2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations

Louise Arimatsu
International Law Programme
Chatham House
London, UK
larimatsu@chathamhouse.org

Abstract: Despite a greater willingness on the part of States to enter into a dialogue on the potential implications of cyber warfare, there is continued disagreement on whether new rules are required to govern this 'new domain' and, if so, whether such rules should be in codified form or be left to evolve through a natural progression of customary international law. Closely interlinked with these questions is the distinct issue of whether there is a need for an arms control treaty. To speak of an arms control treaty or the regulation of a particular weapon by reference to the law of armed conflict (LOAC) is to presuppose a common conception of the particular type of weapon that is under discussion. This paper therefore poses the question, 'What is a cyber-weapon?' before considering whether an arms control treaty is a feasible option, let alone whether such a treaty would be capable of addressing the concerns that have been raised by its proponents. This paper also considers existing LOAC rules to identify the issues that are unique to cyber-weapons and, in doing so, it is argued that further clarification is indeed merited.

Keywords: *cyber-weapons, arms treaty, law of armed conflict*

1. INTRODUCTION

On 12 September 2011 China and the Russian Federation, together with Tajikistan and Uzbekistan, submitted a draft United Nations General Assembly resolution on an *International code of conduct for information security.*[1] The unexpected move, just prior to a global conference on cyberspace, was described by some as an attempt to 'regain the initiative' on a topic that has commanded increasing attention by the international community over the last several years.[2] The draft code requires States to comply with the UN Charter and 'universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States' and 'not to use information and

1 UN GA Doc. A/66/359 of 14 September 2011.
2 For details on 2011 London Conference on Cyberspace see http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/.

communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'. Though described as a draft voluntary code, this document not only illuminates what interests are perceived to be at stake by the sponsoring States but exposes the potential difficulties that would be encountered in any attempt to negotiate a cyber treaty, not least one that is concerned with stemming the proliferation of cyber-weapons or what the draft code refers to as 'information weapons'.

The potential benefits and practical limitations of a treaty to govern cyber-weapons can only be fully appreciated with an understanding of the historical and political context within which the cyber discourse has evolved in recent years. This paper therefore opens with a brief look at the context and the issues upon which States have traditionally divided to assess whether there is any prospect for agreement (section 2). While such divisions are founded primarily on disparate ideological and political views on the role of the State, legal experts also differ on whether new rules are required to govern cyber warfare and, if so, whether such rules should be in codified form or be left to evolve through a natural progression of customary international law. Often intermingled with this question is the distinct issue of whether there is a need for an arms control treaty of sorts, as inferred by the Sino-Russia draft code of conduct. The objective, according to the proponents of such a treaty, is to limit the digital or cyber 'arms race' between States, with a view to constraining or even prohibiting the use of cyber-weapons in certain circumstances.[3] Obviously these questions are not unique to the cyber warfare discourse. Progress in the realms of science and technology, which invariably feeds into warfare, has always prompted similar anxieties.

In section 3 of the paper, I pose the simple, yet often ignored question, *what is a cyber-weapon*? I do so because to speak of an arms control treaty or the regulation of a particular weapon by reference to the law of armed conflict (LOAC) is to presuppose a common conception of the particular type of weapon that is under discussion. And although the term 'cyber-weapon' is entrenched throughout the policy and legal literature on cyber warfare, it is telling that in November 2011, the US Department of Defense stated, '[t]here is currently no international consensus regarding the definition of "cyber weapon"'.[4] From this, should we surmise that there is something unique about the cyber-weapon that inhibits definitional agreement? What are the attributes that distinguish such weapons from conventional weapons and do these tell us anything about why agreement continues to prove elusive?

In this context I consider whether an arms control treaty is a feasible option let alone whether such a treaty would be capable of addressing the concerns that have been raised in respect of the prospect of cyber warfare.[5] International law has historically dealt with weapons through two parallel approaches: regulating the manner in which weapons are used or by focusing on a particular type of weapon.[6] Whether cyber-weapons are better suited to be governed by LOAC

3 John Markoff and Andrew Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace' 28 June 2009, New York Times. Franz-Stefan Gady and Greg Austin, 'Russia, the United States and Cyber Diplomacy', EastWest Institute paper 2010, 6.

4 United States Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 8.

5 The problem of attribution is probably of most concern.

6 Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol I' IRRC (2003) Volume 85, No. 850, 397.

or whether an arms control treaty is warranted will be explored given the different rationale upon which each approach is founded. In the penultimate section I ask whether, all things considered, existing LOAC rules are adequate but that, nonetheless, the particular context of cyber warfare demands greater clarity as to how the rules are interpreted and applied and what form this might take.[7] Not all experts share the view that the law in its current form can respond fully to the particularities of the cyber challenge; as a consequence, some have called for far more proactive measures including a treaty to govern cyber warfare.[8] The recent developments at the international level would suggest that there may be an emerging consensus among States in favour of a set of agreed rules governing cyber warfare more generally although both form and content may be difficult to secure.

I conclude with some thoughts on areas for further exploration.

Before proceeding, one note of caution is required. A persistent problem that has characterised this entire discourse is the prevalence of misleading language and 'parallel vocabularies' in discussions on all aspects of cyber space and security.[9] For example, as one legal expert has noted, despite widespread use of the terms 'cyber warfare' and 'cyber attack', the vast majority of cyber activity targeting the U.S. cannot, under existing law of armed conflict, be described as an 'attack' that would give rise to a situation of armed conflict operationalising that body of law.[10] This problem is compounded by the strategic choice of some of the leading players to use phrases that are broad in scope to safeguard what are genuinely regarded as legitimate sovereign interests, made even more pressing by the extent to which the Arab Spring revolutions were facilitated by the digital revolution.

7 C. Joyner and C. Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' 12 EJIL (2001) 825-65.

8 Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' 47 Harvard International Law Journal, 179-221.

9 Russia-U.S. Bilateral on Cybersecurity - Critical Terminology Foundations, K. F Rauscher and V. Yaschenko (eds), 2011 EastWest Insitute and the Information Security Institute of Moscow State University. See also 'Technology, Policy, Law and Ethics Regarding U.S. Acquisition of Use of Cyberattack Capabilities' W. Owens, K. Dam and H. Lin (eds) National Research Council (2009) 14-15, Box1.2 [hereinafter Technology, Policy, Law]; according to the report, under current US military doctrine computer network operations include computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE), 161.

10 Commander Todd C. Huntley, 'Controlling the use of force in cyber space: the application of the law of armed conflict during a time of fundamental change in the nature of warfare' 60 Naval Law Review (2010) 2.

2. THE CONTEXT

The United States' decision in October 2009 not to oppose a draft UN General Assembly resolution to explore possible measures to 'strengthen information security at the global level' signalled a fundamental shift in its cyber security policy.[11] For over a decade the US had resisted the repeated attempts by Russia – under the auspices of the UN Committee on Disarmament and International Security[12] (hereinafter First Committee) – to explore the possibility for formalising the rules pertaining to cyber security. Ideological differences coupled with mistrust as to motive on the part of *both* sides had created gridlock and it was only with significant redrafting of Russia's 1998 draft resolution to address US concerns combined with the re-assessment by the Obama administration in 2009 that US cyber strategy would benefit from greater international engagement, that progress, albeit limited, was secured.[13]

These developments paved the way for the release, in July 2010, of a report by the Group of Governmental Experts (GGE) comprising cyber security specialists and diplomats representing 15 countries including Russia and the US.[14] By contrast to an earlier attempt in 2005 the GGE, established by General Assembly resolution 60/45, was able to reach agreement in respect of a number of recommendations.[15] These included: to pursue further dialogue among States to discuss norms pertaining to the use of information and communication technologies (ICTs); to consider measures to address the implications of ICTs by States in situations of armed conflict; and to explore possibilities for elaborating on common terms and definitions.[16] Although the challenges identified in the GGE report are of pressing concern to all States, profound disagreements founded on radically differing perspectives and perceived interests are likely to hinder speedy progress, at least insofar as any treaty regime is concerned.

Russia and the US have approached the issue of cyber security from fundamentally different legal perspectives with the former favouring the development of a binding international regime while the latter has treated cyber security as falling, first and foremost, within a law enforcement paradigm and therefore better governed through suppression conventions and

11 Draft Resolution A/C.1/64/L.39 (16 October 2009) on Developments in the field of information and telecommunications in the context of international security was adopted by the General Assembly without a vote on 29 October 2009; see http://daccess-dds-ny.un.org/doc/UNDOC/LTD/N09/563/73/PDF/N0956373.pdf?OpenElement and http://www.un.org/News/Press/docs/2009/ga10898.doc.htm.

12 The Disarmament and International Security Committee deals with disarmament and related international security questions.

13 Recognizing that the US could not work in isolation if it wanted to succeed in cyberspace, the review called for a 'strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issued such as technical standards acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force.' The review was released in May 2009 and can be found at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

14 A/65/201 of 30 July 2010. The GGE was established under UN GA resolution 60/45.

15 On 11 January 2011, the General Assembly welcomed the report and took note of the recommendations contained therein; a new paragraph was introduced requesting the Secretary-General to establish a new GGE in 2012 to submit a report at the 68th session in 2013 (A/RES/65/41). See also A/RES/66/24 of 13 December 2011 adopting draft resolution A/66/407, 10 November 2011.

16 Report by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July 2010, A/65/201.

mutual assistance.[17] While both regard cyberspace as a domain of economic opportunity as well as of heightened risk, for the US, the primary threat is criminal rather than political in origin.[18] Consequently, it regards Russia's demands for a broad international legal regime as overly prescriptive and fears that any concessions made on its part will assist in legitimising State censorship and repressive domestic policies. Such concerns are not without foundation. The very term 'information security' preferred by Russia, and often equated to 'cyber security', belies the reality that it is a far more 'sweeping concept tied to the State's need for control over the information space of its citizenry'.[19] In light of the *Information Security Doctrine of the Russian Federation* released by President Putin in 2000, it is difficult to escape the impression that Russia's broader concern is with how it can effectively maintain social control of the Internet in the face of both external and internal challenges.[20] At its most basic, the different approaches pursued are primarily, although not exclusively, a reflection of the different ideological viewpoints on the role of the State.[21]

A supplementary reason driving Russia's ambitions for an international cyber arms control treaty (and one that must not be under-estimated) is its perceived inferiority in the field of communications technology.[22] Although the US's investment in, and reliance on, information technology – whether civilian or military – may in the short term make it far more vulnerable to malicious digital intrusions, Russia's reliance on commercial off-the-shelf hardware and

17 The US is party to the Convention on Cybercrime (Budapest Convention) which it ratified in September 2006. The Convention was drafted by the Council of Europe (COE) and despite its official 'observer' status, the US played an 'especially influential role, in part because it had more experience than other countries in addressing cybercrime and entered the process with well-formulated positions'; Michael Vatis 'The Council of Europe Convention on Cybercrime' in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, National Academies Press (2010) 207, available at http://www.nap.edu/catalog.php?record_id=12997. By contrast, although Russia is a member of the COE, it has neither ratified nor signed the Convention on the grounds that it views the provision allowing unilateral trans-border access by law enforcement agencies to computers or data with the consent of the computer- or data-owner, as a violation of sovereignty; Vatis 218.

18 As a UN report acknowledged in 2010, it is difficult to estimate the extent of the financial loss and number of offences committed by cybercriminals. Although guarded, the report refers to some sources estimating losses to businesses and institutions in the US due to cybercrime to be worth as much as US$67 billion per year; A/CONF.213/9 of 22 January 2010. According to the 2011 Norton Cybercrime Report the cost of global cybercrime stands at US$114 billion annually.

19 Christopher A. Ford, 'The Trouble with Cyber Arms Control' The New Atlantis 2010, 52-68, 63. See also Timothy L. Thomas, 'The Russian Understanding of Information Operations and Information Warfare' in Information Age Anthology: the Information Age Military, D. Alberts and D. Papp (eds) 2001, available at www.dodccrp.org.

20 The Information Security Doctrine of the Russian Federation, 9 September 2000, available at http://www.mid.ru/ns-osndoc.nsf/osnddeng.

21 This observation might apply equally to China which also adopts a far broader understanding of cyber threats; Ford, 'The Trouble with Cyber Arms Control', 62-66. That Russia and China share many of the perceived threats is best exemplified by the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security which was adopted at the 61st plenary meeting of the Organization on 2 December 2008. Nevertheless, there is also evidence to indicate that at a strategic/operational level, China may adopt a radically different approach from Russia in that it sees cyber warfare as an 'equalizer' in potential military conflicts with a technologically superior adversary such as the US; Technology, Policy, Law, 332-33.

22 Information Security Doctrine of the Russian Federation.

software and lack of home-grown expertise makes it far more vulnerable in the long run.[23] Thus, as in 1899, Russia envisages that an international treaty may function to address its position of relative disadvantage.[24] While much of the cyber security discourse over the last decade has been dominated by Russia and the US, China's emerging status and participation within this field poses questions that have yet to be explored adequately. How it frames both opportunities and risks in this domain is likely to shape any global progress on an internationally agreed regime.[25] Finally, it is necessary to ask whether, despite the US's long held scepticism over the prospect of an arms control treaty, there are any emerging or potential future benefits or threats that might alter its stance in favour of such a treaty.

Since taking office, the Obama Administration has responded robustly to its critics' charges that a comprehensive national security strategy that embraced both the domestic and international aspects of cyber security was lacking.[26] In May 2011, the White House released its *International Strategy for Cyberspace* – 'the first attempt by the US to lay out an approach that unifies its engagement with international partners on the full range of cyber issues' and it concurrently embarked on a variety of outreach efforts to enhance existing military alliances and to pursue closer cyber security partnerships with like-minded States. But despite its willingness to engage in a more pro-active dialogue, what is striking is the Administration's continued emphasis on developing the law enforcement paradigm to counter malicious cyber activities with little evidence to suggest that there has been a fundamental shift in its position on the need for an arms control treaty. Rather, the message that is repeatedly heard is that existing international law suffices.[27]

Any consideration as to whether a new treaty regime to govern a particular weapon is necessary

23 'Russia's international cooperation in ensuring information security has two distinctive features: international competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allow them to build up their potential for information warfare. Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure.' A.A. Streltsov, State Information Policy: The Basis of the Theory, 2010, Moscow, 345 cited by Franz-Stefan Gady and Greg Austin, 'Russia, the United States and Cyber Diplomacy' EastWest Institute (2010) 6.

24 According to Jozef Goldblat, 'the Hague Conferences of 1899 and 1907 were convened at the initiative of the Emperor of Russia, which was lagging in the European arms race and could not afford to catch up with its rivals because of its economic weakness'; Arms Control: The New Guide to Negotiations and Agreements (2003) Sage Publications, section 2.1.

25 See for example, submissions by China's representative to the 17th meeting of the First Committee, 20 October 2011, GA/DIS/3442.

26 James A. Lewis, 'Cyberwarfare and its Impact on International Security', United Nations Office for Disarmament Affairs (UNDOC) Occasional Paper No. 19 June 2010; 'Securing Cyberspace for the 44th Presidency: A Report of the Center for Strategic and International Studies Commission on Cybersecurity, December 2008. At the domestic level, U.S. Cyber Command (USCYBERCOM) was established in June 2009 with the responsibility for centralizing command of cyberspace operations. Nevertheless, see also US Government Accountability Office (GAO) report, Cyberspace: US Faces Challenges in Addressing Global Cybersecurity and Governance (GAO-10-606) July 2010.

27 See for example the EU-US Working Group on Cybersecurity which was established in November 2010 and tasked principally with strengthening transatlantic cooperation in the field of cyber-crime, PRES/10/315 available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246. The most recent Department of Defense reports indicate that the US remains unconvinced that a convention governing cyberwar or more specifically, cyber-weapons is warranted; see for example, Department of Defense Strategy for Operating in Cyberspace, July 2011 and Department of Defense Cyberspace Policy Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 of November 2011.

and, if so, what form this might take requires an understanding of the nature of the weapon under examination. In the following section I pose the simple yet vexing question, '*what is a cyber-weapon?*' before assessing whether an arms control treaty will adequately address the concerns raised by its proponents.

3. AN ARMS CONTROL TREATY FOR CYBER-WEAPONS

By contrast to most commentaries on cyber warfare where the preliminary concern is with the question what is an '*armed attack*',[28] this paper asks, *what is a cyber-weapon*? A weapon is generally understood to be an instrument of offensive or defensive combat and has been defined as a device that is 'designed to kill, injure, or disable people, or to damage or destroy property''.[29] 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. Moreover, even if 'property' is to encompass digital network systems, programmes and data, this particular definition is arguably under-inclusive if 'damage' or 'destruction' of property is narrowly defined. For example, the purpose of Duqu, a remote access Trojan which was discovered in September 2011 and believed to have been invented by the same authors as Stuxnet, was to *gather intelligence data and assets to enable an attack* by a worm such as Stuxnet.[30] Duqu was designed neither to damage nor destroy, yet there is evidence to suggest that the capacity of Stuxnet to achieve *its* design objective was dependent on the prior implanting of Duqu, which went undetected for four years. Nonetheless, the suggestion that a 'cyber-weapon' might be defined by its capacity for inflicting 'harm' is unconvincing for being over-inclusive.[31]

An alternative definition that begins to address the shortcomings of the above definition is any 'malicious software that possesses an offensive capability'.[32] The problem with this definition is self-evident. As with the term 'cyber-attack' which is commonly used to describe any action ranging from penetrating a network and implanting malicious codes, to downloading information and disrupting the services provided by those networks, it lacks the specificity that

28 Technology, Policy, Law, 1-2.

29 G. Intoccia and J. Wesley Moore, 'Communications Technology, Warfare, and the Law: Is the Network a Weapon System?' 28 Houston Journal of International Law (2006) 467-489, 480 citing Air Force guidance can be found in AFPD 51-4, which addresses Air Force regulatory compliance with LOAC and defines.

30 Brigid Grauman, 'Cyber-security: the vexed question of global rules' Security and Defence Agenda Report, February 2012, 30. See also Symantec Security Response briefing paper 'W32.Duqu: The precursor to the next Stuxnet' 23 November 2011; available at http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

31 Dorothy Denning, 'Reflections of Cyberweapons Controls' 16(4) Computer Security Journal (2000) 43-53, 46.

32 This definition borrows from one that was used to define conventional weapons as having 'an offensive capability that can be applied to a military object or enemy combatant'; McClelland, IRRC (2003) Volume 85, No. 850, 397-415, 405.

is necessary for legal regulation.[33] Thus, just as it is now generally recognised that it is the *effect* of the cyber-attack that determines whether or not the law of armed conflict is operationalised, a malicious code might be deemed a 'weapon' not solely by its intrinsic properties but also by the outcome it is designed to produce.[34] In other words, only if it is established that a malicious code possesses an offensive capability and there is an intention to use it in a manner which comports with its offensive capability might the malware be deemed a 'cyber-weapon'. Accordingly, it is both the offensive capability of the malicious code and the intended outcome or effect produced by that code that transforms it into a weapon that would be governed, as with any conventional weapon, by the law of armed conflict.[35]

In June 2011, it was reported that the Pentagon had developed a classified list of cyber-weapons and cyber-tools including viruses with the capacity to sabotage an adversary's critical networks.[36] This announcement would seem to suggest that the absence of international consensus on a definition for a 'cyber-weapon' might be indicative of a political impasse rather than there being any intrinsic attribute that precludes cyber-weapons from definition.[37] However, there is an enormous gulf between policy assessments and legal classification and since most of the technology relied on in an offensive capacity is inherently dual-use, and non-malicious 'software might be minimally repurposed for malicious action', drawing the line between the two is likely to be hugely challenging.[38] Even if agreement can be reached on what constitutes a cyber-weapon, whether their very properties make cyber-weapons simply incompatible with the rationale upon which arms control treaties are founded is warrants consideration.

Broadly stated, arms control treaties aim to establish legal regimes that 'deter challenges to peace'.[39] There are various categories of arms control and disarmament treaties that can broadly

33 James A. Lewis, 'Cyberwarfare and its impact on international security' (2009) UNODA Occasional Paper No. 19, 8.

34 Michael Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' 87 International Law Studies, Naval War College (2011); Charles Dunlap 'Perspective for Cyber Strategists on Law for Cyberwar' Strategic Studies Quarterly (Spring 2011) 81-99, 85.

35 This however does not resolve the definitional problem in its entirety since there will be some digital tools that only if directed at or used in a certain manner will produce an outcome, albeit indirectly, that can be equated to other traditional weapons. Since the same 'cyber-weapon' deployed in a different manner may result in an effect that is simply disruptive, regulating the use of the weapon, rather than the weapon per se may present a more viable option.

36 Ellen Nakashima, 'List of cyber-weapons developed by Pentagon to streamline computer warfare' in The Washington Post, 1 June 2011.

37 In the Shanghai Cooperation Organization's agreement on Cooperation in the Field of International Information Security which was adopted at the 61st plenary meeting of the Organization on 2 December 2008 'information weapon' is defined very broadly as 'information technologies, ways and means of waging an information war'.

38 United States Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 8.

39 Richard Betts, 'Systems for Peace or Causes of War? Collective Security, Arms Control and the New Europe' 17 International Security (1992) 5-43, 30. It is worth pondering on whether the absence of a cyber-weapons control convention has the counter-intuitive effect of promoting deterrence. The risk that an adversary has already developed and implanted malware that has the capacity to control a State's offensive and defensive capabilities may in fact serve to deter the kinetic use of force. That a State may not realise until some time later that its military capabilities have been eroded, may have a beneficial effect of instilling caution.

be grouped[40] into those that: i) limit the level of armaments;[41] ii) prohibit or restrict the use of specific weapons;[42] iii) prohibit the testing and deployment and attacks on the environment;[43] and iv) prohibit development and acquisition of specific weapons.[44] By contrast to the law of armed conflict, the objective of such regimes is to make conflict less likely by reducing the existence of, or restricting the use of certain weapons irrespective of whether the particular weapon is more or less cruel or indiscriminate than others which may not be the subject of such negotiations.[45] In addition to reducing the risk of armed conflict by imposing limitations on the development and proliferation of weapons to constrain capabilities, the purpose of such regimes can include:

- minimizing disparities among States to remove the source of instability;
- increasing predictability in relations between potentially hostile States;
- pre-empting the development of new weapons;
- decreasing expenditure on armaments to divert resources to economic and social development;
- contributing to conflict management by establishing a framework to enable negotiation between belligerent States;
- generally fostering a non-hostile atmosphere; and
- alleviating the suffering and damage in armed conflict.[46]

The distinction between the objectives of an arms treaty and LOAC is worth noting since cyber-weapons do not directly inflict the harm that LOAC is concerned with regulating. Arms treaties by contrast are generally agreed to not on the basis that the weapon is, all things considered, offensive to fundamental LOAC principles but rather because, as a matter of military and political judgment, the new restrictions can be the subject of agreement.[47] The agreement is treated as a 'contractual undertaking' adopted on the basis of a common interest: in other words, arms control treaties are the product of a policy choice rather than a legal necessity.

40 These categories of agreements were identified by Frits Kalshoven in The Centennial of the First International Peace Conference: Reports and Conclusions (2000) Kluwer Law International, 61-96.

41 1990 Treaty on Conventional Armed Force in Europe; 1972 Strategic Arms Limitation Talks I (SALT I); 1972 Anti-Ballistic Missile Systems Treaty; 1979 SALT II; the 1987 Intermediate-Range Nuclear Forces Treaty; 1991 Treaty on the Reduction and Limitation of Strategic Offensive Arms (START I); 1993 START II; START III.

42 1925 Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases and of Bacteriological Methods of Warfare; 1981 Convention on Excessively Injurious or Indiscriminate Conventional Weapons and Protocols.

43 1963 Partial Test Ban Treaty; 1974 Threshold Test Ban Treaty; 1996 Comprehensive Nuclear Test Ban Treaty; 1977 Convention on the Prohibition of Military or Any Other Hostile use of Environment Modification Techniques; 1959 Antarctic Treaty; 1967 Outer Space Treaty; 1971 Seabed Treaty.

44 1968 Non-Proliferation Treaty; 1972 Biological Weapons Convention; 1993 Chemical Weapons Convention; 1997 Ottawa Convention on Anti-Personnel Mines.

45 Christopher Greenwood, 'The Law of Weaponry at the Start of the New Millennium' in Essays on War in International Law (2006) Cameron May, 223, 231.

46 Daniel Frei 'International Humanitarian Law and Arms Control' IRRC, No. 267 November-December 1988, 491, 493-94. According to Goldblat, compared to its original narrow meaning to denote rules for limiting arms competition, 'arms control' is now often used to refer to a broad range of measures including those intended to: freeze, limit, reduce or abolish certain categories of weapons; ban the testing of certain weapons; prevent certain military activities; regulate the deployment of armed forces; proscribe transfers of some military items; reduce the risk of accidental war; constrain or prohibit the use of certain weapons or methods of war; and build up confidence among States through greater openness in military matters; Goldblat, Arms Control: The New Guide to Negotiations and Agreements, 3.

47 Ashley Roach, 'Certain Conventional Weapons Convention: Arms Control or Humanitarian Law?' 105 Military Law Review, (1984) 3-72, 17.

What is of note is that such treaties have usually aimed to construct a military balance between States based on the simple reasoning that a parity in available arsenal would in itself dissuade the resort to force because it cannot be effectively exercised.[48] Thus, the key to such treaties is the ability to maintain a balance of power between *States*.[49] This is a perfectly reasonable rationale if the particular weapon is predominantly accessible – and affordable – only to States, as in the case of nuclear weapons. In the case of malware, this rationale offers little traction. Compared with other kinetic weapons, malicious software is easy to use and relatively cheap. These two factors make cyber-weapons widely accessible to non-state actors – from criminal gangs to the lone hackers. According to McAfee, every year sees one million new viruses, from worms to logic bombs; and that figure is climbing.[50] Moreover, unlike other weapons, cyber-weapons can be reproduced and distributed globally at minimal cost.[51] Even if a significant proportion of these malicious codes are generated by State actors, that still leaves a large number being created in the private sector. In the face of the sheer volume at which malware is being constituted, particularly by non-state actors, demands for an arms treaty comparable to the Chemical Weapons Convention (CWC)[52] to prohibit 'the development, spread and use of the 'information weapon'' appears a daunting, if not futile, exercise.[53]

Nevertheless, would it be feasible to introduce a system of classification for cyber-weapons linked to the level of harm that could potentially be caused by the malware? In other words, to adopt an approach comparable to the CWC and to focus efforts on malicious codes which have been designed primarily with offensive capabilities, the use of which is likely to result in serious harm comparable to a kinetic weapon? The CWC may also offer guidance in respect of exclusion clauses, as for example, malware that is produced for the very purpose of enabling the development of new programmes to detect and counter the intended harm. But what it cannot do is to provide a template. The speed at which technology is evolving means that the methods and tools of attack are constantly altering making any listing of prohibited cyber-weapons simply redundant.

For the purpose of argument, if distinguishing between offensive and defensive cyber-weapons is possible and the former is made subject to prohibitions, this still leaves the problem of dual-use software. As the DoD noted in its 2011 report to Congress, 'most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action.'[54] Although the issue of dual-use arose in the case of the CWC and the Nuclear Non-Proliferation Treaty (clearly chemical products and nuclear energy can be produced for

48 Betts 'Systems for Peace or Causes of War?' 30.

49 This reasoning was based primarily in the context of a bipolar world in the context of nuclear weapons. Experts have suggested that where there is more than just one pair of competing powers with overlapping rivalries, arms races are likely to be interconnected, and the stability of any one pair of rivals might be affected negatively by developments in other dyads. This means that there is even greater risk of instability and this 'increased political complexity of the post-bipolar world calls for more rather than less arms control.' Harald Muller 'Compliance Politics. A Critical Analysis of Multilateral Arms Control Treaty Enforcement'The Nonproliferation Review (2000) 77-90, 78.

50 Grauman, 'Cyber-security: the vexed question of global rules', 10.

51 In addition, in contrast to for example chemical weapons, cyber-weapons can be stored with no physical risk.

52 J. Markoff and A. Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace' New York Times, 28 June 2009.

53 See 2000 Russian Federation Information Security Doctrine, section 7 on 'International cooperation by the Russian Federation in the realm of information security'.

54 United States Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 8.

both peaceful and non-peaceful purposes) in the case of cyber-weapons, the question of dual-use takes on another dimension. This is because cyber-weapons possess multiple properties (e.g. destroy, degrade, exploit, control, deceive, alter) and thus to describe them as '*dual*-use' is potentially misleading.[55] The distinction between malware that seeks to exploit (e.g. for commercial gain) or is implanted to gather intelligence (e.g. State-sponsored espionage) and malware that is potentially offensive (to destroy or control) is tenuous at best as the Duqu/Stuxnet example aptly demonstrates.

Of course, irrespective of motive, the intruder must first be able to access a system or network and identify vulnerabilities in the hardware, software, hardware-software interfaces, communication channels, configuration tables, users, and/or service providers.[56] But the 'payload' or the malicious code or programme that performs a particular action, once a vulnerability has been detected, can take many forms. A bot or botnet is sometimes designed to disable websites and networks and sometimes to gather information,[57] a 'logic bomb' which is hidden in computers to halt them at crucial times or damage circuitry is designed to degrade or destroy, a microwave radiation device that can burn out computer circuits from a distance is principally designed to destroy, a distributed denial of service (DDoS) programme aims to disrupt, and other hacking tools including viruses, worms, spyware, or Trojan horses can be designed to perform one or a combination of operations. This attribute of cyber-weapons means that, rather than identifying specific categories of malware that would be subject to prohibition, it would seem far more effective to regulate the use of such weapons.

A further distinguishing property of malware is that in contrast to conventional weapons where the State has full control over the means by which weapons are deployed, it is the private sector or individuals who have ownership and operational rights over networks.[58] As a consequence any treaty system would require, at a minimum, a commitment on the part of the private sector to collaborate in what will likely be an operation of unprecedented complexity.

What will however be the Achilles' heel of a cyber-weapons control treaty is non-compliance since there is little prospect of integrating a reliable verification mechanism into such a treaty regime. It is unlikely that any State would agree to external verification measures which would necessarily require scanning all computers and storage devices owned and used by the State including all classified systems.[59] This is a significant drawback as past experience demonstrates that the success of arms control treaties has been contingent largely on the existence of a robust compliance and verification regime. For example, although the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (BWC) entered into force in 1975 and has 165 State Parties, it has repeatedly been criticised for lacking credibility on the grounds that it contains

55 Denning has described 'dual use' weapons to include password crackers and vulnerability and port scanners; as she notes, 'great caution would be required as many of these tools help system administrators find and correct security problems'; Dorothy Denning, 'Reflections on Cyberweapons Control' 16(4) Computer Security Journal (2000) 43-53, 43.

56 P. Denning and D. Denning, 'Discussing Cyber Attack' 53(9) Communications of the ACM (2010) 29.

57 Botnets may be designed simply to gather information; botnets refer typically to ordinary computers hijacked by viruses to perform attacks without their owner's knowledge; Duncan Hollis 'Why States need an international law for information operations' 11 Lewis & Clark Law Review (2007) 1023-1061, 1025.

58 GGE report, 6, A/65/201.

59 Dorothy Denning, 'Obstacles and Options for Cyber Arms Controls' presented at Arms Control in Cyberspace, Heinrich Böll Foundation, Berlin, Germany, 29-30 June 2001, 3.

no effective verification provisions.[60] The combined effect of having no means by which to independently verify compliance together with the ease at which malware can be secreted and the high degree of anonymity in cyber-space which makes the tracking of the origin of the malware and the discovery of the identity and motivation of its author hugely challenging, will inevitably mean that in the event of a serious and sophisticated cyber-attack, accusations of State sponsored involvement will persist. The uncertainties regarding attribution suggest that an arms control treaty is neither likely to increase the predictability in relations between potentially hostile States nor foster a more cordial atmosphere. If these are indeed the objectives sought by the proponents of an arms control treaty, there are perhaps more effective ways to secure such goals.[61]

In calling for the convening of the 1899 and 1907 Hague Peace Conferences, Russia was motivated by two factors: that, due to its economic weakness, it could not compete in the arms race with its rivals and in addition, its precious resources were being channelled into unproductive ends, namely, armaments.[62] This latter argument – that economic and social development should not be sacrificed for the benefit of military aggrandizement – was revived during the 1970s and 1980s under the UN rubric 'disarmament and development'.[63] In contrast with other weapons, cyber-weapons may paradoxically turn this argument on its head since the cost of enforcing a global prohibition may exceed any expected reduction in the level of risk. Moreover, as defensive tools acquire greater sophistication and capacity to detect and effectively respond to malicious codes, a complex regime to effectively monitor treaty compliance may prove far from cost-effective and even of subsidiary importance much in the same way that the utility of chemical weapons diminished considerably with the development of protective equipment.[64]

In the absence of agreement for an arms control treaty I consider in the following section whether existing LOAC rules offer an adequate basis for regulating cyber-weapons and their use. Since by contrast to other weapons, attacks using cyber-weapons are not primarily intended to produce a direct but rather an indirect kinetic outcome, does this require the re-evaluation of how LOAC rules pertaining to the means and methods of warfare apply? In particular I ask whether cyber-weapons are challenging to the law because they represent the essence of an ever

60 As experts have observed despite more than six years of negotiation on a proposed verification protocol, in 2001 the US withdrew its support although this came as little surprise given that the terms of the proposal were regarded by many of the participants as intrusive. See for example, Michael Moodie, 'Fighting the Proliferation of Biological Weapons: Beyond the BWC Protocol' 4 Disarmament Forum (2000) 33-42 and Kenneth Ward 'The BWC Protocol: Mandate for Failure' The Nonproliferation Review (Summer, 2004) 1-17. By contrast, verification under the CWC includes compulsory national declarations about relevant industrial and military activities, and a regime of routine inspections of declared industrial and military facilities. A particularly important feature is the provision for a 'challenge inspection' whereby a State party can request an inspection of any site in another State party at short notice; Robert Mathews and Timothy McCormack 'The influence of humanitarian principles in the negotiation of arms control treaties' IRRC No. 834, 30 June 1999.

61 '[U]ncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception'; Group of Governmental Experts report, 7 paragraph 7. 'The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult'; United States Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 8.

62 Goldblat, Arms Control: The New Guide to Negotiations and Agreements, 2.1.

63 Kalshoven, The Centennial of the First International Peace Conference: Reports and Conclusions, 97.

64 Mathews & McCormack, 'The influence of humanitarian principles in the negotiation of arms control treaties', 4.

inter-connected world in which conceptual and physical boundaries are being eroded, the very foundations upon which the law itself was constituted.

4. THE LAW OF ARMED CONFLICT: MEANS AND METHODS

It is self-evident that the ever-expanding use of information and communication technology in the critical infrastructure of States has created new vulnerabilities and opportunities for disruption, not least in the context of armed conflict.[65] Moreover, as the 2008 conflict in South Ossetia all too clearly demonstrates, adversaries will increasingly resort to strategies involving digital tools as an integral part of any military operation. Since the law of armed conflict applies to all situations that fulfil the criteria of an armed conflict, there is no coherent reason why the rules pertaining to the means and methods of warfare should not apply irrespective of methodology if the effects of deploying the malware produce the same outcomes as a kinetic weapon.[66] In fact, LOAC explicitly anticipates the emergence of new weapons and in doing so requires States to determine whether the use of any new weapon, means or method of warfare would be prohibited by international law.[67]

The law of weaponry which seeks to regulate both the means and methods of warfare can be traced back many centuries and its rules and principles are found in treaty and customary international law and in the growing body of case law generated by international courts and tribunals.[68] Although the St Petersburg Declaration is often cited for having been the first treaty to ban a particular type of weapon, a more important aspect of the Declaration is its preamble which, in setting out the reasoning behind the prohibition, articulates the general principles that have continued to inform the evolution of the law as it has confronted new means and methods of warfare.[69] The preamble reads:

> 'That the only legitimate object which State should endeavour to accomplish during war is to weaken the military forces of the enemy, […]
>
> That this object would be exceeded by the employment of arms which aggravate the sufferings of disabled men or render their death inevitable, [and]
>
> That the employment of such arms would, therefore, be contrary to the laws of humanity.'

65 GGE report paragraph 9, (A/65/201).

66 Commenting on the list of so-called weapons or 'fires', a senior military official indicated that the deployment of, for example, a computer virus would be governed by the same rules that apply to other military weapons, in other words, IHL; see The Washington Post, 1 June 2011.

67 Article 36 of Additional Protocol I provides, 'In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.'

68 As Greenwood notes, by the late 19th century, there was considerable support for the proposition that international law imposed some constraints upon the weaponry which a belligerent might employ; Greenwood, 'The Law of Weaponry at the Start of the New Millennium', 226.

69 The 1868 St Petersburg Declaration prohibited the 'use of explosive and incendiary projectiles weighing under 400 grammes which is either explosive or charged with fulminating or inflammable substances'. The convention did not prohibit the use of explosive projectiles per se as such weaponry was considered to be militarily necessary.

Two principles can be extrapolated from this. The first invokes the concept of military necessity, according to which only those weapons and means of combat which are necessary to attain the military purposes of war are permitted; this was subsequently given further weight with the incorporation of Article 22 of the 1907 Hague Regulations which explicitly provides that 'the right of belligerents to adopt means of injuring the enemy is not unlimited' (Article 22). More specifically, Article 23(e) prohibits the employment of 'arms, projectiles, or material calculated to cause unnecessary suffering'.[70] This principle is understood to prohibit both the use of weapons calculated to cause unnecessary suffering (means) and the use of otherwise lawful weapons if used in a manner that causes unnecessary suffering since to do so would serve no military purpose (methods).[71] A more recent expression of this principle is found in Article 35(2) of Additional Protocol I which provides that:

'It is prohibited to employ weapons, projectiles and materials and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.'[72]

At first glance it is difficult to see how this prohibition would apply to cyber-weapons since the principle is concerned with the superfluous injuries and unnecessary suffering directly inflicted by the particular weapon on a combatant. Unlike in the case of other weapons, this principle would therefore appear to have little purchase on cyber-weapons insofar as their direct effects are concerned. If, however, the indirect effects of such weapons are taken into consideration it may be that malware designed to carry out specific tasks may potentially violate the principle, as for example where the destruction of medical data results in the provision of improper care of wounded combatants.[73]

Although the principle of unnecessary suffering has historically served as a basis upon which some weapons have been prohibited,[74] a compelling case can be made that the principle may make the use of cyber-weapons *more* likely. This is because if 'the essence of the unnecessary suffering principle is that it involves a comparison between different weapons in determining whether the injuries and suffering caused by a particular weapon are necessary', the cyber-weapon has the potential – to the frustration of those who wish to see its total prohibition – to 'outclass' all conventional weapons by inflicting least suffering.[75] Echoing the findings of a 1999 Department of Defense report, Denning observes 'instead of dropping bombs on an enemy's military communication systems, for example, cyber forces could take down the system with a computer network attack, causing no permanent damage and no risk of death or injury to soldiers or civilians. The operation would be more humane and should be preferred

70 The principle does not possess an absolute character because it only prohibits weapons that cause unnecessary suffering that cannot be justified by the military advantage that may be gained from its use.

71 'The only legitimate purpose of any use of weapons is the disabling of enemy combatants'; Dieter Fleck, Humanitarian Law in Armed Conflicts (1999) OUP, 121. The ICJ has described the principle of unnecessary suffering together with the principle of distinction as the two cardinal principles of international humanitarian law; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, paragraph 78.

72 See also rule 70, ICRC Customary International Humanitarian Law Study.

73 Arie Schaap, 'Cyber warfare operations: development and use under international law' 64 Air Force Law Review (2009) 121-174, 159.

74 For example, Declaration Concerning Expanding Bullets, 1899; Protocol on Non-detectable Fragments (CCW 1980, Protocol I); Protocol III (incendiary weapons primarily designed to set fire to materials, objects or to cause burn injury to persons; Gas Protocol 1925: prohibits use of chemical weapons directly against the enemy and to the toxic contamination of war-supply installations and food-stuffs; Biological Weapons Convention 1973; Chemical Weapons Convention 1993.

75 Greenwood, 'The Law of Weaponry at the Start of the New Millennium', 240.

over more destructive alternatives'.[76] Whether there would be an *obligation* on technologically advanced States to resort to digital options that cause less suffering if doing so does not reduce their military advantage remains far from clear.

The second general LOAC principle that unambiguously applies to cyber-weapons is the prohibition on the use of indiscriminate weapons or the indiscriminate use of any weapon. Once again, as with the principle of unnecessary suffering, these principles must be interpreted as applying to the intended indirect effect of the malware since 'the computer or network attacked is much less relevant than the systems controlled by the target computer or network […] [and] indeed the indirect effect is often the primary purpose of the attack'.[77]

As Greenwood notes, the principle of discrimination is a compound of three separate principles of customary international law: the principle of distinction, the principle of proportionality and the requirement to take all feasible precautions.[78] It therefore follows that if a particular cyber-weapon is incapable of being used in a way which enables a distinction to be drawn between military targets and civilians or civilian objects, it is inherently indiscriminate and therefore unlawful.[79] To the extent that a particular cyber-weapon can be deployed to attack a purely military objective and its destruction or neutralization provides a definite military advantage, the use of the malware would comply with the law.[80] Malware that cannot be contained or controlled and one that may cause injury to civilians or damage to civilian objects will constitute a prohibited indiscriminate weapon.[81] The proportionality principle which requires a balancing of the military advantages to be gained from an attack on a military target against the expected civilian harm and damage is even more difficult to evaluate for cyber-weapons given the interconnectedness of civilian and military networks.[82] This means that unless a rigorous assessment of the potential unintended consequences is conducted, a legitimate objective of attack may result in excessive collateral damage rendering the use of the malware unlawful in the circumstances.[83] As with the principle of unnecessary suffering, if the use of a cyber-

76 Denning, 'Obstacles and Options for Cyber Arms Controls', 7. See also Michael Schmitt, 'War, Technology, and International Humanitarian Law' HPCR Occasional Paper Series (2005), 55-56. See also DoD report As Assessment of International Legal Issues in Information Operations, May 1999, at 45: 'there is an obvious military interest in being able to interfere with an adversary's information systems, and in being able to protect one's own. Used as an instrument of military power, information operations capabilities have the significant advantage that they minimize both collateral damage and friendly losses of personnel and equipment. Their use may avoid unwanted escalation of a dispute or conflict'.

77 Technology, Policy, Law, 19.

78 Greenwood, 'The Law of Weaponry at the Start of the New Millennium', 242-243. See also ICRC Study, Rule 71.

79 'States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets'; Legality of the Threat or Use of Nuclear Weapons, paragraph 78.

80 Article 52(2) of Additional Protocol I requires that attacks are limited strictly to military objectives. It further provides that military objectives are limited to those objects which by their nature, location, purpose or use make and effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

81 Article 51(4)(c) of Additional Protocol I defines indiscriminate attacks as 'those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol.' See also Schmitt, 'War, Technology, and International Humanitarian Law' footnote 114.

82 Technology, Policy, Law, 81 and 121-26.

83 '…cyberattacks aimed at military computer systems can have unforeseen consequences for civilian computers. Dams, nuclear power stations and civilian air traffic control all need computers in order to operate and to stay safe'; 'Cyber warfare and IHL' ICRC comment of 16 August 2011. For examples, see Schaap, 'Cyber warfare operations', 159.

weapon can secure the same objective as one involving the use of a kinetic weapon, it may well be the case that LOAC's obligation to take precautions in attack requires the State to the use of the former means because the risk of collateral damage and incidental injury would be considerably lower.[84]

Although the primary concern of this paper is with the law of weaponry and the means and methods of warfare, some comment is merited in respect of the rules on targeting. Although often conflated, because the principles that form the basis of a judgment as to whether a particular weapon or its use complies with the principle of discrimination are also relevant in respect of targeting, these two topics address separate questions. Be that as it may, discussions involving cyber-weapons consistently prompt two inter-related questions: the first concerns dual-use facilities; the second, whether the critical infrastructure of a State should be immune from a cyber-attack. The law regarding the former is fairly well settled since the question of targeting dual-use facilities is not unique to cyber-weapons.[85] Dual-use targets are understood as those that are used for both military and civilian purposes, as for example, power plants, oil and gas facilities, railroad and other transportation systems. In the digital age, this list has expanded to include, for example, computer networks of certain research facilities, air traffic control networks regulating both civilian and military aircraft, computerized civilian logistics systems upon which military supplies will be moved, electronic grid control networks, communications nodes and systems including satellite and other space-based systems.[86] For an object to qualify as a military objective, the target must 'make an effective contribution' to the enemy's military action; in other words, its destruction must provide a definite military advantage to the attacker.[87] The phrase 'make an effective contribution' is broad in scope and does not limit targets to only military objectives but to objects that make an effective contribution to the military; such objects may concurrently be of vital interest to the civilian population, as the examples above illustrate. However, before the target can be attacked, a proportionality test must be applied to ensure that the collateral damage to civilians or civilian objects is not excessive in relation to the concrete and direct military advantage anticipated.[88]

In a digitalized age, not only has there been an unprecedented increase in the number of potential targets that are dual-use in nature, but because networks are so interconnected, the resultant harm of an attack using malware is potentially enormous. Complying with existing LOAC rules that extend protected status to an area, or personnel or infrastructures will in practice be more difficult to observe since the interconnectedness of contemporary global society makes isolating specific interests that much more testing. For example, modern hospitals are 'highly networked facilities, dependent on telemedicine, and continuous retrieval of geographically remote information that is most likely stored in a data center that also houses other industrial

84 Article 57(2)(a)(ii) of Additional Protocol I requires those who plan or decide to pursue an attack to 'take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects.'

85 For example, see Lawrence Greenberg, Seymour Goodman, Kevin Soo Hoo 'Information Warfare and International Law' National Defense University Press (1998) 12 and 37.

86 Schapp 'Cyber warfare operations' 156.

87 Article 52(2) of Additional Protocol I defines military objectives as 'limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.

88 Article 51(5)(b) provides that an indiscriminate attack is one which 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.

and administrative data, and possibly even defense-related data.'[89] If such facilities are considered dual-use because they store defence-related data that is considered to make an effective contribution to the military action, would its destruction by the release of malware be lawful as long as the proportionality rule was satisfied? This has led some to suggest that certain critical infrastructures that are reliant on networks for their effective performance should be designated as immune from attacks by cyber-weapons.[90]

This cursory and partial[91] examination of existing LOAC rules suggests that the advent of the 'cyber-weapon' does not render the law obsolete. Nevertheless, as observed, 'applying pre-existing legal rules to a new technology raises the question of whether the rules are sufficiently clear in light of the technology's specific – and perhaps unprecedented – characteristics, as well as with regards to the foreseeable humanitarian impact it may have.'[92] Since malicious codes are designed to have different – and sometimes multiple – intended objectives, distinguishing between exploitation, intelligence-gathering, disruptions and conduct that is the prelude to something more serious will be challenging at best.[93] It may prove impossible to detect the existence of an armed conflict; destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems may amount to use of force but it is unlikely to be regarded as an armed attack unless the outcome results in loss of life, injury and damage. But by contrast to an equivalent kinetic attack, the perpetrator may be difficult to identify since malware is often routed through servers in different countries. Perhaps more than any other domain of warfare, the unintended consequences in this new domain are the most troubling – both in respect of mistaken attribution and the level of harm that the deployment of a particular malware may inflict on the civilian population. While a cyber-weapons treaty or code of conduct will clearly not address all the most pressing issues pertaining to cyber warfare, it may assist in resolving some.

89 Karl Frederick Rauscher and Andrey Korotkov, 'Working toward rules for governing cyber conflict' EastWest Institute (2011) 22.

90 One problem that would first need to be overcome is that there is no consensus on what comprises the critical infrastructure. One definition is provided in the US Patriot Act, Section 1016(e), October 2001 which states: '[…] systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'; cited by Rauscher & Korotkov, 'Working toward rules for governing cyber conflict', 12.

91 Issues that are not addressed in this paper include for example the protection of the environment, perfidy, neutrality.

92 'International Humanitarian law and New Weapon Technologies' Keynote address by Dr Jakob Kellenberger, ICRC, 34th Roundtable on Current Issues of International Humanitarian Law, San Remo, 8 September 2010. See also United States Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 8 which also concludes that 'the principled application of existing norms must be developed' to 'to clarify the application of norms and principles of customary international law to cyberspace'.

93 Technology, Policy, Law at 116. See also 2011 DOD strategy 9 on different categories of activities.

5. TENTATIVE CONCLUSIONS AND A POINT OF DEPARTURE

The prospect of a cyber arms control treaty cannot be dismissed outright since such treaties are always the product of a political choice governed by ever-changing priorities and perceived vulnerabilities. Once thought beyond effective proscription, mounting concerns over the horizontal proliferation of chemical weapons combined with the recognition by both the US and Russia that they did not need to retain their chemical weapons stockpiles following the Cold War culminated in the CWC.

That there is now greater willingness among States to enter into a dialogue on the implications of this new technology to armed conflict is to be welcomed. Where disagreement still persists is on the objectives that are being sought. For those that champion an arms control treaty, the critical question is whether there is any compelling reason why this particular weapon should be prohibited? As inferred above, the historical reasoning upon which other arms control treaties have been successfully negotiated and implemented have little bite. This is because in contrast to kinetic weapons, cyber-weapons are relatively inexpensive and widely accessible to non-state actors; the identity of the originating party behind a significant cyber-attack can be concealed with relative ease compared to that of a significant kinetic attack; it would be impossible to destroy all copies of the malicious code which may be stored in countless digital devices across the globe; and an effective inspection or verification mechanism is unlikely to materialise. Moreover, by contrast to other weapons that command public condemnation because they appear unambiguously indiscriminate or inflict unnecessary suffering, cyber-weapons are often regarded as a panacea that can achieve precisely the opposite: sanitize warfare and even prevent the use of kinetic force. Thus, rightly or wrongly, there is little public appetite to support a total ban.

In March 2009 Vladislav P. Sherstyuk, Deputy Secretary of the Russian Security Council, raised the possibility of a treaty to ban States from secretly embedding malicious codes or circuitry that could be later activated from a distance in the event of war. This comment raises an interesting question as to what constitutes a cyber-weapon, a question that I have attempted to answer above. However, if malware can be implanted that completely debilitates the armed forces of a State from resorting to kinetic force and does so without causing any casualties or damage, is such a device a weapon as understood under LOAC? The Stuxnet virus may have violated the principle of non-intervention and prohibition on the use of force but was its use governed by LOAC?

Such questions would probably not be answered by any multi-lateral agreement or code of conduct but a formal agreement of some form would provide a valuable framework within which to facilitate direct communication between States particularly in times of tension or crisis. The most serious threat that cyber space has engendered is the potential for armed conflict as a consequence of mistaken identity or alternatively, a misinterpretation as to intention.[94] The similarities between a cyber-attack and cyber exploitation mean that a targeted party may not

94 'After a call for a US-Russian bilateral high-level cyber security working group from Moscow in February 2011, US and Russian Delegations met in June with the goal of 'preventing misunderstanding and inadvertent escalation of cybersecurity incidents'; Joshua McGee, 'US-Russia Diplomacy – the 'Reset' of Relations in Cyberspace' Center for Strategic & International Studies, 5 August 2011 available at http://csis.org/blog/us-russia-diplomacy-reset-relations-cyberspace.

be able to distinguish between the two raising the risk of unwarranted or misinformed decisions in response.[95] This is compounded by the very nature of cyberspace such that there is now a need for more rapid responses creating higher levels of risk that a mistake will occur. A formal agreement may assist in addressing this problem possibly through a procedural mechanism or through the creation of an independent technical body that would assist with identifying sources of attack. A multi-lateral agreement would contribute to confidence-building, create an opportunity for States to affirm the applicability of LOAC principles and rules to cyber warfare and allow for the articulation of new norms should they be required. Such an agreement would also present an ideal opportunity to clarify the cyber lexicon and potentially allow for agreement to prohibit the use of cyber-weapons against critical infrastructures including for example, national power grids, financial markets or institutions, air traffic control systems.[96]

The modern law of armed conflict is founded on clearly delineated boundaries both conceptual and real. This vision of the world and the laws that were constituted upon this vision are now being challenged by cyber-space that thrives on the absence of boundaries. By their very properties, cyber-weapons are forcing us to re-evaluate our pre-conceptions about the nature of space, how we order our world, and the values which we most seek to preserve, not least in times of conflict.

95 Denning 2010; see also National Research Council, Letter report for the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 25 March 2010, 3. 'Cyberattack and cyber exploitation are technically very similar, in that both require a vulnerability, access to that vulnerability, and a payload to be executed. They are technically different only in the nature of the payload to be executed. These technical similarities often mean that a targeted party may not be able to distinguish easily between a cyber exploitation and a cyberattack.'

96 National Research Council, Letter report for the Committee on Deterring Cyberattacks, 21.