BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 13, NUMBER 1 (2020)
ISSN 2029-0454

sciendo

Cit.: *Baltic Journal of Law & Politics* 13:1 (2020): 51-80
https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml
DOI: 10.2478/bjlp-2020-0003

CONTEMPLATING A CYBER WEAPONS CONVENTION: AN EXPLORATION OF GOOD PRACTICE AND NECESSARY PRECONDITIONS

Julija Kalpokienė

Ph.D. Candidate (1); Advocate's Assistant (2)
(1) Vytautas Magnus University, Faculty of Law (Lithuania)
(2) Law Firm JurisConsultus (Lithuania)

Contact information
Address: K. Donelaičio str. 62-503, Kaunas 44248
Phone: +370 607 73770
E-mail address: j.kalpokiene@jurisconsultus.lt

Ignas Kalpokas

Associate Professor (1); Associate Professor (2)
(1) Vytautas Magnus University, Faculty of Political Sciences and Diplomacy (Lithuania)
(2) LCC International University, Department of International Relations and Development (Lithuania)

Contact information
Address: V.Putvinskio str. 23-608, LT-44211 Kaunas, Lithuania
Phone: +370 37 327891
E-mail address: ignas.kalpokas@vdu.lt

Received: April 16, 2020; reviews: 2; accepted: July 14, 2020.

ABSTRACT

Despite being a crucially important domain for states, businesses, and individuals, cyberspace still suffers from a regulation deficit. This article takes up one such dangerously underregulated area: cyber warfare and regulation of cyber weapons. For that purpose, the authors first analyse the threats posed by weaponised malicious code, including some examples of its use and potential considerations that could sway states towards engaging in a multilateral cyber weapons regulation regime. These considerations are then converted into some major principles and points to be regarded should a potential cyber weapons convention be contemplated. These are subsequently further elaborated in light of the Chemical Weapons Convention, particularly with regard to specific provisions and possibility of adoption. The article concludes with the assertion that an international agreement is feasible in principle, but its focus should be on regulating the ways of employing cyber weapons rather than on the specific weapons themselves.

KEYWORDS

Cyber warfare, cyber weapons, arms control, Chemical Weapons Convention, cyberspace regulation, agreement design

INTRODUCTION

Nowadays every aspect of personal, state, and business affairs is permeated by information technology (IT) and dependent on the Internet. This reliance has been further underscored during the lockdowns imposed in the wake of the Covid-19 pandemic: with physical interactions severely restricted, online communications and transactions have become the lifeline for public institutions, businesses, and individuals alike. Nevertheless, the downside of the ubiquity of IT systems is that people, businesses, and states have become vulnerable to cyberattacks and acts of cyber warfare. Such threats are borderless and thus cannot be effectively mitigated without inter-state cooperation. As cyberspace, and the global dependence on it, has developed rapidly, there exists a clear 'international governance deficit', with states being able to develop their own doctrines and practices without international community's oversight.[1] Hence, there is a need for a global agreement that could bring about a long-term solution. Admittedly, there are significant obstacles to possible adoption of such an agreement; hence, preconditions that would make such an agreement rational for states to enter into should be explored.

Although cyberspace is relatively new, there are lessons to be learned from existing arms control treaties. In this article, particular emphasis will be placed on the Chemical Weapons Convention (CWC). This is because the CWC regime is considered to be the fullest and most elaborate of all arms control regimes: it is global, encompasses non-proliferation and total prohibition, makes use of confidence-building measures and verification mechanisms, has its own organisation (Organization for the Prohibition of Chemical Weapons, OPCW), and is explicitly business-friendly. Moreover, an argument can also be made that there is conceptual similarity between chemical weapons and cyber weapons, in that the former are 'logical, discrete combinations of elements of the periodic table' and the latter are similar combinations of code. Moreover, both can be concocted from off-the-shelf elements, potentially even by those with limited formal professional training and without purpose-built facilities.[2] Of course, the CWC's success may partly be attributed to the normative bias against the use of chemical weapons.[3] However, treaty arrangements of the regime are to be seen as no less important.

The article first presents the specificities of cyberspace and the nature of cyber threats as well as the challenges posed to the established traditions of warfare in order to set out the context as to why states may find a cyber weapons

[1] Christian Leuprecht, Joseph Szeman, and David B. Skillcorn, "The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity," *Contemporary Security Policy* 40 (2019): 384.
[2] Alexi Franklin, "An International Cyber Warfare Treaty: Historical Analysis and Future Prospects," *Journal of Law and Cyber Warfare* 7 (2018): 154.
[3] Jason Enia and Geffrey Fields, "The Relative Efficacy of the Biological and Chemical Weapons Regimes," *The Nonproliferation Review* 21 (2014).

convention to be an attractive option. Then, the discussion moves to the necessary conditions and clauses for a cyber weapons convention to become a rational option for states. The third part examines the CWC and the lessons that can be learnt from it in terms of both adoption and particular provisions. Lastly the article outlines some of the necessary conditions for a treaty regime to materialise.

1. CYBERSPACE AND CYBER WEAPONS

Technically, cyberspace is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures,"[4] an intangible space which is impossible to grasp, one without frontiers or limits, allowing instantaneous transfer of data.[5] This space is "both a technical and a human construct, rapidly changing, opaque to non-experts, and with a 'geography' that is decoupled from the physical world."[6] It is, at least as yet, futile to discuss what a 'cyber war' is because no 'cyber war' has yet taken place; even the term 'cyberattack' is debatable in a military context,[7] although it could be defined as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[8] As a result, the first challenge of the prospective drafters of the cyber weapons convention would be to clearly delimit the object of regulation.

In the context of military use, the first operational linkages between information technology and kinetic action date back to the 1990s. The ability to degrade or paralyse the communications systems of an opponent was first emphasised by the US military during the 1991 Persian Gulf War. Then, the 1999 Kosovo campaign was marked by the first signs of asymmetric retaliation: distributed denial of service (DDoS) attacks were used against the countries involved in military action against Serbia and against NATO itself, which triggered the Alliance to rethink its network security.[9] Another wake-up call for NATO, which resulted not only in a reconsideration of defence policy but also in the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in

[4] United States Department of Defense, "The National Military Strategy for Cyberspace Operations" (December 2006) // http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf
[5] *eDate Advertising GmbH v X* and *Olivier Martinez and Robert Martinez v MGN Limited*, Joined Cases C-509/09 and C-161/10 [2011] OJ C370/9, Opinion of AG, para 43.
[6] Leuprecht, Szeman, and Skillcorn, *supra* note 1: 384.
[7] See e.g. Jonathan A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke Law & Technology Review* 9 (2010): 3-4.
[8] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge and New York: Cambridge University Press, 2013), 30.
[9] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better": 145; in: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds., *Proceedings of the 2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).

Tallinn,[10] was the Distributed Denial of Service (DDoS) attack against Estonia, during which the country's government, bank and media websites were rendered inaccessible for a prolonged period of time.[11] It also clearly pointed out the inadequacy of concentrating national security measures on military networks and classified information but leaving critical state and private infrastructure relatively unprotected.[12]

Another example dates from 2008 when, just before and during the Russian-Georgian conflict, Georgia's government and media websites went under attack. If Russia was behind this cyber operation, as it is widely believed to have been the case, this would be a clear example of the use of cyber means to complement kinetic attacks.[13] Meanwhile, probably the best-known example of employing cyber tools for strategic gain was the Stuxnet worm, discovered in 2010. The sheer sophistication of it indicates that there was likely a state actor behind it. The worm was specifically designed to attack Supervisory Control and Data Acquisition (SCADA) systems produced by Siemens and appeared to have been targeted at Iran's nuclear programme: 60% of known infections were in Iran and also, even when infections did occur elsewhere, no harm was done.[14] Much more poignant for the civilian population, though, was the 2015 hack (commonly attributed to Russia) of the Ukrainian power grid, which disabled power supply in the middle of winter, thereby demonstrating the potentially broad-reaching impact of such attacks.[15] Even more so, the Petya malware of 2016 and the NotPetya malware of 2017, despite in all likelihood having been directed against Ukraine, caused worldwide damage, including paralysing large global corporations and the British National Health Service.[16]

The interconnection of military and private uses and networks is a significant issue. For example, as much as 98% of US government communications travel through civilian networks.[17] First of all, such dependence increases vulnerability because civilian networks are often not adequately, or not at all, protected.[18] In addition, various security products are usually procured from civilian companies

[10] Vincent Boulanin, "Cybersecurity and the Arms Industry": 220; in: *SIPRI Yearbook 2013: Armaments, Disarmament and International Security* (Oxford and New York: Oxford University Press, 2013).
[11] See e.g. Arie J. Schaap, "Cyber Warfare Operations: Development and Use under International Law," *Air Force Law Review* 64 (2009): 144.
[12] Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective": 67; in: Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2009).
[13] Schaap, *supra* note 11: 145.
[14] Franklin, *supra* note 2.
[15] *Ibid*., 150.
[16] See e.g. Leuprecht, Szeman, and Skillcorn, *supra* note 1: 397-398.
[17] Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review* 88 (2010): 1542.
[18] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 100.

which are then also responsible for maintenance and updates.[19] Similarly, hardware is usually produced by civilian firms, and this contains the risk of rogue code being implanted during the manufacture process.[20] Moreover, cyber operations have a tendency to transcend the traditional dichotomies of 'human-artificial', 'civil/military', or 'violent/non-violent' – they are always a mixture of both.[21] This blurring of lines, in turn, causes a challenge to International Humanitarian Law. After all, military use of civilian infrastructure puts it at risk of attack because it may be deemed as a dual-purpose target and, hence, legitimate military objective.[22] And yet, no clear-cut threshold has so far been established – something that might well be done in a cyber weapons convention, especially if it is oriented towards certain uses of code rather than towards specific weapons, and those that pose threat to civilian populations are much more likely than others to feature in such a convention.[23]

A convincing case has been made that operations involving cyber weapons must be offence-dominant, the reason being that it is both strategically and technically advantageous to attack rather than to defend oneself.[24] That is also coupled with a limited shelf-life of a cyber weapon as the vulnerability that it is designed to exploit might be patched at any time, henceforth motivating the wielder to use the weapon before it is too late.[25] As such, cyber weapons tend to be single use (as security patches are likely to be developed).[26] Indeed, while even some of the most primitive weapons, such as a spear or a sword, could still cause harm today, cyber weapons would lose their lethality in a matter of years or even much sooner.[27] This feature also implies that cyber weaponry is costly as 'constant (re)investment is required for the development of a sustainable, constant offensive capability'.[28] The presence of a cyber weapons convention might make cyber weapons even more costly and thus reduce their appeal.

Moving to the weapons themselves, they could be defined as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or human beings".[29]

---

[19] Jensen, *supra* note 17: 1544.
[20] I*bid*.: 1543; Lynn III, *supra* note 18: 101.
[21] Mariarosaria Taddeo, "An Analysis for a Just Cyber Warfare"; in: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds., *Proceedings of the 2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).
[22] Schmitt, *supra* note 8, Rule 37
[23] Franklin, *supra* note 2: 163.
[24] Jiang Zhifeng, "Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-Finding Body Proposal," *LSE Law Review* 5 (2020): 58-59.
[25] *Ibid*.: 59
[26] Leuprecht, Szeman, and Skillcorn, *supra* note 1: 384.
[27] Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41 (2018): 7
[28] *Ibid*.: 26.
[29] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157 (2012): 7.

For example, a DDoS attack works by instructing large numbers of infected computers to send multiple queries to the target thus overwhelming and then temporarily disabling it.[30] Malicious programmes such as viruses, worms, and Trojan horses are employed to either disrupt the normal functioning of a computer or a computer system, or open a back door through which an attacker can control the system.[31] Malicious programmes spread by attaching themselves to a legitimate programme or posing as such a programme and self-replicating to spread the infection.[32] The functions of malware differ: while a virus usually modifies or deletes data in a system, a worm is traditionally used to slow down or crash a system by sending bogus messages, and a Trojan horse gives an attacker remote access to the system.[33] While the aforementioned malware most often starts to operate immediately after infection, a logic bomb is a code that remains idle in a system until a specified event or time and then causes a computer or an entire system to crash, deletes data, or otherwise detriments the target.[34] Obvious advantages of a logic bomb are its ability to remain undetected for extended periods of time and to act only if and when needed: if infecting a system with 'instant' malware at a specified time might be challenging, a logic bomb can be planted well in advance. This is, of course, not an exhaustive list but rather an illustration of the varied nature of malicious code. Nevertheless, they all have something in common – their lack of 'conventional physicality', which makes them more difficult to trace and protect against, but also brings traditional notions of harm into question.[35]

A compelling argument can be made that "[i]n cyberspace, the offence has the upper hand" because of the open collaborative design of the Internet.[36] First, because the concept of distance does not apply in cyberspace, the source of a cyber incident could equally be in an adjacent room and on the different side of the globe.[37] Likewise, as mentioned above, cyber weapons can be pre-planted in an adversary's infrastructure, or be precision-targeted (if the attacker cares to do so), and their attribution is extremely difficult.[38] This makes protection from cyberattacks and their detection difficult. Then, while in the case of kinetic warfare accumulation of mass requires significant resources in terms of equipment and manpower, in cyberspace there are no such limitations because multiple copies of a

[30] Schaap, *supra* note 11: 134.
[31] *Ibid*.: 135.
[32] Marco Roscini, "World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force," *Max Planck Yearbook of International Law* 14 (2010): 93-94.
[33] *Ibid*.: 94.
[34] Schaap, *supra* note 11: 137.
[35] Tim Stevens, "Cyberweapons: An Emerging Global Governance Architecture," *Palgrave Communications* 3 (2017): 2.
[36] Lynn III, *supra* note 18: 99.
[37] Leuprecht, Szeman and Skillcorn, *supra* note 1: 385.
[38] *Ibid*.: 384.

cyber weapon can be created instantly and distributed via countless hacked computers.[39] After all, it must also be kept in mind that "an attacker must succeed only once, while a defender must always succeed".[40] This is combined with a low entry cost, since the knowledge for exploiting cyberspace is rather cheaply and readily available.[41] However, there is a caveat: wide proliferation and low cost only apply to the low-tech and relatively low-impact cyber weapons, while the more targeted and high-impact weapons have to be specifically targeted and, therefore, require considerable resources and intelligence.[42] As a result, conventionally powerful states, given their material and intelligence resources, are likely to remain crucial actors at least as far as the sophisticated high-impact weapons are concerned.[43]

Cyber weapons are difficult to predict. While one could reasonably expect a bullet to act in a certain way, cyber environment is mutable, and, therefore, tools may operate differently than expected.[44] Hence, the nature and actions of yet unknown weapons are much more difficult to predict in cyberspace than in the physical space:[45] while one could reasonably foresee the operating principles of, for example, an adversary's missile system, that is not the case with cyber weapons. Also, cyberspace is all-pervasive: it not only relates to itself but also to land, sea, air, and space – therefore, cyber defence is, in effect, the defence of the entire perimeter.[46] Therefore, the concept of deterrence is problematic in cyberspace. For a state to be able to deter a cyber-adversary, it has to be capable and willing to retaliate; however, this capability is significantly undermined by the difficulty to unequivocally attribute a cyberattack.[47] Even if it can be shown that an attack has originated from computers located in a given country, that is still no proof that the state itself has been involved.[48] Furthermore, since cyberattacks are especially attractive to non-state actors, there could be no tangible enemy to retaliate against.[49]

And yet, paradoxically, the difficulty of cyber defence is also a factor that reduces cyber threats: a state which resorts to cyber warfare, especially in a way which allows attribution (for example, as part of the general war effort), is itself highly vulnerable to retaliatory cyber action and this, in turn, reduces the

[39] Lynn III, *supra* note 18.
[40] Leuprecht, Szeman, and Skillcorn, *supra* note 1: 390.
[41] John B. Sheldon, "The Rise of Cyberpower": 309; in: John Baylis, James J Wirtz, and Colin S Gray, eds., *Strategy in Contemporary World* (Oxford and New York: Oxford University Press, 2013).
[42] Rid and McBurney, *supra* note 29: 6.
[43] *Ibid*.: 11-12.
[44] Leuprecht, Szeman, and Skillcorn, *supra* note 1: 384-385.
[45] *Ibid*.
[46] Sheldon, *supra* note 41: 310.
[47] Dunn Cavelty, *supra* note 9: 147.
[48] Roscini, *supra* note 32, 96.
[49] *Ibid*.

willingness to employ cyber weapons.[50] In some respects, this is not dissimilar to the nuclear deterrence of Mutually Assured Destruction (MAD): since it is impossible to avoid a potentially catastrophic retaliation, it becomes rational not to employ certain means of warfare at all. Additionally, previous research has demonstrated that at least the 'specifically coded, offensive destructive cyber weapons' would meet the threshold for being categorised as WMDs,[51] hence, further meriting a consideration in the light of an arms control treaty in general, and CWC in particular.

Of the possible targets, attacks against critical infrastructure are the most likely to cause wide-scale damage. 'Critical infrastructure' refers to assets, very often in private hands, that are crucial to the functioning of society and state,[52] for example, the power grid, rail networks, airports and air traffic controls, communication networks, banking and finance systems, water purification and supply, fuel storage and transportation, traffic control, or public administration.[53] Critical infrastructure is often more vulnerable compared to military targets, especially, if its protection is left solely in civilian hands.[54] In other cases, attacks on certain devices and infrastructures can become critical because of their scale, for example, hacking medical implants or car electronics if carried out en masse.[55] A crucial paradox here is the gap between the rather small role a state does and can play in providing solutions in critical infrastructure protection and the huge detrimental impact that a breach of this infrastructure can have on a state concerned.[56]

Even though no specific cyber treaty regime exists yet, the basic principles regulating the use of cyber force should be inferred from the currently established norms of customary international law.[57] Also, some basic norms could be inferred from the existing treaty law, even though these treaties were, of course, drafted without cyberspace in mind. Similarly, case law can be applied to cyberspace. Nevertheless, some crucial ambiguities remain. For example, although use of force against other states is prohibited,[58] with the obvious exception of legitimate self-

[50] Dunn Cavelty, *supra* note 9.
[51] See, particularly, Benjamin B. Hatch, "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits," *Journal of Strategic Security* 11 (2018): 55.
[52] Dunn Cavelty, *supra* note 9: 145.
[53] See, e.g. Leuprecht, Szeman and Skillcorn, *supra* note 1: 390.
[54] Lynn III, *supra* note 18: 100.
[55] Scott D. Applegate, "The Dawn of Kinetic Cyber"; in: Karlis Podins, Jan Stinissen, and Markus Maybaum, eds., Proceedings of the 5th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications, 2013).
[56] Dunn Cavelty, *supra* note 9: 146.
[57] See Preamble, *Hague Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulation Concerning the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900)*, (1899) 187 CTS 429; Preamble, *Hague Convention (IV) (n 85)*; *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) (entered into force 7 December 1978)*, 1125 UNTS 3, art 1(2).
[58] *Charter of the United Nations (signed 26 June 1945)*, 1 UNTS XVI (UN Charter), art 2.

defence,[59] what in fact constitutes use of force in cyberspace remains a contentious issue. Then, attribution of attacks and the standards to be used are a particularly grey area. Conclusive evidence that a particular state was behind an attack are unlikely; or, if the attacks are carried out by a cyber militia or other non-state actor under the instruction of a state, the standard of effective control over a non-state actor, as set out in the *Nicaragua* case,[60] could be even more difficult to prove in cyberspace than it is in the physical world.[61] Even though a less stringent criterion of 'overall control' was set by the ICTY in the *Tadic* case,[62] the test involved in attributing the acts of cyber actors is not yet clear. It would, therefore, be beneficial for a prospective treaty to set out the applicable standard and the criteria for its application.

If cyber operations can be a means of warfare, they must abide by international humanitarian law (IHL).[63] Notable examples are the principles of necessity and proportionality,[64] distinction,[65] prohibition of attacks against civilian targets,[66] prohibition of superfluous injury or unnecessary suffering,[67] and the prohibition of attacks against 'works and installations containing dangerous forces', such as dams, dykes, and nuclear power stations,[68] as well as objects indispensable to survival of the civilian population'.[69] However, the characteristics of cyber infrastructure extend the list of legitimate targets: for example, because of the entanglement of military and civil networks, potentially almost anything could be described as dual-use objects, including large amounts of primarily civilian networks which are also used for military communications.[70] Hence, the applicability of IHL remains ambiguous and may be clarified in a cyber convention should it be concerned with particular uses of weaponised code.

In addition, states are expected to prevent their territory from being used for launching unlawful acts against other states and punish perpetrators if such acts are committed.[71] This argument was, for example, used in extending the responsibility for the 9/11 attacks to the Afghan Taliban government and for the

[59] *Ibid*., art 57.
[60] *Military and Paramilitary Activities (Nicaragua v United States)*, (Merits) [1986] ICJ Rep 14.
[61] Schaap, *supra* note 11: 146.
[62] *Tadic Case (Judgment)*, ICTY-94-1-A (15 July 1999).
[63] See e.g. Schaap, *supra* note 11.
[64] See, for example, *Military and Paramilitary Activities*, *supra* note 60, 176; *The Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, 1996 ICJ Rep 226; Schmitt, *supra* note 8, 51.
[65] *Additional Protocol I*, *supra* note 57, arts 50-51; *The Legality of the Threat or Use of Nuclear Weapons*, *supra* note 64; Schmitt, *supra* note 8, 31.
[66] *Hague Convention (IV)*, *supra* note 57, art 25; Schmitt, *supra* note 8, 37.
[67] *Additional Protocol I*, *supra* note 57, art 35(2); Schmitt, *supra* note 8, 42.
[68] *Additional Protocol I*, *supra* note 57, art 56; Schmitt, *supra* note 8, 80.
[69] *Additional Protocol I*, *supra* note 57, art 54(2); Schmitt, *supra* note 8, 81.
[70] Scott D. Applegate, "Cybermilitias and Political Hackers – Use of Irregular Forces in Cyber Warfare," *IEEE Security and Privacy Magazine* 9 (2011).
[71] *UNGA Res 56/83 (28 January 2002)*, UN Doc A/RES/56/83; see also *Corfu Channel Case (UK v Albania)*, (Merits) [1949] ICJ Rep 4.

subsequent invasion of Afghanistan.[72] Apparently, this responsibility to prevent unlawful acts seems to apply in cyberspace as well.[73] However, determining actual or even implied knowledge is difficult in cyberspace. Moreover, there may be little use of the obligation to prevent if a state's network infrastructure was used merely for transit because even if action is taken to prevent transmission, malicious data can easily be rerouted.[74] Again, this is something that needs further clarification.

2. ARMS CONTROL: SOME CRUCIAL ISSUES

Despite the relatively short history of cyber weapons, some of the core features of their regulatory regime can be inferred from past experience, whereby "multilateral agreements, carefully drafted to reduce fears and tensions, increase transparency, and facilitate reciprocal arms reductions" have proved their worth.[75] Simultaneously, caution is necessary, because consensus on regulating cyber warfare has already proved to be difficult to achieve.[76] Thus far, perhaps the most comprehensive calls for a cyber arms treaty have been those of Eilstrup-Sangiovanni,[77] Franklin,[78] and Jeutner.[79] Alternatively, a call has recently been made for an establishment for a fact-finding body without prosecutorial or enforcement capacity that would operate simply by way of naming and shaming and thus, allegedly, would be likely to be accepted by states.[80] Nevertheless, it would not solve the issues of verification, attribution, and plausible deniability. For that reason, a cyber weapons convention is still to be considered as a suitable solution.

First, for an arms control regime to be successful, confidence building measures are key, their main functions being reassurance of peaceful intentions, reduction of perceived threat or actual intimidation, and minimisation of the possibility of inadvertent escalation.[81] Hence, "norm subscribers need to have confidence that their peers are obeying their normative commitments," potentially

[72] Cassandra M. Kirsch, "Science Fiction No More: Cyber Warfare and the United States," *Denver Journal of International Law & Policy*, 40 (2012): 636.
[73] Schmitt, *supra* note 8, 5.
[74] Wolff Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace": 17; in: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds., *Proceedings of the 2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).
[75] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology* 31 (2018): 380.
[76] Jacqueline Eggenschwiller and Jantje Silomon, "Challenges and Opportunities in Cyber Weapon Norm Construction," *Computer Fraud & Security* 12 (2018): 11.
[77] Eilstrup-Sangiovanni, *supra* note 75.
[78] Franklin, *supra* note 2.
[79] Valentin Jeutner, "The Digital Geneva Convention," *Journal of International Humanitarian Legal Studies* 10 (2019).
[80] Zhifeng, *supra* note 24.
[81] Jozef Goldblat, *Arms Control: The New Guide to Negotiations and Agreements* (London and Thousand Oaks: SAGE Publications 2002), 10; Eilstrup-Sangiovanni, *supra* note 75: 391.

even more so in case of cyber weapons due to their intangible nature.[82] If such reassurance measures are in place, an arms control regime is likely to reduce arms races, increase predictability in relations among states, reduce the possibility of war, pre-empt new kinds of weapons and warfare from being developed, reduce disparity of power among states, encourage peaceful dispute resolution, allow states to channel resources to socioeconomic development rather than to military programmes, reduce suffering and destruction if conflicts do happen, diminish environmental risks, and generally promote better understanding between state parties.[83] Otherwise, there is little chance of such norm-based cooperation.[84]

Other necessary features include predictability, deliberateness, and changeability.[85] With regards to predictability, the law must operate reliably and be applied consistently. Deliberateness refers to purposefulness of measures taken within the arms control regime: only those measures that clearly contribute to the prescribed goal are acceptable. Changeability, meanwhile, is crucial if an arms control regime is to remain up to date with the latest developments in technology. The latter, however, is problematic because amendments are usually very difficult to agree, especially if state parties have conflicting interests. An alternative could be leaving the regime as flexible as possible, although this option also has its pitfalls: lack of specificity might create confusion, conflict of interpretation, and general incapacity of the regime. Non-justiciability is also important because, it is claimed, disputes would not be referred to third parties and, therefore, all treaty provisions should be clear and self-evident.[86] For example, the chemical weapons prohibition regime has dispute resolution procedures within the OPCW, although a possibility to refer the matter to the International Court of Justice (ICJ) is also included.[87]

Of course, states would accept only such arms control agreements that appear to offer some benefits or, more precisely, if the expected benefits are higher than the projected costs or detriment.[88] The problem, however, is that what states see as being beneficial could, and often does, differ. In addition, although the importance of rational calculations cannot be underestimated, their influence on policy decisions, including those pertaining to arms control, should not be taken as absolute. Another variable to be taken into account is the position of leaders, since

[82] Eggenschwiller and Silomon, *supra* note 76.
[83] *Ibid*.: 11-12.
[84] *Ibid*.
[85] Julie Dahlitz, "The Role of Customary Law in Arms Limitation": 160; in: Julie Dahlitz and Detlev Dicke, eds., *The International Law of Arms Control and Disarmament* (UN 1991).
[86] *Ibid*.: 160.
[87] *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (As Amended on 21 December 2001)*, 10 October 1980, 1342 UNTS 137, XIV [hereafter *CWC*].
[88] Coit D. Blacker and Gloria Duffy, *International Arms Control: Issues and Agreements* (Stanford: Stanford University Press, 1984): 19-20; Franklin, *supra* note 2: 161.

their personal convictions can play a significant role in swaying a state's negotiating position to one side or another, especially if the leaders concerned are strong enough domestically to pursue their own agenda.[89] For example, part of the impetus behind the early successes of the CWC was the support of the US President Bill Clinton and the Russian President Boris Yeltsin.[90] With regards to a possible cyber weapons convention, political will in the United States, the European Union, Russia, and China would be needed as a minimal precondition.[91]

Also, it would be wrong to assume that arms control in itself could decrease the likelihood of war. It can, at most, build or strengthen trust and maintain the status quo.[92] However, even if war does take place, prohibition of certain arms could still be instrumental in making it more humane. Therefore, although arms control is far from a universal remedy, it certainly offers important benefits. Clearly, a treaty completely prohibiting the employment of cyber weapons among states is both belated and not feasible.[93] However, selective limitations of certain forms of cyber warfare might still be an option. The fear is that "[i]f cyberattacks become an acceptable form of international protest, the effects could be extremely destabilizing economically and could open the door to conventional military conflict."[94] As already demonstrated, the defender is always at least one step behind in cyberspace – and that is increasingly so as the sophistication of cyber weapons increases. Therefore, assurances that certain kinds of offensive weaponry are not to be developed and used could be welcomed and would be rational for the states to engage in.

A cyber arms control regime, in addition to the limitations already present (for example in IHL), would add certainty prohibiting some weapons or ways of their usage irrespective of the (often inconclusive) considerations of applicability and specific requirements, such as proportionality or distinction.[95] Thus, although IHL could be useful as an interim option, an arms control regime is the most desirable outcome for cyber warfare regulation. Also, it is worth noting that the law of armed conflict, although applicable to cyberspace,[96] can only apply when cyber operations are part of an armed conflict or are on their own able to reach the threshold of armed conflict. However, determining what an armed cyber conflict is might prove

[89] Lisa Baglione, *To Agree or Not to Agree: Leadership, Bargaining, and Arms Control* (University of Michigan Press, 1999), 3.
[90] Kenneth Geers, *Strategic Cyber Security* (Tallinn: NATO CCD COE Publications 2011), 125-126.
[91] *Ibid*., 127.
[92] Blacker and Duffy, *supra* note 88, 335-338.
[93] See Roscini, *supra* note 32.
[94] Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity* (New York: Council on Foreign Relations 2010), 23.
[95] See Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations"; in: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds., *Proceedings of the 2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).
[96] Schmitt, *supra* note 8, 20.

extremely difficult. Once again, outlawing certain categories of weapons or their uses irrespective of other considerations would make regulation and prevention significantly more effective.

The next question is whether a 'hard' binding treaty is needed. There have been suggestions that 'soft' law of non-binding agreements and gradual norm-building is a much more effective tool for regulating conduct on the international level both because it is easier to persuade states to join a non-binding agreement and because such 'soft' regime is much more flexible and, therefore, can be adapted to changing circumstances more easily.[97] The premises of such approach are correct: states are more likely to join if they feel they would not be bound by an agreement, and making amendments could, indeed, be easier too. However, it must be argued that, for the very same reason, the agreement itself matters less. In fact, the argument for 'soft' law is contradictory: it simultaneously presumes that states take a light-hearted approach towards an agreement or a norm when endorsing it and are completely serious about it when it comes to observing its requirements. Of course, the very presence of a norm, even of a non-binding nature, could have a certain influence on state behaviour and, arguably, in time solidify into a custom. However, at least in short and medium term, only a binding agreement, and especially one with a robust verification and enforcement mechanism, could be seen as ensuring compliance. Definitely, such an agreement is much more difficult to achieve, but it must still be seen as the main objective.

Arguably, there are two main reasons for proliferation of norms: an actor may be motivated by 'doing the right thing' or simply wish to maximise utility.[98] Of course, normative regimes are the most effective when the two reasons coincide. In fact, "[c]onsiderations of economy and the fear of becoming the victim of cruel weaponry alternate in primacy with the desire to achieve security by out-arming one's rivals".[99] Of course, in setting up an arms control regime, a lot of confidence building is necessary. Here one encounters a version of Prisoner's Dilemma: while it is best if all states disarm, what happens if some do and others do not? To make matters more complicated, some states may be driven by motivations other than rational calculation and, therefore, may be even more difficult to convince to become a party to the regime.[100] Therefore, even if a state is inclined to the 'right thing', and its leaders are sympathetic towards the general goals of arms control, they may still not engage in negotiations unless there is sufficient certainty that

[97] See Daniel H. Joyner, "Jus ad Bellum in the age of WMD Proliferation," *George Washington International Law Review* 40 (2008).
[98] Stevens, *supra* note 35: 156.
[99] Detlev F. Vagts, "The Hague Convention and Arms Control," *American Journal of International Law* 94 (2000): 41.
[100] Berhanykun Andemichael and John Mathiason, *Eliminating Weapons of Mass Destruction: Prospects for Effective International Verification* (London and New York: Palgrave Macmillan, 2005), 9-10.

core national security interests or even state survival would not be threatened by complying.

One of the crucial reasons why some, especially the technologically developed, states might find it rational to commit themselves to a cyber weapons treaty is the increased dependence on cyberspace in carrying out daily activities and functions and also the influence a major cyber incident would have on the economy.[101] Meanwhile, ascending states have more to lose because an important tool for asserting themselves would thus be discarded. With this in mind, an arms control agreement not imposing a blanket ban could be, once again, a more realistic option.[102] But even then, as indicated above, there are states that are more inclined than others to enter international agreements, including arms control ones. This could possibly be attributed to a prevailing ideological consensus within those states, leading to reliance on a broadly liberal agenda emphasising the importance of international cooperation, international institutions, and international law.[103] Purely in terms of priorities, these states could be given less attention when drafting an agreement because they are very likely to become parties to it anyway. By contrast, emphasis should be put on convincing those states that either lack such ideological consensus and, therefore, oscillate between different positions depending on election results (this group includes some key states, for example, the US) or manifestly lack commitment to international law and, therefore, can only be persuaded to cooperate through appeals to their self-interest.[104] Providing strong incentives that, nevertheless, do not jeopardise the essence of prospective agreement would be a necessary condition to success. For the same reason, emphasis on compliance and enforcement should not overshadow positive incentives, such as cooperation between state parties in areas ranging from economy to security in order to sway the cost-benefit analysis in favour of entering into an arms control regime.[105] Easier trade in dual-use materials between states parties and mutual assistance in defence and prevention are examples of positive incentives that are present in the CWC and could be transferred to a cyber weapons convention. The absence of positive incentives and straightforward reliance on enforcement and punitive measures could significantly de-incentivise the less committed states.

[101] Paul Meyer, "Cyber Security through Arms Control: An Approach to International Co-operation," *The RUSI Journal* 156 (2011): 25.
[102] Franklin, *supra* note 2: 162.
[103] Manfred Elsig, "Who is in Love with Multilateralism? Treaty Commitment in the Post-Cold War Era," *European Union Politics* 12 (2011); Srini Sitaraman, *State Participation in International Treaty Regimes* (London and New York: Routledge 2009).
[104] See, generally, Eric A. Posner and Alan O. Sykes, *Economic Foundations of International Law* (Harvard UP 2013).
[105] Thilo Marauhn, "Dispute Resolution, Compliance Control and Enforcement of International Arms Control Law": 251-252; in: Geir Ulfstein, ed., *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge and New York: Cambridge University Press, 2007).

Currently, significant resources are needed to mitigate the risk of high impact attacks, the probability of which is, nevertheless, very low; such strategy, it has been suggested, makes little sense.[106] However, instead of simply withdrawing from this escalating arms race, it would be more rational to choose another alternative – to eliminate the high impact threats altogether. There would be a twofold economic benefit of entering into a cyber weapons control agreement: first, the aforementioned high costs of defending oneself against possible attacks would be diminished and, second, the likelihood of a large-scale cyber attack, which may result in high economic costs, would also be lowered. However, the high economic cost of suffering an attack might act as a disincentive too. If a state leaves itself vulnerable and there still are states that either refuse to take part in the cyber weapons control regime or are engaged in covert cyber weapons programmes, the risks are extremely high. Therefore, an assistance and protection clause whereby all states parties take on responsibility for helping a state in case of an attack or threat of it by the weapons or their uses prohibited by the convention, is crucial.[107] Another possible economic disincentive is the importance of cyberspace to economic development because restrictions on certain technologies that may potentially be dual-use may seem to be more costly than the risks associated with abstention from an arms control regime. The CWC may again serve as a good example in this instance, because its provisions cannot be implemented in ways that hamper economic development.[108]

The emphasis on WMD in arms control is not without its critics. It could be argued that actually light arms are the real weapons of mass destruction: they are cheap, widely available, easy to use, convenient to smuggle, highly mobile, and extremely lethal and effective.[109] Indeed, similar logic could be applied to cyberspace, where primitive and inexpensive malicious codes are usually deemed to be blunt tools. However, large concentration of small cyber incidents in addition to cybercrime could pose a significant threat through cumulative effect. In case of state-backed cybercrime and swarming of small-scale cyberattacks committed by a state, focus on effect rather than on means as the basis for arms control would be beneficial.

The above-mentioned point addresses the issue of approach to regulation, which has to be either means- or effects-based. One could choose to only outlaw the use of such cyber weapons which in the scope of its intended effects,

[106] See Dunn Cavelty, *supra* note 9: 151.
[107] Goldblat, *supra* note 81, 154.
[108] *Ibid*., 155.
[109] Ramesh Thakur, "Chemical Weapons and the Challenge of Weapons of Mass Destruction": 3; in: Ramesh Thakur and Ere Haru, eds., *Chemical Weapons Convention: Implementation, Challenges and Opportunities* (Tokyo: United Nations University Press, 2006).

irrespective the means employed, may amount to the use of weapons of mass destruction. However, establishing intention and setting a threshold of effect might prove to be a challenge. And yet, if an alternative approach is chosen and particular means are outlawed, an even more difficult problem arises – such a regime becomes easily susceptible to technological change and would quickly be rendered ineffective by the development of new means.[110] Therefore, compilation of a list of banned code, similar to the annexes to the CWC, is clearly undesirable. Another argument towards outlawing certain uses of cyber weapons rather than the weapons themselves could be drawn from the experience of the CWC: even if a timeframe for destruction of weapons is set, in the absence of clear measures to enforce destruction, some states, especially the more powerful ones, might feel inclined to hold on to their arsenals for as long as possible.[111] Indeed, although the original deadline for destroying chemical weapons has already passed, there still are state parties in possession of significant stockpiles (especially the United States and Russia).[112]

A further issue is that arms control has traditionally focused on states. In the case of cyber weapons, however, it is an entirely different story because an exceptionally high volume of weaponry is available to non-state actors as well.[113] And yet, as already indicated, the really high-impact attacks still usually require a state actor with its resources and intelligence. Indeed, there appears to be a continuum: the more sophisticated and resource-intensive the attack (and, consequently, the higher the likely damage), the more it is likely that a state is involved. [114] Furthermore, borders are not rendered completely irrelevant by cyberspace, especially in terms of law enforcement and, increasingly, protection of critical infrastructure, and this is yet another reason why states play a crucial role.[115] As a result, the emphasis on states might not be a crucial flaw of even a cyber weapons control regime.

3. THE CWC: EXPERIENCE AND APPLICABILITY

The CWC is a product of twenty years of negotiations and is significant because of the involvement of various actors in the negotiating process, including

[110] See Arimatsu, *supra* note 95.
[111] Andemichael and Mathiason, *supra* note 100, 140.
[112] Arms Control Association, "Chemical and Biological Weapons Status at a Glance" (February 2014) // https://www.armscontrol.org/factsheets/cbwprolif.
[113] Arimatsu, *supra* note 95: 100.
[114] Cutts, *supra* note 12: 68.
[115] Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?"; in: Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press 2009).

the global chemicals industry.[116] Clearly, the involvement of businesses is crucial when a regulatory regime includes agents and technologies that have huge economic significance.

Broadly, the CWC obliges states parties not to ”develop, produce, otherwise acquire, stockpile or retain chemical weapons’ or transfer them or ‘assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a state party” under the CWC.[117] Also, the states are obliged to destroy any existing arsenals[118] and production facilities.[119] The definition of chemical weapons includes “toxic chemicals and their precursors” unless they are intended for purposes that are not prohibited under the CWC and are not produced and stockpiled in militarily significant quantities; munitions and devices that are designed to cause death by spreading the chemicals described above; also, any equipment which is directly used in the employment of these munitions.[120] The prohibitions are formulated in the broadest terms possible in order not to leave any loopholes for states parties to retain chemical weapons of any sort. This is clearly commendable in a convention that aims to impose a blanket ban on a whole category of weapons. However, keeping a possible cyber weapons treaty in mind, the extent to which the broad definitions of the CWC are to be taken as an example depends on what type of ban is deemed to be desirable and feasible. If cyber weapons are to be outlawed completely, they also would have to be defined in broad terms. The same applies if only certain uses of computer code are outlawed: the means to achieve the outlawed effect must be kept as broad as possible. However, if only specific cyber weapons or their uses are to be prohibited, then clarity and specificity would be of utmost importance and thus the definitions provided in the CWC would not constitute a good example.

The CWC does not prohibit development and production of toxic chemical agents for “[i]ndustrial, agricultural, research, medical, pharmaceutical or other peaceful purposes”; purposes that are “directly related to protection against toxic chemicals” and chemical weapons; military purposes that are not related to chemical warfare; finally, law enforcement.[121] Not only these uses are not prohibited, but also research and free trade in materials intended for the uses listed above are encouraged, except in cases when the Convention itself is contravened.[122] In this way, positive incentives are created for countries to join the Convention. Meanwhile, countries that choose not to become parties to the

[116] Thakur, *supra* note 109: 7.
[117] *CWC*, *supra* note 87, I (1).
[118] *Ibid*., I (2).
[119] *Ibid*., I (3).
[120] *Ibid*., II (1).
[121] *Ibid*., II (9).
[122] *Ibid*., XI.

Convention are indirectly punished because they cannot freely trade in chemicals with parties to the CWC and, therefore, numerous sectors, from pharmaceuticals to agriculture, can be hit. Again, such approach, combining economic incentives for signatories and disincentives for non-signatories, has to be emulated in a successful cyber weapons agreement.

A limitation, common to most international regimes, is that the Convention does not deal with issues relating to non-state actors,[123] even though the non-proliferation clause is left open-ended and the states parties are prohibited to transfer chemical weapons to 'anyone'.[124] Thus the global arms control regime had to be supplemented by United Nations Security Council Resolution 1540,[125] which requires states to 'refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons or their means of delivery'[126] as well as to 'adopt and enforce appropriate effective laws' prohibiting non-state actors from committing the aforementioned acts.[127] States are also required to establish domestic controls and accountability measures in order to prevent proliferation of weapons of mass destruction (WMD).[128] However, some of these measures would not be exactly applicable to cyberspace. For example, the requirement of maintaining "appropriate effective border controls"[129] is perfectly reconcilable with the tangible nature of kinetic weapons but could hardly be enforceable in cyberspace. The same difficulty arises as far as export controls[130] are concerned. As a result, any cyber weapons convention will have to devise counter-proliferation measures of its own. It has been argued that non-state actors are far less likely to develop really sophisticated cyber weapons on their own. However, the danger is that non-state actors can come into possession of sophisticated weapons developed by states. Therefore, a strong counter-proliferation regime, centred on domestic controls, law enforcement, and, similarly to Resolution 1540, international cooperation and assistance,[131] has to be included in any cyber weapons control agreement.

The CWC, in order to observe state compliance and keep track on the effort to eliminate all chemical weapons, has a dual structure, based on input from both states and the OPCW – something that a cyber weapons convention would have to

[123] Ron G. Manley, "Restricting Non-State Actors' Access to Chemical Weapons and Related Materials: Implications of UNSCR 1540": 78; in: Olivia Bosch and Peter van Ham, eds., *Global Non-Proliferation and Arms Control: The Impact of UNSCR 1540* (Baltimore: The Brookings Institution Press, 2007).
[124] *CWC*, *supra* note 87, I (1) (a).
[125] *UNSC Res 1540 (28 April 2004)*, UN Doc S/RES/1540.
[126] *Ibid*., 1.
[127] *Ibid*., 2.
[128] *Ibid*. 3.
[129] *Ibid*., 3(a).
[130] *Ibid*., 3(b).
[131] *Ibid*., 7.

adopt as well. States have a duty to declare their chemical weapons, facilities directly intended to produce such weapons or their precursors and components,[132] or facilities capable of producing such materials.[133] All information provided is subject to verification. Meanwhile, the OPCW has the task of monitoring dual-use chemicals, chemicals production factories, and destroying of stockpiles and facilities prohibited by the CWC.[134] In short, OPCW's duty is to check whether the states parties have been open and transparent in their declarations and are on track to meeting their targets. However, since cyber weapons are intangible and, therefore, significantly more difficult to verify, a similar cyber weapons organisation would need to have forensic functions as well, acting as the authoritative arbiter of attribution if a suspected unlawful use of cyber weapons occurs. In fact, in case of cyber weapons, the threat of sanctions automatically triggered by unlawful use would acquire paramount importance.

Such robustness of reaction is, certainly, not something that can be learnt from the CWC. Notably, the CWC was designed to provide 'maximum flexibility' in deciding what further action is to be taken in case of non-compliance,[135] and article XII offers a variety of measures, including restriction and/or suspension of the rights and privileges enjoyed by the state concerned under the Convention, non-mandatory collective measures against the deviant states, and, in particularly grave cases, referral to UN General Assembly (UNGA) and UN Security Council (UNSC).[136] Evidently, the political element prevails in the treatment of a non-compliant state. This, admittedly, constitutes a significant weakness of the CWC regime.

The CWC's verification regime is probably the most intrusive of all arms control treaties, and this accounts for its relative success.[137] It is also the most extensive one, comprised of state declarations, routine inspections, challenge inspections, and inspections in case of suspected use of chemical weapons.[138] However, it is not only states that are significant here. Clearly, because of the dual-use nature of most chemical agents included in the Convention, support of the chemical industry is as crucial as the support of states.[139] Similarly, in any future cyber weapons agreement, industry input must not be underestimated. Businesses have to be confident that the production of crucial agents will be permitted at least

[132] *CWC*, *supra* note 87, III.
[133] *Ibid*., VI.
[134] Andemichael and Mathiason, *supra* note 100, 21-22.
[135] *Ibid*., 295.
[136] *CWC*, *supra* note 87, XII.
[137] Manley, *supra* note 123.
[138] Lisa Tabassi, "The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention)": 279; in: Geir Ulftein, ed., *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge and New York: Cambridge University Press, 2007).
[139] Manley, *supra* note 123: 76-77.

in quantities that match their needs and that commercial secrets will be protected.[140] This also would be relevant to any future cyber arms agreements.

The experience of the prohibition of chemical weapons clearly shows the importance of industry. The information technology (IT) industry, as the chemical one, is likely to protect its interests. The chemical industry lobby was able to render chemical weapons control hardly effective in the 1920s but its support for the CWC significantly contributed to the relative success of the modern chemical weapons prohibition regime. Therefore, the IT industry must be included as much as possible in the preparation of a cyber weapons control regime in order to ensure its support and cooperation or, at least, non-hindrance.

An effective cyber verification mechanism would require to instantly cross legal, national, and technical borders and unprecedented observation of traffic flows – something that does not bode well with concerns over sovereignty and data protection.[141] Due to the nature of cyberspace and cyber weapons, such a regime would have to be more intrusive in terms of sovereignty, privacy, and industry interests than the analogous CWC regime. Therefore, whereas a precedent of states and the industry agreeing to some form of intrusion does exist, this clearly does not mean that a sufficiently robust cyberspace control and verification regime can actually be established. Perhaps a reasonable partial amelioration of the verification challenge could be inclusion of complementary trust-building measures, such as provisions for cooperation between national Computer Emergency Response Teams (CERTs) and similar institutions as well as exchange of principles and drafts of national cyber strategies.[142]

Definitely, guarantees provided by the CWC regarding assistance in the case of chemical attack or a threat of chemical attack against a state party[143] are worthy of emulation because they potentially contribute to the sense of security – the threat posed by non-state actors, non-parties or state parties engaged in covert activities is thereby reduced. As a result, a cyber weapons convention would benefit from a similar clause, especially keeping in mind that response to sophisticated cyber incidents requires significant expertise which many countries lack.[144] Nevertheless, the voluntary nature of the mutual assistance clause diminishes the guarantees provided by the CWC and weakens positive incentives for states to join and comply.[145] Of course, this does not seem to be an issue for the CWC, given its almost universal acceptance (after all, only Israel, Myanmar, Angola, Egypt, North

[140] *Ibid*.: 76-77.
[141] Geers, *supra* note 90, 128-129.
[142] Eggenschwiller and Silomon, *supra* note 76.
[143] *CWC*, *supra* note 87, X.
[144] Geers, *supra* note 90, 128.
[145] Marauhn, *supra* note 105: 254.

Korea and South Sudan are not yet parties to the Convention).[146] However, for any future arms control regime guaranties should be made stronger even if, admittedly, they are likely to be more difficult to agree to.

The imposition of strict timescales for destruction of weapons, as provided in the CWC, while strengthening the urge to destroy existing stockpiles, can also act as a disincentive to join at a later for possessor states that were not the initial parties because they would have less time to fulfil treaty obligations.[147] Such clauses should, therefore, be discarded when designing a cyber weapons convention, especially given the fact that the deadlines set out in the CWC have not been met even by the original state parties.

Enforcement is the real issue since an arms control regime, just like any other normative structure, cannot be established once and for all but instead has to be maintained. However, a strong enforcement regime involving automatic triggers for measures intended to compel deviant states to comply with a cyber arms control regime (just like any other regime), be it sanctions or military measures as a tool of last resort, is highly unlikely, if not impossible, to be developed. Clearly, it was not seen as feasible for the CWC and, although the absence of one does not seem to have had a significant adverse effect, at least as yet, cyber weapons, being less tangible and more easy to hide and disguise, may provide significant incentives for states to engage in clandestine weapon development programmes. As a result, possible deterrents must also be stronger and the costs of non-compliance higher.

The crucial thing to note is that arms control is always an ongoing process and, therefore, "the engine that ultimately makes treaties work is […] the hard work of collective deliberation, justification, persuasion and judgement".[148] Without it, one could argue, even a robust enforcement mechanism would be significantly less effective. So far, there has been evident state commitment to the general provisions of the CWC, even though in real terms fulfilment of precise requirements appears to have been of low priority, and the failure to meet the destruction deadlines is a clear proof of that. Nevertheless, some movement in the prescribed direction is seen. At least the same amount of willingness by states to achieve the goal of the cyber convention would be needed for the convention to work. Indeed, a strong case can be made in favour of an arms control approach with regards to cyber weapons.[149] Further and further militarisation of cyberspace would definitely

[146] Organisation for the Prohibition of Chemical Weapons, "Member States" // https://www.opcw.org/about-us/member-states.
[147] Tabassi, *supra* note 138: 288-289.
[148] Jutta Brunée, "Compliance Control": 390; in: Geir Ulfstein, ed., *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge and New York: Cambridge University Press, 2007).
[149] Meyer, *supra* note 101.

not contribute to cyber security.[150] However, rather than embracing the other extreme and pushing for disarmament,[151] limitation and norm-building would be a more feasible task.

4. NECESSARY CONDITIONS

The divergence of interests among the most powerful states is likely the reason why efforts aimed at finding consensus in fora such as the UN produce more squabbles than tangible results.[152] Indeed, at the moment a clash of two different worldviews and aspirations is evident: the United States is concerned with free flow of information and trade, advocating a mixture of public and private involvement in cyber governance (a multi-stakeholder approach) while Russia is more concerned with securing its 'own' part of cyberspace and sees state control as a way of doing it.[153] Until both sides are prepared to move towards the middle ground, any agreement is not likely.

Transparency is another important requirement for arms control success. And yet, transparency alone might not be a sufficient answer, especially if there is a significant degree of mistrust between the parties. A verification procedure capable of ensuring transparency and providing impartial information trusted by all sides is, therefore, crucial. It is important to ensure state compliance with the regulatory regime because non-compliance by one party might jeopardise the entire regime by giving other states a pretext to deviate from their obligations as well. Of course, verification by itself cannot ensure compliance – it can only aim to sway states towards observing their treaty obligations.[154] Therefore, other measures addressing non-compliance have to be present. Furthermore, in case of cyber weapons, verification might be extremely problematic. Although information exchange and norm- and trust-building are more feasible options, they are just as well limited by the near impossibility of inspecting and verifying another state's cyber arsenal.[155] Indeed, out of the three parts of effective verification process: the possibility of detection, decision on legality, and response to illegal activities, detection and response are especially difficult in cyberspace. While the latter one is problematic in any regime, for example, due to lack of political will, the former is more difficult

[150] Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* 17 (2012).
[151] *Ibid*.
[152] Eggenschwiller and Silomon, *supra* note 76.
[153] Eva Claessen, "Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU," *Journal of Cyber Policy* (2020) // DOI: 10.1080/23738871.2020.1728356.
[154] Guido den Dekker, "The Effectiveness of International Supervision in Arms Control Law," *Journal of Conflict and Security Law* 9 (2004): 323.
[155] See e.g. Arimatsu, *supra* note 95: 101.

with cyber weapons than with the conventional ones because computer code is less tangible and much easier to hide. In addition, no specific production facilities are needed to produce computer code.

The lack of a robust regime of compliance and verification is a serious blow to the effectiveness of an arms control regime.[156] Yet, it might be suggested that although attribution and verification are extremely difficult in cyberspace, if some sort of arms control agreement for cyberspace existed, the stigma of being associated with breaching an agreement may prove to be a powerful deterrent, at least for state actors. In addition, the international community could exert pressure even if definitive proof of breach of the convention was lacking, as illustrated by, for example, Iran's nuclear programme. However, although it may be possible to regulate strategically-minded state-controlled forces, semi-autonomous forces characterised by intermingling of public-private and military-criminal elements would be more difficult to regulate.

States must be responsible for the weapons they sell, be it to state or non-state actors, especially in cases when they are subsequently used in a way contrary to international law and this use was actually known or should have been foreseen.[157] This must apply not only to kinetic but also to cyber weapons. Definitely, arms control by itself cannot guarantee non-acquisition of certain weapons by state or non-state actors. Realistically, it can only provide disincentives, albeit, arguably, strong ones.[158] Counter-proliferation vis-à-vis non-state actors is a crucial issue, and non-proliferation of know-how and actual malicious code to non-state actors needs to be included into the convention outright. And yet, a single arms control regime is unlikely to solve counter-proliferation issues. Instead, a web of bilateral and multilateral measures, legal, political, and technological tools and arrangements and, perhaps, most importantly, interest and willingness of the relevant actors are crucial.[159] In case of cyber weapons, because of the versatility of computer code and the wide supply of know-how, states should be even more involved in cooperation ensuring that malevolent non-state actors are unable to develop dangerous cyber capabilities.

Of course, a popular argument is that the very presence of non-state actors capable and willing to carry out cyberattacks significantly diminishes any regulatory regime because it makes both attribution and punishment for violations almost (if not completely) impossible. However, that is not necessarily the case. For example,

[156] *Ibid*.: 101-102.
[157] Zeray Yihdego, *The Arms Trade and International Law* (Portland: Hart Publishing, 2007), 291.
[158] Michael A. Levi and Michael E. O'Hanlon, *The Future of Arms Control* (Baltimore: The Brookings Institution Press, 2005), 6.
[159] John Baylis, "The Control of Weapons of Mass Destruction": 225-226; in: John Baylis, J.J. Wirtz, and Colin S. Gray, eds., *Strategy in the Contemporary World* (Oxford and New York: Oxford University Press, 2016).

with terrorist organisations, claiming responsibility is a usual tactic and there is no reason to believe this would be different in cyberspace – after all, terrorist attacks are the means to promote their agenda and without the associated publicity such promotion is impossible. Thus, contrary to popular wisdom, it might be possible to argue that attribution in case of an attack by a non-state actor is even less problematic than in cases when states are involved. And counter-terrorism sanctions regimes already indicate that there are means of tackling even the threats from non-state actors.[160]

CONCLUSIONS

With militarised use of cyberspace dating back to the 1990s, the question is not whether cyber weapons can be pre-empted or outlawed but, instead, whether they will be regulated at all and, if so, how. It has been shown that the case for regulation can be made in terms of both potential military harm and likely widespread damage arising from the close interconnection between military and civilian infrastructure. Additionally, regulation would also clarify the standing of cyber weapons in IHL.

Drawing from the experience of existing arms control regimes, the article defines key elements of such a regime as confidence building, predictability, deliberateness, and changeability while also concluding that a cost-benefit calculation would likely be positive towards states joining a cyber weapons regulation regime. Certainly, as evidenced in this article, the intangibility and malleability of both cyberspace and cyber weapons makes regulation and verification more difficult than it is for physical weapons. Nevertheless, these downsides can be ameliorated through treaty design. To this end, it is demonstrated that the CWC could act as a useful framework for constructing a cyber weapons convention due to the typically dual nature of its object, its intrusive enforcement procedures, focus on industry involvement, and cooperation and assistance mechanisms. Hence, while a cyber weapons convention might not currently be on the table, it is, nevertheless, a viable future option.

BIBLIOGRAPHY

1. Andemichael, Berhanykun, and John Mathiason. *Eliminating Weapons of Mass Destruction: Prospects for Effective International Verification*. London and New York: Palgrave Macmillan, 2005.

[160] See, e.g. Andrea Charron, *UN Sanctions and Conflict: Responding to Peace and Security Threats* (London and New York: Routledge, 2011).

2. Applegate, Scott D. "Cybermilitias and Political Hackers – Use of Irregular Forces in Cyber Warfare." *Security & Privacy* 9 (2011): 16-22.
3. Applegate, Scott D. "The Dawn of Kinetic Cyber": 163-178. In: Karlis Podins, Jan Stinissen, and Markus Maybaum, eds. *Proceedings of the 5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2013.
4. Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations": 91-110. In: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds. *Proceedings of the 2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.
5. Arms Control Association. "Chemical and Biological Weapons Status at a Glance" (February 2014) // https://www.armscontrol.org/factsheets/cbwprolif.
6. Baglione, Lisa. *To Agree or Not to Agree: Leadership, Bargaining, and Arms Control*. University of Michigan Press, 1999.
7. Baylis, John. "The Control of Weapons of Mass Destruction": 212-230. In: John Baylis, J.J. Wirtz, and Colin S. Gray, eds. *Strategy in the Contemporary World*. Oxford and New York: Oxford University Press, 2016.
8. Blacker, Coit D., and Gloria Duffy. *International Arms Control: Issues and Agreements*. Stanford: Stanford University Press, 1984.
9. Boulanin, Vincent. "Cybersecurity and the Arms Industry": 218-226. In: *SIPRI Yearbook 2013: Armaments, Disarmament and International Security*. Oxford and New York: Oxford University Press, 2013.
10. Brunée, Jutta. "Compliance Control": 373-390. In: Geir Ulfstein, ed. *Making Treaties Work: Human Rights, Environment and Arms Control*. Cambridge and New York: Cambridge University Press, 2007.
11. Charron, Andrea. *UN Sanctions and Conflict: Responding to Peace and Security Threats*. London and New York: Routledge, 2011.
12. Claessen, Eva. "Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU." *Journal of Cyber Policy* (2020) // DOI: 10.1080/23738871.2020.1728356.
13. Cutts, Andrew. "Warfare and the Continuum of Cyber Risks: A Policy Perspective": 66-76. In: Christian Czosseck and Kenneth Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press 2009.
14. Dahlitz, Julie. "The Role of Customary Law in Arms Limitation": 157-178. In: Julie Dahlitz and Detlev Dicke, eds., *The International Law of Arms Control and Disarmament*.UN 1991.

15. Den Dekker, Guido. "The Effectiveness of International Supervision in Arms Control Law." *Journal of Conflict and Security Law* 9 (2004): 315-330.
16. Dunn Cavelty, Myriam. "The Militarisation of Cyberspace: Why Less May Be Better": 141-154. In: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds. *Proceedings of the 2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.
17. Eggenschwiller, Jacqueline, and Jantje Silomon. "Challenges and Opportunities in Cyber Weapon Norm Construction." *Computer Fraud & Security* 12 (2018): 11-18.
18. Eilstrup-Sangiovanni, Mette. "Why the World Needs an International Cyberwar Convention." *Philosophy & Technology* 31 (2018): 379-407.
19. Elsig, Manfred. "Who is in Love with Multilateralism? Treaty Commitment in the Post-Cold War Era." *European Union Politics* 12 (2011): 529-550.
20. Enia, Jason, and Geffrey Fields. "The Relative Efficacy of the Biological and Chemical Weapons Regimes." *The Nonproliferation Review* 21 (2014): 43-64
21. Franklin, Alexi. "An International Cyber Warfare Treaty: Historical Analysis and Future Prospects." *Journal of Law and Cyber Warfare* 7 (2018): 379-407.
22. Geers, Kenneth. *Strategic Cyber Security*. Tallinn: NATO CCD COE Publications 2011.
23. Goldblat, Jozef. *Arms Control: The New Guide to Negotiations and Agreements*. London and Thousand Oaks: SAGE Publications, 2002.
24. Hare, Forrest. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?": 88-105. In: Christian Czosseck and Kenneth Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare.* Amsterdam: IOS Press 2009.
25. Hatch, Benjamin B. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." *Journal of Strategic Security* 11 (2018): 43-61.
26. Jensen, Eric Talbot. "Cyber Warfare and Precautions against the Effects of Attacks." *Texas Law Review* 88 (2010): 1533-1569.
27. Jeutner, Valentin. "The Digital Geneva Convention." *Journal of International Humanitarian Legal Studies* 10 (2019): 158-170.
28. Joyner, Daniel H. "Jus ad Bellum in the age of WMD Proliferation." *George Washington International Law Review* 40 (2008): 233-288.
29. Kirsch, Cassandra M. "Science Fiction No More: Cyber Warfare and the United States." *Denver Journal of International Law & Policy* 40 (2012): 620-647.
30. Knake, Robert K. *Internet Governance in an Age of Cyber Insecurity*. New York: Council on Foreign Relations 2010.

31. Levi, Michael A., and Michael E. O'Hanlon. *The Future of Arms Control.* Baltimore: The Brookings Institution Press, 2005.
32. Leuprecht, Christian, Joseph Szeman, and David B. Skillcorn. "The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity." *Contemporary Security Policy* 40 (2019): 382-407.
33. Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (2010): 97-108.
34. Manley, Ron G. "Restricting Non-State Actors' Access to Chemical Weapons and Related Materials: Implications of UNSCR 1540": 73-85. In: Olivia Bosch and Peter van Ham, eds. *Global Non-Proliferation and Arms Control: The Impact of UNSCR 1540.* Baltimore: The Brookings Institution Press, 2007.
35. Marauhn, Thilo. "Dispute Resolution, Compliance Control and Enforcement of International Arms Control Law": 243-272. In: Geir Ulfstein, ed. *Making Treaties Work: Human Rights, Environment and Arms Control*. Cambridge and New York: Cambridge University Press, 2007.
36. O'Connell, Mary Ellen. "Cyber Security without Cyber War," *Journal of Conflict and Security Law* 17 (2012): 187-209.
37. Meyer, Paul. "Cyber Security through Arms Control: An Approach to International Co-operation." *The RUSI Journal* 156 (2011): 22-27.
38. Ophardt, Jonathan A. "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield." *Duke Law & Technology Review* 9 (2010): 1-28.
39. Posner, Eric A., and Alan O. Sykes. *Economic Foundations of International Law*. Cambridge (MA): Harvard University Press, 2013.
40. Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157 (2012): 6-13.
41. Roscini, Marco. "World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force." *Max Planck Yearbook of International Law* 14 (2010): 85-130.
42. Schaap, Arie J. "Cyber Warfare Operations: Development and Use under International Law." *Air Force Law Review* 64 (2009): 121-174.
43. Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge and New York: Cambridge University Press, 2013.
44. Sheldon, John B. "The Rise of Cyberpower": 303-320. In: John Baylis, James J Wirtz, and Colin S Gray, eds. *Strategy in Contemporary World*. Oxford and New York: Oxford University Press, 2013.
45. Sitaraman, Srini. *State Participation in International Treaty Regimes*. London and New York: Routledge 2009.

46. Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41 (2018): 6-32.
47. Stevens, Tim. "Cyberweapons: An Emerging Global Governance Architecture." *Palgrave Communications* 3 (2017): 1-6.
48. Tabassi, Lisa. "The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention)": 273-300. In: Geir Ulftein, ed. *Making Treaties Work: Human Rights, Environment and Arms Control*. Cambridge and New York: Cambridge University Press, 2007.
49. Taddeo, Mariarosaria. "An Analysis for a Just Cyber Warfare": 209-218. In: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds. *Proceedings of the 2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.
50. Thakur, Ramesh. "Chemical Weapons and the Challenge of Weapons of Mass Destruction": 1-14. In: Ramesh Thakur and Ere Haru, eds. *Chemical Weapons Convention: Implementation, Challenges and Opportunities*. Tokyo: United Nations University Press, 2006.
51. United States Department of Defense. "The National Military Strategy for Cyberspace Operations" (December 2006) // http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf
52. Vagts, Detlev F. "The Hague Convention and Arms Control." *American Journal of International Law* 94 (2000): 31-41.
53. Von Heinegg, Heintschel Wolff. "Legal Implications of Territorial Sovereignty in Cyberspace": 7-20. In: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds. *Proceedings of the 2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.
54. Yihdego, Zeray. *The Arms Trade and International Law.* Portland: Hart Publishing, 2007.
55. Zhifeng, Jiang. "Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-Finding Body Proposal." *LSE Law Review* 5 (2020): 59-88.

LEGAL REFERENCES

1. *Charter of the United Nations (Signed 26 June 1945)*. 1 UNTS XVI.
2. *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have*

Indiscriminate Effects (and Protocols) (As Amended on 21 December 2001). 10 October 1980, 1342 UNTS 137.

3. *Corfu Channel Case (UK v Albania)*. (Merits) [1949] ICJ Rep 4.
4. *eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited*. Joined Cases C-509/09 and C-161/10 [2011] OJ C370/9, Opinion of AG.
5. *Hague Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulation Concerning the Laws and Customs of War on Land (Adopted 29 July 1899, entered into force 4 September 1900)*. (1899) 187 CTS 429.
6. *Military and Paramilitary Activities (Nicaragua v United States)*. (Merits) [1986] ICJ Rep 14.
7. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) (Entered into force 7 December 1978)*. 1125 UNTS 3.
8. *Tadic Case (Judgment)*. ICTY-94-1-A (15 July 1999).
9. *The Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*. 1996 ICJ Rep 226.
10. *UNGA Res 56/83 (28 January 2002)*. UN Doc A/RES/56/83.
11. *UNSC Res 1540 (28 April 2004)*. UN Doc S/RES/1540