake Williams, *What You Need to Know About the SolarWinds Supply-Chain Attack,* SANS Blog (Dec. 15 2020).

[15] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012).

[16] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Initial Elements as adopted by the Plenary of 11 - 12 July 1996 [hereinafter Wassenaar Arrangement].

[17] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, Cat 4 5P2, WA-LIST (19) 1, 223.

[18] Mimasa Ambashta, *Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications*, Berkeley Tech. L.J. Blog (Apr. 22, 2019).

https://doi.org/10.1017/aju.2021.6 Published online by Cambridge University Press

potential for malicious actors to exploit a weakness in a system. On the other hand, even states which have implemented vulnerability disclosure policies[19] nevertheless report only around 90 percent of the discovered vulnerabilities,[20] with the rest presumably stockpiled for national security purposes. This seems unlikely to change, given that state officials have described calls for immediate disclosure of vulnerabilities as "tantamount to unilateral disarmament."[21]

The reason for this perception is twofold. First, although vulnerability disclosure is a norm of responsible behavior[22] that states have agreed to be guided by, there is currently a lack of transparency with regard to vulnerability disclosure practices of major cyber powers such as Russia and China as well as other states, which results in a lack of trust. Second, and more importantly, the functioning of cyber tools which are based on intrusion into computer systems is dependent on the presence of an exploitable vulnerability in the target system. Once a vulnerability is disclosed, it gets patched, rendering useless any cyber tools that exploited it. Therefore, the effectiveness of any cyber weapon (or software used for espionage or law enforcement purposes) depends on its secrecy. This applies not only to the exploit element of a cyber tool, but also to its payload.

And herein lies the main problem with any cyber weapons control and inspection regime: even if states manage to agree on what constitutes a cyber weapon and on which cyber weapons are to be subjected to a control regime, verification of compliance through inspections would pose the risk of compromising their function. Inspecting a cyber weapon would require inspecting its code. But once the code is known, other states can effectively protect against it by patching their systems and updating their malware detection software, thus rendering the weapon useless.

Moreover, unlike traditional weapons systems which are quantifiable and usually accessible either to observation from space or to inspections of specialized production and storage facilities, cyber weapons, like any other computer code, are intangible and can be easily copied, stored, and transported. Thus, on-site inspections would require access not only to particular sites, but to the entire governmental network, which no state would accept.

Is There a Way Forward?

Given that traditional arms control mechanisms appear ill-suited to tackle the challenges posed by cyber weapons, the key question is whether there are other ways to create transparency with respect to the proper implementation of mechanisms devised to reduce risks, and to build confidence in parties' willingness to comply with those mechanisms.[23]

The current approach to tackling these challenges consists of two prongs: one normative and the other responsive-deterrent.[24] The normative prong aims at the promotion of rules of responsible behavior in cyberspace, mainly through clarifying how international law applies to cyber conduct as well as building new norms of responsible behavior. This first prong is pursued by two UN bodies: the Group of Governmental Experts and the

[19] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, Binding Operational Directive 20-01 (Sept. 2, 2020).

[20] *Cybersecurity, Encryption and United States National Security Matters: Hearing Before the S. Comm. on Armed Services*, 114th Cong. 60 (2016) (statement of Admiral Michael S. Rogers, Commander, United States Cyber Command).

[21] Rob Joyce, White House Cybersecurity Coordinator, Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do (Nov. 15, 2017).

[22] Report of the Group of Governmental Experts, *supra* note 3, at para. 13(j).

[23] Stefan Oeter, *Inspection in International Law: Monitoring Compliance and the Problem of Implementation in International Law*, 28 NETH. Y.B. INT'L L. 101, 107 (2009).

[24] Christopher A. Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, *International Security in Cyberspace: New Models for Reducing Risk*, I(20) ARMS CONTROL & INTERNATIONAL SECURITY PAPERS (Oct. 20, 2020).

https://doi.org/10.1017/aju.2021.6 Published online by Cambridge University Press

Open-Ended Working Group.[25] The second prong aims at enforcing the rules of responsible behavior, primarily through public attribution of cyber operations[26] and sanctions.[27]

This two-pronged approach should be further pursued and improved to root out inherent weaknesses and inconsistencies and strengthen implementation. With respect to the normative prong, the promotion of rules of responsible behavior in cyberspace requires that rules are known, understood, and observed. To this end, the currently voluntary practice of publishing views on how international law applies to cyber operations should be further expanded, including by requiring states to report their views to the UN Secretary-General. Established cyber powers and like-minded states could aid this endeavor by increasing capacity-building efforts and engagement with countries which have a poorer understanding of cyber issues. Furthermore, cyber powers should lead by example and avoid inconsistencies or gaps in their own positions. For instance, the view that non-consensual cyber intrusions in foreign networks do not violate international law if they do not produce significant adverse effects[28] should be re-evaluated, given that it may lead to situations where large-scale cyber operations such as the recent SolarWinds hack are not regulated at all. Establishing cyber-specific rules on vulnerability disclosure, supply-chain integrity, and cooperation through a duty of "cyber due diligence"[29] would also improve the current framework.

For its part, the responsive-deterrent prong so far exhibits only limited influence on adversaries' behavior. While states must be able to individually or collectively counter adverse cyber operations, unilateral strategies which do not take into account other cyber powers' threat perceptions or military calculus may not solve the problem. Although difficult to implement in the current climate, international review, reporting, and follow-up mechanisms based at international institutions could help to build confidence between adversaries.

Lastly, states can reduce the threat posed by the offensive use of cyber weapons through strengthening cybersecurity and increasing cooperation with the private sector.[30] After all, as shown above, malicious cyber operations using sophisticated cyber weapons rely on vulnerabilities in commercial software products. Improving cybersecurity for critical infrastructure through better coordination, incident reporting, vulnerability sharing, and a cybersecurity-minded management culture would not totally eliminate malicious cyber operations. It may, however, make those operations more costly and difficult for the attacker.

Conclusion

Simply copying established models, such as arms control mechanisms created for conventional weapons, is unlikely to significantly reduce the threat of adversaries' use of cyber weapons. Nevertheless, current regulatory approaches can be improved by furthering a common understanding of how international law applies in cyberspace; establishing rules on vulnerability disclosure, notification, and cooperation requirements for cyber incidents; and creating international review and enforcement mechanisms. In addition, states and private actors should cooperate to strengthen the cybersecurity of critical systems, thereby reducing the effectiveness of cyber weapons and increasing the cost of developing them. Certainly, as SolarWinds has shown, there is much room for improvement in this regard.

[25] *Supra* note 2.

[26] Florian Egloff, *Public Attribution of Cyber Incidents,* 6 J. Cybersecurity 1 (2020).

[27] *See, e.g.*, Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States, 2019 O.J. (LI 129/1) 1-12.

[28] Paul. C. Ney, DoD General Counsel, Remarks at U.S. Cyber Command Legal Conference (Mar. 3, 2020).

[29] *E.g.*, Antonio Coco & Talita de Souza Dias, *Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the COVID-19 Pandemic*, 11 J. Int'l Humanitarian Legal Stud. 218 (2020).

[30] *See, e.g.*, Brad Smith, Microsoft President, *A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response*, Microsoft Blog (Dec. 17, 2020).

https://doi.org/10.1017/aju.2021.6 Published online by Cambridge University Press