Challenges for Non-Proliferation and Disarmament in the Field of Information Communications Technology

Executive Summary and Recommendations

Alexander Lee
584665@soas.ac.uk

I. Introduction

It is taken for granted that at any level of operation, from personal interconnectivity to the stable operation of national critical infrastructure, network dependency is deepening in all societies. This increased engagement with information communications technology has occurred in all societies irrespective of the differences in capacity. Increasingly sophisticated information and telecommunications technology (ICT) is now an essential underpinning of successful economic and social development. Based on this reason alone, all states should recognise that the domain of ICT should be a peaceful, secure, open and cooperative environment.

However, insecurity characterises the domain of information communications technology with security concerns fixed upon the malicious employment of ICTs by States as instruments of warfare and intelligence. This has fuelled what may be loosely termed a cyber-arms race among a small number of States generating an environment of uncertainty and mistrust for all. In 2012, in a McAfee released the findings of a survey of cybersecurity experts from 250 leading authorities on the subject, 57% believed that an arms race was taking place. [1] The proliferation of offensive information communications technologies among States and non-state actors represent a system-level threat to international security, and whose effects may be of substantial disruption and damage to the global economy, the security of nations and the stability of the international community as a whole. While this danger has been universally recognised by all UN Member States, it should also be realised that the issues regarding ICT-security are too complex for any one State to address by themselves.

Since the arms race is relatively immature, the intellectual architecture for describing the strategic environment is still not fixed with meaning: notions such as offense, defence, deterrence, escalation and the particularity of what is a weapon in information or cyber-terms are not well-defined. In this regard, the cyber arms race of the 2010s resembles the uncertainty of nuclear strategy of the 1950s. While this poses serious intellectual challenges, especially to any proposal of an arms control treaty to govern cyber-weapons, it presents a unique opportunity to reshape the character of international relations, and a way for the

[1] Götz Neuneck, ‘Chapter 1, Civilian and Military Capabilities: Shifting Identities and Attribution’, in Götz Neuneck & James A. Lewis, ‘The Cyber Index: International Security Trends and Realities’, United Nations Institute for Disarmament Research [UNIDIR] (March 2013)

United Nations as a multilateral vehicle to reassert its relevance in mediating and managing the security concerns and disputes of States and their sovereign peoples.

Following by way of historical analogy, the recommendations of this paper do not set out intending to be a definitive arms control treaty to the like of the Chemical Weapons Convention. Indeed, multilateralism has been most effective in applying retroactive regulatory frameworks after devastating fait accomplis. However, in this case serious challenges at a technical level and a normative one prevent the regulation and governance of any weapon system associated with information communications technology. This paper instead seeks to proactively address security concerns of States by meaningfully reducing uncertainty and risk by managing the number of actors in the domain, directly increasing predictability in State relations, through the creation of a normative agreement on the conduct of cyber-relations in peace and war that may act as a 'best fit' agreement to prevent the excesses of unrestricted cyber-war and cyber-insecurity.

Note that the terms ICT and the 'cyber' prefix will be used interchangeably. This is not to reflect a Western bias for cybersecurity but of practicality, as the frequent use of ICT is cumbersome.

II. Emergent Threats

Information communications technology has created an arena for new and old strategic interests. Threats to international security arise from a series of problem sectors. However, these problem sectors are too complex to address unilaterally. As will be apparent, these aggregate threats cut across horizontal cleavages and require co-operation between states and their public and private institutions cross-borders and across levels of society.

1) The greatest threat is that an environment of uncertainty has been generated by a small number of States who use ICT as tools of warfare and intelligence, prompting an escalatory circle of militarisation among other States. It is believed that approximately a dozen countries possess cyberwarfare capabilities of an advanced kind with a further 30 who identify cyber-operations as a military priority.[2]

    a) In addition, State theorists are normalising a theory of interstate cyber war producing destabilising effects. While there are strong incentives for States to pursue ICT-based warfare seriously, either as a primary mode of warfighting or complimentary to existing electronic warfare, interstate cyber war will result in massive civilian casualties. Cyberspace promotes the use of countervalue military strategy, with echoes of 'nation killing' in 1950's nuclear strategy, which will target the nation's capacity to sustain war.[3] In practical terms, this will result in the deliberate targeting

[2] James A. Lewis & Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR (2011)

[3] Consider the discourse in early nuclear strategy over 'nation killing' and also the rationalisation of nuclear warfare in 'counterforce' strategy.

of critical national infrastructure and other 'dual-use' targets especially in communications, transportation and energy.

b) Moreover, the preparation for interstate cyber war involves the compromise and intrusion of state's security systems to 'prepare the battlefield'. This may involve an intelligence component: reconnaissance of enemy network systems, and also a speculated and disputed sabotage component: the implantation of logic-bombs and other malware to be used in the event of an attack.[4] On this phenomenon, De Spiegel ran a piece earlier in 2015 based on additional Snowden leaked files that reveal activities of some agencies are tending towards 'preparing the battlefield'.[5]

c) Cyber-warfare has been tied to the security of the space domain. The tools of weaponised ICT are perceived as means to redress strategic imbalance perpetuated in technological terms. A lack of consensus regarding weapon systems designed to destroy space-based property and a trend toward satellite-reliant informationized doctrines in militaries has prevented progress in the space domain and this has knock-on effects for cyberspace.

2) Ideologically motivated non-state actors of both violent and non-violent kinds utilise ICT either as their primary tool-set or complimentary to existing actions in the physical space. ICT is attractive to smaller actors because of the low cost of entry, anonymity and asymmetric vulnerability. Two trends can be identified, first that non-violent non-state actors tend to restrict their operations to ICT-based ones (ie. hacktivists largely use ICT as a means of protest and subversion) while violent non-state actors have used ICT as a medium for information operations and have yet to weaponise ICT (ie. terrorist groups internationally have largely used ICT for propaganda)

   a) There may be a trickledown or blowback from interstate competition in ICT-based warfare resulting in non-state actors intensifying their efforts to seek strategic parity in cyberspace. Furthermore, this will relate to cyber-actors in the black market who develop malware. This is evident in the replication of the weaponised code of Stuxnet.

3) Non-state actors with a primary motive of profit proliferate secure access and disruptive ICT tools for the purposes of crime and other illicit activities. This sector shares characteristics with ideologically motivated non-state actors but are differentiated by the assessment of their criminalisation. Profit-motivated non-state actors contribute an illegal alternative market for cyber-actors.

[4] Logic bombs are programmed to cause failures in the operation of programmes at certain stages, eg. Stuxnet had three logic bombs to cause machine failure in centrifuges.

[5] Jacob Appelbaum et al., 'The Digital Arms Race: NSA Preps America for the Future Battle', De Spiegel (17 January 2015), available: http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html, accessed 24/02/2016

4) Private sector actors operating to provide ICT services for States are oriented by the dual focuses of interstate competition and private individual need for security. Private sector actors are overwhelmingly oriented towards developing the tools for intrusion that make warfare and intelligence possible without adequate oversight or regulation. Such tools include espionage and surveillance programs and looking for zero-day vulnerability exploits.

III. Main Challenges to Multilateralism

In face of aggregate and complex threats, multilateral engagement offers the best route for comprehensive agreement to reduce uncertainty in the strategic environment and promote the resolution of security concerns through cooperation rather than unbalanced deterrence. However, multilateralism has been slowed by serious challenges to its effectiveness.

Semantic

5) The lack of robust definitions in the sphere of ICT impedes communication of States and ultimately produces misunderstanding. There is disagreement in the international community regarding terminology, with preferences for cybersecurity or information security linked to greater concepts regarding state sovereignty and the access to the World Wide Web as a global technological commons.

6) The intellectual architecture that gives meaning to the use of terminology such as ‘weapon’ is immature. Consensus over what constitutes a weapon represents both a semantic challenge and a technical one. Disputes are largely about differences between direct kinetic and indirect kinetic outcomes: destructive programs cause damage through the manipulation of existing vulnerabilities; they do not cause kinetic damage by themselves. As earlier noted, in order for cyber war to occur, opposing states must prepare the battlefield through extension intrusion, reconnaissance in depth and implantation. Weapons lack clear defined roles in ICT as they may perform the tasks of intelligence, communication and disruption. Semantic differences between the use of ‘information weapon’ and ‘cyber-weapon’ exacerbates this problem.

    a) It follows that semantic disputes over what is and is not a weapon is more easily solved by addressing the outcomes of the ICT tool than the intrinsic qualities of a cyber-weapon. However, this would lock-out the possibility of establishing a global arms control regime for ICT.[6]

Normative

[6] Louise Arimatsu, ‘A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations’, 4th International Conference on Cyber Conflict (NATO CCD COE, Tallinn, 2012)

7) There is a particular dispute whether transborder information content can be controlled as a matter of national security. The *International code of conduct for information security*[7] put forward by China, the Russian Federation, Tajikistan and Uzbekistan called for the compliance of States to respect the universally recognised norms regarding sovereignty, territorial integrity and political independence. As a result, while cybersecurity is largely concerned with the syntactical and physical protection of ICT infrastructure (software and hardware), information security is used to suggest a State right to the semantic content of information. As such it is largely believed that information security is understood as a right to limit the access of citizen to the public cyberspace.

8) There is disagreement as to what constitutes an armed attack. The Russian Federation tabled in the *International code* that cyber-intrusions should constitute interstate aggression. Furthermore, the immaturity of the cyber-deterrence concept is demonstrable in ill-defined thresholds for state retaliation. While some states may prefer to use in policy documents the notion of 'serious consequence', this threshold is yet to be defined and communicated clearly.

    a) A prohibition on cyber-intrusions would also prohibit interstate espionage, and notably no consensus on the legality of the practice exists internationally.

9) In theory, current international agreements provide many of the guarantees needed to de-escalate tensions between States regarding militarisation of ICT and the conduct of cyber war. The Law of Armed Conflict (LOAC) espouses as a general principle that the only legitimate object in war between States are objects of military value. Due to the dual-use nature of many ICT targets, in war time many objects used by civilians could be reasonably seen as military targets producing effects that are definite military advantages.

    a) However, this breaks the second general principle that military action is prohibited from causing superfluous injury or unnecessary suffering. Military doctrine has yet to communicate a consensus on the ethics of targeting critical national infrastructure in order to affect a change in the nation's will to fight.

    b) Furthermore, cyber war will rely on the element of surprise to be most effective. Weapons are best utilised covertly to prevent the target from having the ability to close vulnerabilities.

10) Communication between States in matters of policy and military doctrine is vague and ill-defined, and moreover there is rational cause to disregard reassurances as ploys to cover for first-use. Not only has the thresholds for escalation been ill-defined foregoing the

[7] UN General Assembly Doc., Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*,* A/66/359 (14 September 2011)

possibility of ‘firebreaks’ as moments to step away from escalation, States seeking advantage over the enemy using ICT have little incentive to declare the extent of their military operations in the ICT-sphere.

Technical

11) Attribution is technically difficult. Cyber-actors lack identity markers or other ‘functionally observable differences’ that aid in identification of aggressing forces. Although, location is possible, it is not possible to distinguish between civilian or military intent behind the transmission of a cyber-attack.

    a) The capacity to attribute an attack is a key component to registering violations to a given accord.

    b) Proxy and false flag attacks further complicate attribution making State intent difficult to assess.

12) Verification technology is unable to keep up with the proliferation of malware making the endeavour of tracing and banning ‘cyberweapons’ futile. Nor would it make much sense to call for States to submit to an international authority that would scan the hard-drives of military agencies. Cyberweapons are exceptionally easy to conceal and no State would consent to a full scan of its computer systems.

    a) It also follows that it makes identifying States with break-out weapons programmes impossible to detect.

Strategic

13) The use of ICT for malicious purposes is expedient for strategic interests, as a result well-developed ‘Cyber Powers’ will unlikely to accept major reductions in their pre-existing programmes of surveillance, interstate intrusion, and warfare.

14) Additionally, smaller States actors who perceive ICT as a means to obtain strategic parity are unlikely to give it up as well. Great ‘Cyber-Powers’ are likely to possess greater ICT-integration and therefore are more likely to be affected by cyber-warfare. This is ideal for States seeking competitive advantage, cyber-warfare is a domain to seek new coercive tools to redress strategic concerns in other domains.

IV. Main Recommendations

International security is at critically high risk from a combination of escalating and emerging threats, and slow policy making hindered by semantic, normative, technical and strategic challenges. Policy making at an international level needs to engage more proactively to prevent and regulate malicious information communications technology.

International security diplomacy has been most successful in countering new threats when acting proactively with preventative strategies than permitting threats to develop, set precedents and then retroactively applying regulation. Malicious ICT is a system-level threat that no State can robustly address unilaterally, rather it is multilateralism that should be advanced as the vehicle of the day.

However, it should be noted that despite stressing the primacy of the State it is also key to engage in two-track diplomacy with non-state actors and private interests. The ICT-sphere is a multi-stakeholder project requiring the use of incentives and negotiation to bring about a secure settlement.

Reduce Uncertainty

15) Uncertainty needs to be reduced in the ICT-sphere through a combination of 'rules of the road' agreements and 'actor reduction and regulation' initiatives. The first of these is the role of bilateral and multilateral diplomacy in achieving consensus over shared definitions that will allow for constructive dialogue to communicate security interests.

16) Furthermore, acceptable State behaviour should be clarified and norms established. These should include proscriptions for ICT-based warfare such as: avowing first use, reaffirming the demilitarization of Outer Space, banning the testing of ICT-weapons outside the environment of war, affirming a humanitarian imperative to avoid unnecessary harm which includes an obligation for discriminatory targeting and design of ICT-weapons.

    a) This proscription should also agree on an inventory of objects for which military attack by ICTs is prohibited. Precedent exists in the 2010 Beijing Convention and Beijing Protocol on Civil Aviation that criminalized technological attacks on civil air navigation facilities and aircraft in flight.

    b) Furthermore, perfidy about the use of malicious ICT should be an international crime.

17) States should cooperate on matters of transborder cyber-crime to a greater degree, incorporating international agencies. Malware databases should be shared and cyber-criminals should be considered for extradition.

18) States should re-design contracts and engagement with the private sector to focus on improving network resilience and engage with civic society through funded initiatives promoted through civilian enforcement.

Confidence Building Measures

19) Regular dialogue in multilateral and bilateral forums should be agreed to and States should be held accountable to maintaining these talks.

20) States should establish Computer Emergency Response Teams (CERT) and promote the establishment of CERTs in States with less capacity. This should also include communication channels for de-escalation during crisis.

21) States should all uphold that information communications technology should be employed in peaceful and cooperative ways and that the military interest in cyberspace should be limited and disarmed.

References and Select Bibliography:

Jacob Appelbaum et al., 'The Digital Arms Race: NSA Preps America for the Future Battle', De Spiegel (17 January 2015), available: http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html, accessed 24/02/2016

Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations', 4th International Conference on Cyber Conflict (NATO CCD COE, Tallinn, 2012)

Caroline Babylon (ed.), *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives* (Chatham House, 2014)

Caroline Babylon et. al., *Cyber Security at Civil Nuclear Facilities: Understanding the Risks* (Chatham House, 5 October 2015)

Ivanka Barzashka, 'Are Cyber-Weapons Effective?', *RUSI Journal* 158:2 (May 2013)

Lawrence Cavaiola, David Gompert and Martin Libicki, 'Cyber House Rules: On War, Retaliation and Escalation', *Survival* 57:1 (February 2015)

Paul Cornish et. al., *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House, 2009)

Götz Neuneck & James A. Lewis, *The Cyber Index: International Security Trends and Realities*, United Nations Institute for Disarmament Research [UNIDIR] (March 2013)

James A. Lewis & Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR (2011)

Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, 2007)

Jon Lindsay, 'Exaggerating the Chinese Cyber Threat', Policy Brief, Belfer Centre for Science and International Affairs (May 2015)

Jon Lindsay, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39:3 (Winter 2014)

Paul Meyer, 'Cyber-Security Through Arms Control: An Approach to International Co-operation', *RUSI Journal* 156:2 (April/May, 2010)

Bruce McConnell et al., A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets, EastWest Institute (January 2014)

Alberto Muti, Katherine Tajer, and Larr MacFaul, 'Cyberspace: An Assessment of Current Threats, Real Consequences and Potential Solutions', Remote Control Project (October 2014)

David Omand, *Securing the State* (London: Hurst, 2010)

Thomas Rid and Ben Buchanan, ‘Attributing Cyber Attacks’, *The Journal of Strategic Studies* 38:1-2,4-37 (2015)

NATO CCD COE, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, 2013)

Cyber Power Index 2012, Economist Intelligence Unit & Booz Allen Hamilton, http://www.boozallen.com/insights/2012/01/cyber-power-index, accessed 24/02/2016

UK National Security Review 2010: *A Strong Britain in an Age of Uncertainty* (London, 2010)

UN General Assembly Documents, Group of Governmental Experts: Developments in the Field of Information and Telecommunications Technology in the Context of International Security, A/60/202 (5 August 2005), A/65/201 (30 July 2010), A/68/98 (24 June 2013), A/70/172 (22 July 2015)

UN General Assembly Doc., Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*,* A/66/359 (14 September 2011)

US Department of Defence, *National Defence Strategy 2008* (Washington D.C. 2008)

US Department of Defence, *Cyber Strategy 2015* (Washington D.C. 2015)