AARMS Vol. 15, No. 1 (2016) 61–73.

Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions

Dóra DÉVAI[1]

The development, acquisition and deployment of cyber weapons is becoming a routine activity of national military and law enforcement communities. This leads to a demand to introduce new strategic and regulatory regimes based on solid legal and policy structures. However, technical and legal experts face several complications when trying to meet these demands. The article gives a cursory overview of the particular difficulties and potential pathways to a solution with regard to cyber weapons use. Special attention is devoted to the international efforts involving Hungary.

Keywords: *legal review, arms race, cyber arms control*

Introduction

Since the early years of 2010s, nation states have been increasingly open about exploiting the strategic advantages of cyberspace as a domain of national interest. Facilitating the digitalization of the economy and commerce, the operation of public infrastructures and services have been integrated into national development policies. As a result, increasing volume of valuable assets are reachable in or through cyberspace. This also means that these are up for grabs and national governments are obliged to provide for some means of protection. Cyber weapons, most basically software technology, enable a wide variety of actors to fulfil both kind of efforts and therefore their role has undeniably risen recently. Nation states need to find solutions for how to integrate cyber weapons into their strategic arsenal, while they also have to install mechanisms to limit the detrimental and damaging impacts of cyber weapons used against them.

Difficulties start not only at the technical detection and elimination of malware from cybered systems, but also at how to analyze, understand, designate and regulate all these control mechanisms. In parallel, the legal expert communities have devoted more and more attention to the legal definition and the lawful applicability of cyber weapons, especially in the context of international conflicts. All these current trends illustrate a large scale overall process of strategic thinking and nascent norm building in regulating nation state use of cyber weapons.

Despite the greater willingness of experts and decision makers to openly discuss the use of cyber weapons, with regard to the inherent national security sensitivity, abundant authoritative data is still hard to come by. Major differences linger between and often within particular security communities. Cybersecurity and cyber strategic thinking is in a nascent phase, according to security and strategic studies researchers, this area is at a pre-strategic stage.

[1] E-mail: thedevai@gmail.com

This article is not an in-depth analysis of strategic cyber issue areas. By giving a brief introduction into the evolution and the proliferation of cyber weapons, the article rather seeks to illustrate that one of the consequences is a shift towards offensive strategic thinking and an increasing risk of conflict in cyberspace. Consequently, it is necessary to develop a more profound understanding and transition between the foundational technical, legal and strategic approaches of cyber weapons and force development. This is the first step towards building national military cyber strategies without upsetting international strategic stability. Through the eye of the strategist, one fundamental question is whether traditional strategic concepts and strategies can be applied in cyberspace. Following this deductive logic, these concepts in cyberspace seem to have limited applicability in cyberspace. Thinking inductively, a more viable option is the integration of the expertise of the technical epistemic community. Finally, without in-depth analysis, this integrative methodology seeks to demonstrate the interplay between the motivation, opportunities and limitation of nation states when drawing up strategy in cyberspace.

Hungary like every country is concerned in cybersecurity. This article also aims to link relevant Hungarian academic, institutional or strategic developments to this general strategic approach discussion of cyber weapons.

The first part starts out with the technical approach to cyber weapons by explaining why even those aware of all the technical intricacies are often of different opinion. Next, some of those comprehension problems are examined that arise when it comes to the legal definition and regulation of the use of cyber weapons. In the third section, the historical context of cyber capability evolution is introduced, followed by the strategic consequences thereby induced. The last part outlines the emerging international efforts into dealing with these strategic challenges by applying the existing arms control mechanisms or strategic application of technical mechanism.

Defining Cyber Weapons. Technical Aspects

As of today, there is no consensus as to what constitutes a cyber weapon or cyber weapons system, however, this is not unique to cyberspace. Many analysts agree that much of the confusion is due to two rudimentary facts. First is the lack of a generic definition of kinetic weapons in military strategies or legal codes. By default, the emerging conceptual approach applied in cyber weapon debates is a functional one, cyber weapon is any software component *used or designed to do harm*. This line of argument will be continued in the section on legal issues. As an illustration, an often cited example conceived by a legal expert at the Italian Ministry of Defense shows this trend: "… [an] *appliance, device or any set of computer instructions* designed to unlawfully damage a computer or telecommunications system having the nature of critical infrastructure, its information, data or programs contained therein or pertaining there to, or to facilitate the interruption, total or partial, or alteration of its operation." [1: 22]

The other source of confusion when defining cyber weapons is that the terminology and concepts used in cyber weapon discourse are directly taken over from strategic thinking based on conventional weapons or weapons of mass destruction. When it comes to cyberspace, though, these analogies are dysfunctional at several points. Terms used in legal and policy paradigms like "war", "weapon" and "destruction", "attack" or "deterrence" play out differently in cyberspace. Moreover, the usage of these terms is wide ranging and unconsolidated. For example, the term "cyber warfare" is used to describe the use of the cyber domain to conduct military operations ranging from the cyber equivalent of logistical convoys to the delivery of violent military attacks. [2]

Alternatively, as malware analysis methodology becomes increasingly sophisticated, a narrower and more bottom-up technical and thus more factual approach might take the place of business as usual strategy formation. Dorothy Denning from the Naval Postgraduate School, one of the hubs of cyber strategic thinking, was among the first discussants from the technical community who called attention to the wider national security implications of cyber technology. Her cyber weapon classification is focused more narrowly on the type of malware and what it is used for. Denning distinguishes between offense-only cyber weapons that are *used* only for the purpose of attack or to cause harm, defensive weapons that are used primarily to protect against such attacks, and dual-use weapons that are used for both offense and defense. The first category includes most computer viruses and worms; Trojan horses; e-mail bombs; denial-of-service tools; exploit scripts and programs that take advantage of vulnerabilities such as buffer overflows to gain access; rootkits with Trojan system utilities, backdoors, and system log cleaners to cover tracks; and copyright crackers. Defensive cyber weapons comprise encryption, authentication, access controls, firewalls, anti-viral software, audit tools, and intrusion detection systems. She mentions some dual-use and defensive weapons such as supercomputers, encryption devices, TEMPEST, and stealth technology. [3] This differentiation, however, can be misleading and indeed highly challenging as many technologies can be characterized as dual-use, for example, penetration testing methods and exploits are used as defensive weapons too, or non-malicious code is easily converted into weapons through minimal change. In addition, cutting-edge cyber weapons are composed of several different kinds of combination of the above mentioned components.

What proves to provide more clarity as of the nature and potential division of cyber weapons comes from an increasing number of technical research based on advanced malware analysis. These research explore the construction and behavior of malicious software. The rationale behind this approach is the possibility to recognize typical patterns providing information about the identity and motivation of the perpetrators. The following modular division well reflects this approach: "A Propagation Method (Pr) is the means by which malware is inserted into a target network or system, such as an infected USB stick or email carrying a compromised attachment. An Exploit is code designed to compromise some aspect of a software system which allows third parties to effect unintended operations or consequences. A Payload is the code with a malicious purpose whose delivery and execution are the goals of any piece of malware." [4: 1]

A cyber weapon is the combination of these three elements designed to create destructive physical or *digital effects*. According to this research, as the core functionality of the code is linked to the payload designed to create digital or physical effect, the payload determines the category of the cyber weapon.

"This modular approach to understanding threat software reveals a promising correlation between highly targeted tools (such as Stuxnet) and comparatively simple malware used for bank fraud that might prove useful to both the policy and research communities." [4: 1]

The following table is taken from a legal study and besides accurately depicting the software components of malware, also serves the purpose of highlighting the fundamentally divergent legal and technical analytical approaches. [2]

Table 1. Illustrative examples of technical functional analysis of two cyber weapons. [2]

CYBER WEAPON	TECHNICAL CHARACTERISTICS
ZeuS Trojan ZeuS Trojan is the name given to a family of popular (with cyber criminals) software programs that are part of the larger body of “malware.” While computer viruses are generally considered to be malicious software that disrupts the functions of a system, the ZeuS Trojan, like most Trojans, is configured to operate unobtrusively in the background of a system, where it intercepts banking transactions.	Installable program usually spread by phishing and website compromises. Works as a “man-in-the-middle” keystroke logger and form interceptor. Preconfigured to recognize user access to banking or other websites. Reports the user’s log-in information (in real time) to a contral controller. Also allows for remote updating and execution of downloaded code.
Poison Ivy A “remote access tool” or “RAT,” is a software application that allows a remote user to interact with a computer system as if the operator had physical access to the system. Poison Ivy is similar to the ZeuS Trojan, but has broader applicability as a general purpose “remote access tool” that is freely available on the Internet. It has primarily been designed as a low footprint tool that can be later configured by downloading modules to the client.	Free-ware distributed from an official website. Operates as “client-server” that allows control of a system by a remote operator. Capabilities include: Encrypted communication; Remote file browsing; Process injection; Key logging; Registry manipulation; Screen capture; Audio and video capture; Password stealing.; Proxy services. Payloads customizable by users The code required for initial compromise is very small. 10 kilobytes, but once loaded, individual components may be added depending on user requirements**.**

Another line of differentiation is between cyber espionage and cyber-attacks. Despite the technical similarity between the propagation method and the exploit used for espionage and offensive cyber-attack, most US scholarly and policy sources deny that espionage tools are weapons. It shows a fundamentally different strategic and policy attitude, most probably owning to the fact, that the US possesses the most advanced cyber espionage tools and it is intent on preserving the widest possible space to maneuver. European literature tend to be more sensitive towards espionage. Karlis Podins Lithuanian and Christian Czosseck German scholars define a cyber weapon as: “Data and knowledge that is capable of, designed to and executed with the intention to affect the integrity, availability *and/or confidentiality* of an IT system (target) without its owner’s approval. The target’s defense is overcome by abusing existing vulnerabilities in the target.” [5: 3]

Reviewing the Hungarian academic literature on cyber weapons, both the technical details and the strategic significance of cyber-attacks have been analyzed thoroughly. Extensive legal analysis is still lacking though. Just to mention a few examples, CrySyS Lab the Hungarian academic research institute has become internationally renowned by first reverse engineering the Duqu malware. [6] The notion of cyber terrorism and its information technology arsenal are discussed, [7] as well as the probable tools and tactics used in a complex cyber-attack against Hungary. [8]

Legal Considerations

A previous chapter in the history of cyber weapon regulation goes back to the end of the 1990s, the first time when transboundary regulations concerning cyber capabilities were attempted to be introduced. The demand and debate materialized in several different areas. For example, the export controls regime of dual use technologies in in the US, dubbed ‘crypto wars’. In the field of international nonproliferation law, Russia presented its initiative in the UN General Assembly First Committee in October 1998 calling for states to share their views regarding the “advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons.” [10: 48] The Council of Europe in Strasbourg raised the possibility of limited cyber weapons controls in their draft Cyber Crime Convention. The so-called Budapest Convention obliges States to penalize offenses against the confidentiality, integrity and availability (CIA) of computer data and systems. The production, distribution, and possession of computer programs with which CIA-offenses could be committed would also be illegal under certain conditions. [3] The Cyber Crime Convention treats cyber weapons as a criminal issue, therefore falls beyond scope of the current analysis.

The legal procedure including the definition, categorization and use of cyber weapons is particularly problematic in military issues. The fast-changing nature and diversity of cyber weapons render any legal review based on the enumeration of weapons useless. Nevertheless, militaries keep listing concrete capabilities under the heading of cyber weapons. For a number of other reasons too, military legal experts are in a particularly difficult situation when they have to provide legal advice in concrete cases. Without going into elaborate legalistic analysis, in the case of the law of weaponry, the fundamental referent point on the development, acquisition and use of weapon systems is rooted in the Hague Convention (IV), 1907, in particular Article 22 of its annexed regulations, which states that the “right of belligerents to adopt means of injuring the enemy is not unlimited.” Article 36 of the 1977 Additional Protocol I to the Geneva Conventions of 1949 (API) codifies the requirement to conduct legal reviews of all new weapons.[2] The other legal track derives from *jus ad bellum* and relates to use of force, however, it is beyond the scope of this article. [1] Moreover, military cyberspace operations raise the mixed issues of geography, sovereignty, criminal law, and civil rights. According to *jus in bello* criteria and the general principles of war,[3] legal advisers review weapons of war and the application of those instruments in order to ensure there will be no disproportionate negative effect on the civilian population and property, or unnecessary suffering to combatants. [1] When using cyber weapons, targeting, distinction, proportionality and neutrality are particularly difficult issues. In the Manual cyber weapons are defined restricted to malware that can cause destructive physical effect, excluding damage done to data: “cyber means of warfare that are by design, use, or intended use, capable of causing either injury to, or death of, persons. The “Methods” of cyber warfare are the cyber tactics, techniques and procedures, by which hostilities are conducted.” [9: 141]

[2] The United States is not a party to AP I, it does conduct legal reviews is consistent with the AP I requirement since 1974. [2]

[3] Military necessity, distinction, proportionality, unnecessary suffering, perfidy, neutrality.

According to some experts, similarly to the technical approach the confusion arises from the attempts to define and regulate cyber weapons based on the analogy of kinetic weapon systems. It is difficult to identify the "entity" that would be characterized as a weapon. [1] Legal expert Louise Arimatsu gives a concise summary of the problem. "A weapon is generally understood as a device that is 'designed to kill, injure, or disable people, or to damage or destroy property." [13] Although this definition might adequately encapsulate traditional weapons that have been designed, when utilized, to have a direct kinetic outcome, it fails to capture the essence of what are generally regarded as cyber-weapons. This is because most of the malicious codes or malware that would fall within the parameters of a cyber-weapon are designed to have an indirect kinetic outcome which may, or may not, result in the listed outcomes. In other words, the malware itself is not designed to kill, injure or disable people nor, necessarily, to damage or destroy tangible property." [12: 97]

The other common point of reference in legal argumentation is the effect a malicious code is designed to produce as a basis for judgement. This approach transpires throughout the Tallin Manual in discussing whether cyber-attacks in general fall under the purview of the Law of War. In summary, it is both the offensive capability of the code and the desired effect that can determine if a cyber capability can be considered as a weapon, and thus whether its deployment is permissible or not according to the Law of War.

Proliferation of Cyber Weapons

Surveying the publicly available US secret service Congressional hearings since the mid-1990s reveals that the development and stockpiling of cyber weapons by certain nation states have proved to be a recurring national security threat indicator. [13] By 2007, for example, there were an estimated 120 countries working on cyber-attack commands, and in it was also predicted that on 10 to 20 years countries would be "jostling for cyber supremacy." [14: 123] Experts trace the evolution of cyber capabilities developed by major militaries back at least as early as the 1940s, though the nature of the attempts to penetrate computers and computer networks could be both defensive and offensive. In the 1960s, security analysts in the US Department of Defense developed a professional understanding of computer penetration by analyzing the security of the nation's time-sharing computer systems. In the course of time, this ability to detect the vulnerabilities of one's own computer systems has been turned into an offensive weapon system. [15] According to the one of the most often cited inventories of national cyber capabilities on the level of policy, doctrine and organization the number of these states, based on publicly available information back in 2013, was 18 in Africa, 16 in the Americas, 39 in Asia, 38 states in Europe, and 3 in Oceania. (Table 2) [16] It is important to note, however, that this data set is insufficient to paint an authoritative picture as the nature and maturity of these programs vary greatly by country.

Table 2. The number of countries possessing cyber capabilities in 2015. [13]
(Edited by the author.)

CONTINENT	**COUNTRIES WITH MILITARY CYBER DOCTRINE, POLICIES OR ORGANIZATION**	**COUNTRIES WITH CIVILIAN CYBER DOCTRINE, POLICIES OR ORGANIZATION**
Europe	Albania, Austria, Belarus, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Norway, Poland, Russian Federation, Slovakia, Spain, Switzerland, Ukraine, United Kingdom	Belgium, Bulgaria, Czech Republic, Iceland, Ireland, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Portugal, Republic of Moldova, Romania, Serbia, Slovenia, Sweden
Asia	China, Democratic People's Republic of Korea, Georgia, Indian, Indonesia, Iran (Islamic Republic of Iran), Israel, Japan, Kazakhstan, Malaysia, Myanmar, Republic of Korea, Singapore, Sri Lanka, Syrian Arab Republic, Thailand, Turkey, Singapore, Sri Lanka, Syrian Arab Republic, Thailand, Turkey, Viet Nam, Yemen	Afghanistan, Armenia, Azerbaijan, Bangladesh, Bhutan, Brunei Darussalam, Cambodia, Cyprus, Jordan, Kuwait, Lebanon, Maldives, Mongolia, Nepal, Oman, Pakistan, Philippines, Qatar, Saudi Arabia, United Arab Emirates
Africa	South Africa	Burundi, Cameroon, Egypt, Ethiopia, Ghana, Kenya, Madagascar, Mauritius, Morocco, Nigeria, Rwanda, Sudan, Swaziland, Tunisia, Uganda, United Republic of Tanzania, and Zimbabwe
Americas	Argentina, Brazil, Canada, Colombia, Cuba, United States	Antigua and Barbuda, Dominican Republic, Grenada, Jamaica, Mexico, Panama, Peru, Saint Vincent and the Grenadines, Trinidad and Tobago, Uruguay
Oceania	Australia, Fiji, New Zealand	

Stuxnet malware brought on a tectonic shift in cyber strategic thinking. There is little dissent among information security and industrial control system engineers on the breakthrough value of the complexity and the sophistication of the malware, as well as the fact that a cyber-attack caused physical destruction. [17] Iran's nuclear power plant capacities are directly related to its weapons potential, thus such intervention has strategic implications, and count as coercion against the country. Yet the appraisal of the strategic value of the Stuxnet attack is far from unanimous. Most critiques question the strategic degree of the physical damage and disruption, and its impact on the Iran's overall nuclear policy and international negotiation position. On the other hand, Martin Libicki pointed out the significance of Stuxnet from the wider strategic policy, namely the deterrence value of the attack. According to journalistic assertions, the attack was implemented by nation states, most probably the US and Israel, thus fulfilling two of the fundamental building blocks of retaliatory deterrence, the level of a nation's capabilities and its determination to use them.

Stuxnet attack has been a unique occurrence so far, at least based on publicly available documents. Another type of cyber weapon, nonetheless, has been detected at mass level. The so called Advanced Persistent Threats (APT) is difficult to detect, still since 2010 a growing number of APTs have been detected. There are several definitions of APT.

"Advanced: The hacker has the ability to evade detection and the capability to gain and maintain access to well protected networks and sensitive information contained within them. The hacker is generally adaptive and well resourced. Persistent: The persistent nature of the threat makes it difficult to prevent access to your computer network and, once the threat actor has successfully gained access to your network it is very difficult to remove. Threat: The hacker has not only the intent but also the capability to gain access to sensitive information stored electronically." [18: 1]

Considering the skills necessary to design, implant and maintain such a malware, along with the nature and volume of information so vacuumed from targeted information systems, ATPs can be considered of strategic significance, though not through its destructive capacity.

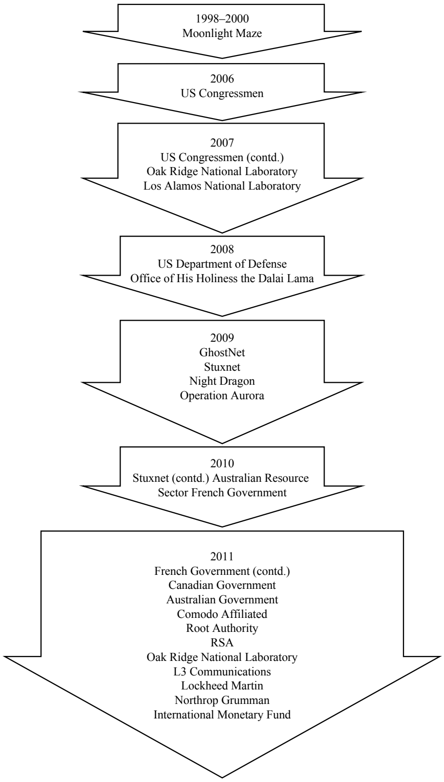

Figure 1. Major ATPs revealed. [18: 3]

The by now canonized list of illustrative cyberattacks on national critical infrastructures well demonstrates that cyber weapons are being deployed with ever growing audacity. This tendency is followed suit by the ever increasing stage of cyber capability development and doctrinal evolution of the defense policy of the countries concerned.

Over the past three years, through a multi-thronged development process the superior US cyber capabilities have been firmly established and integrated with other joint capabilities along the services and the reserve components. Just to highlight one momentous example, the Defense Advanced Research Projects Agency (DARPA), the Pentagon's main research and development organization launched a five-year, $500 million budget research plan to boost research into offensive cyber tools. [19] As Kaigham J. Gabriel, DARPA deputy director testified in 2012 "We need cyber options that can be executed at the speed, scale and pace" of other military weapons. [20: 8]

This new operational stage has been consolidated by the Department of Defense Cyber Strategy published in April 2015, and most recently, by the Department of Defense Law of War Manual issued in June 2015. The Manual focuses on *jus in bello*, law relating to the conduct of hostilities and the protection of war victims that is applicable to the United States, including treaties to which the United States is a Party, and applicable customary international law. [21] The document assesses law of war publications issued hitherto by different services within the military, as well as including conclusions based on consultation with allied nations' legal experts, and is serves as a DoD-wide resource for DoD personnel. As for cyber operations, the U.S. armed forces "are developing tools and capabilities' necessary to carry out its missions set forth in the latest DoD cyber strategy consistent with U.S. and international law." [22] Assessing the overall development in US military doctrines pertaining to cyber weapons, there is a shift towards the openly declared operational use of offensive cyber weapons, accepting even possibly lethal collateral damage, though with the intention and ability to try and keep unnecessary damage rate to the lowest possible level.

Strategic Implications

The strategic aim of the US technical and cyber capability development is declaratively to maintain its superior position vis-a-vis its peer competitors, mainly China and Russia. In terms of cyber weapons, however, relative capability positioning is not so obvious primarily for two reasons. It is common place that the more the number and complexity of computing devices applied, the more exploitable vulnerabilities exist in a system, which makes these inherently vulnerable systems extremely difficult and expensive to defend. The central strategic and policy model of deterrence by punishment as it is known from nuclear strategies is impossible to apply due to the nearly impossible task to unambiguously identify the culprits behind a cyber-attack. In sum, all these strategic determinants of the cyber environment contribute to the belief, mainly prevailing among major powers, that the volume and cutting-edge quality of cyber capabilities is necessary to deter cyber-attacks. By nature, the efficiency of cyber weapons is transitory, and the exploits of any cyber weapon are very specific to a system configuration. Hidden culpability as well as the relatively low costs and short time span demanded by cyber capability development all act as incentives to accumulate a stock of cyber weapons as extensive as possible. The escalatory nature of cyber conflicts became part of the emerging corpus of cyber security strategy literature.

Cybersecurity experts also point out that in terms of action-reaction cycle an arms race is also taking place between non-state malicious hackers and IT security experts. Although among traditional strategists there is no consensus, whether the classic theory of security dilemma is applicable, it is easy to recognize that cyber arms race is almost inevitable for several different reasons. As a result, the exchange of exploits through illegal markets has boomed over the last five-ten years. Illegal exploit research and selling have become lucrative business, nonetheless these mechanisms are shrouded by intractability. What makes matters even more complicated is that in certain aspects, nation states' interests lie more in preserving this fuzziness than bringing transparency and legal clarity. No wonder, that these phenomena alarm a wide variety of different communities ranging from IT security specialists and human rights activists to legal experts and national decision makers. With regard to such a wide range of interests, it is not easy to find optimal solutions.

Arms Control Approach

The discovery of Stuxnet malware and the frustrating results of deterrence strategy options also inspired further potential arms control and regulatory discussions. As already mentioned above, initiatives to restrict the development and acquisition of cyber weapons appeared at the end of the 1990s. Although the Russian proposals were refused by US delegates in the First Committee of the UN General Assembly (UNGA), the wording and content of the proposal got gradually modified, and under the title "Developments in the field of information and telecommunication in the context of security". With gradual changes, the non-binding resolution has been adopted by the UN General Assembly each year. In the resolution of 2001, Russia requested the establishment of a group of governmental experts (GGE) for a study to discuss possible cooperation measures. The second GGE was able to produce a consensus which highlighted the need to continue discussing further *norms* to address existing and potential threats in the sphere of information security. Norms here are meant to be gradually evolving voluntary patterns, though the ultimate Russian ambition is still to establish a binding treaty banning the development, production and use of particularly dangerous information weapons.

Based on the GGE report endorsed by the UNGA, the promotion of cyber security Confidence Building Measures (CBMs) entered the agenda of the regional organizations like the Organization for Security and Co-operation in Europe (OSCE) and Association of Southeast Asian Nations (ASEAN). The package of measures accepted so far are voluntarily carried out by participating states, and they are built around transparency of nation cyber security measures, and the establishment of bilateral and multilateral points of contact.

Policy and legal experts are highly skeptical about the feasibility of cyber arms control treaties. Beyond the ambiguities mentioned in the first part, enforceability, verification and rapid technological change are the most often cited reasons. The evaluation of arms control and disarmament regimes introduced into cyberspace has been given more attention recently. The Biological Weapons Convention and Chemical Weapons Convention are studied in search of useful analogies and lessons learnt. Arimatsu argues that the parties' motivation is different in arms control regimes from that of the Laws of War. In the previous case states are willing to restrain their capabilities in order to achieve military balance, while in the latter, the aim is to reduce the human suffering and unnecessary damage. [15] As the political and strategic climate change, states' political inclination might shift as well, as the precedent of earlier arms control regimes show.

There is also some progress in the regulatory regimes of cyber weapons, though its efficacy is highly controversial. Export controls on encryption stem from agreements made under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods Technologies. The recent round of agreement materialized in December 2013, when the 41 member states including Hungary and Russia, but not China, agreed on principles to control the export of software that can be used for surveillance. The motivation partly serves human rights by limiting the abuse of surveillance technologies produced in developed countries, and partly strategic to enhance the security of the producing countries by reducing the rate of surveillance technology used to spy on them. The agreement does not use the term cyber weapon, but the overly broad expression of "intrusion software," which is defined as "software that is capable of extracting or modifying data or modifying the standard execution path of software in order to allow the execution of externally provided instructions". It also concerns the cross-border use of technology used by the security research and practitioner communities.

Finally, responsible disclosure policy might offer strategic stability at national and international level. According to expert literature, ethical hacking is the earliest example of responsible disclosure. Offering bug bounty by software and hardware is becoming more common, but its amount often lag behind the price offered by nation states or criminals at hidden exploit market outlets. A new concept of coordinated vulnerability disclosure is gaining ground at governmental level. The Netherlands, for example, have launched a disclosure policy on websites of the Dutch central government. [23] International co-operation mechanisms have started to build around the same idea. In April 2015, at the Global Conference on Cyberspace in The Hague, Romania, the Netherlands, Hungary, and Hewlett Packard initiated a voluntary cooperation mechanism under the name Responsible Disclosure Initiative (Ethical Hacking). The cooperation works within the framework of Global Forum on Cyber Expertise, and it is open for others to join. The objective is to share experiences and lessons learned in cyber security mechanisms for responsible disclosure or coordinated vulnerability disclosure policies and discussions on the broader topic of ethical hacking.

Conclusion

Stakeholders are much more open about their cyber capabilities and strategic intentions and vulnerabilities in cyberspace. Cyber-attacks have become part of the national security agenda, which requires new and effective system-level answers, necessitating more transparency and co-operation, even self-restraint in using the available cyber weapons. Nevertheless, the cyber ability to develop or acquire cyber weapons is a strategic asset, the strategic insight and maturity on how to use these weapons is still wanting. The current period is often compared to the pre-strategic era of nuclear weapons between the 1940s and 1960s. Trust is lacking between nation states, or even between different national security communities within national borders. Strategists need to conceive how to balance the different interests on their national foreign and security agenda in an environment fraught with so far unseen technical complexities, existing legal paradigms are obsolete, and due to attribution difficulties the perpetrators are unidentifiable. Decision makers need to work out the trade-offs that best serve the overall national strategic framework. In conclusion, much more cooperative technical, legal and political-military analysis is necessary to achieve a higher level of strategic maturity both in deploying cyber weapons and in developing security strategies against their use.

References

[1] MELE, S.: *Cyber-weapons: legal and strategic aspects version 2.0.* Rome: Italian Institute of Strategic Studies “Niccolo Machiavelli”, 2013.

[2] BROWN, G. D., METCALF, A. O.: Easier Said Than Done. Legal Review of Cyber Weapons. *Journal of National Security Law and Policy*, 7 (2014), 115–138.

[3] DENNING, D. E.: Reflections on Cyberweapons Controls. *Computer Security Journal*, XVI 4 (2000), 43–53.

[4] HERR, T.: *PrEP: A Framework for Malware & Cyber Weapons.* 12 03 2014. http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/53beeb66e4b011fa958a4f17/1410806825334/trey+herr+paper.pdf (downloaded: 28 11 2015)

[5] PODINS, K., CZOSSECK, C.: “A vulnerability model of cyber weapons”. *International Journal of Cyberwarfare and Terrorism*, 2 1 (2012), 14–26.

[6] BENCSHAT B., PÉK G., BUTTYÁN L., FÉLEGYHÁZI M.: *Duqu: A Stuxnet-like malware found in the wild. Laboratory of Cryptography and System Security (CrySyS).* Budapest: Budapest University of Technology and Economics Department of Telecommunications, 2012. www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (downloaded: 28 11 2015)

[7] KOVÁCS L.: Az információs terrorizmus eszköztára. *Hadmérnök*, Robothadviselés 6. (Különszám), 2006. www.hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (downloaded: 28 11 2015)

[8] HAIG Zs.: *Információ – Társadalom – Biztonság.* Budapest: NKE Szolgáltató Kft., 2015.

[9] *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013.

[10] An Assessment of International Legal Issues in Information Operations, Department of Defense Office of General Counsel, May 1999. Cited in DENNING, D.: Reflections on Cyberweapons Controls. *Computer Security Journal*, XVI 4 (2000), 43–53.

[11] INTOCCIA, G., MOORE, W. J.: Communications Technology, Warfare, and the Law: Is the Network a Weapon System? *Houston Journal of International Law*, 28 (2006), 467–489.

[12] ARIMATSU, L.: *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations.* https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf (downloaded: 28 11 2015)

[13] CIA: *Speeches and testimony archive.* www.cia.gov/news-information/speeches-testimony (downloaded: 28 11 2015)

[14] SCHAAP, M. A. J.: Cyber Warfare Operations: Development and Use Under International Law. *The Air Force Law Review*, 64 (2009), 121–175.

[15] HUNT, E.: US Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing*, 34 3 (2012), 4–21.

[16] LEWIS, J. A., NEUNECK, G.: *The Cyber Index International Security Trends and Realities.* New York, Geneva: UNIDIR United Nations Institute for Disarmament Research Geneva, 2013.

[17] *W32.Stuxnet Dossier.* www.symantec.com/content/en/us/enterprise/media/security_response/whitepaper s/w32_stuxnet_dossier.pdf; LANGNER, R.: *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve.* www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (downloaded: 28 11 2015); KOVÁCS L., SIPOS M.: A Stuxnet és ami mögötte a Stuxnet és ami mögötte van: tények és a cyberháború hajnala. *Hadmérnök,* V 4 (2010),163–172. CSERHÁTI A.: A Stuxnet vírus és az iráni atomprogram. *Fizikai Szemle,* 5 (2011), 150. http://fizikaiszemle.hu/fsz1105/cserhati1105.html (downloaded: 28 11 2015)

[18] *Advanced Persistent Threats: A Decade in Review 2011.* www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf (downloaded: 28 11 2015)

[19] *Broad Agency Announcement Foundational Cyberwarfare (Plan X) DARPA-BAA-13-02.* 20 11 2012.

[20] KAIGHAM J. G.: *Submitted to the Subcommittee on Emerging Threats and Capabilities United States House of Representatives*. http://armedservices.house.gov/index.cfm/files/serve?File_id=95e7caf8-5918-4afc-9b33-f504b5ca6555 (downloaded: 28 11 2015)

[21] *Department of Defense Law of War Manual.* www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf (downloaded: 14 11 2015)

[22] STERNSTEIN, A.: The Secret Pentagon Push for Lethal Cyber Weapons. *Defense One,* 05 11 2015. (downloaded: 14 11 2015)

[23] *Introducing Responsible Disclosure Experiences in the Netherlands: A Best Practice Guide.* Netherlands: National Cyber Security Centre, 2015.