2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT

Richard Hill
Hill & Associates
Geneva, Switzerland
rhill@hill-a.ch

Abstract: The cyber security situation is not as bad as most people think it is – it is worse than most people imagine it could be. Indeed the lack of security of the Internet and of the devices connected to it results in serious vulnerabilities. These vulnerabilities create risks for infrastructures that increasingly rely on the Internet, including not just communications, but also power generation and distribution, air transport, and, in the near future, road transport. It is easy and relatively inexpensive to access cyberspace and to obtain the means of conducting offensive cyber attacks. Thus it is tempting to develop offensive cyber capabilities and indeed some states are doing so – as published in their national cyber security strategies, and several states have allegedly carried out cyber attacks. At the same time, a state is bound to protect its citizens, including against cyber attacks and cyber warfare. This will become increasingly difficult, if not impossible, if current trends continue unchecked. This article argues that international agreements on improving cyber security, and limiting cyber attacks would appear to be necessary and appropriate measures. Yet key developed countries resist taking legally binding measures of that nature, see in particular the discussions and outcome of the 2012 International Telecommunication Union (ITU) World Conference on International Telecommunications (WCIT). On the contrary, some of these countries practice mass surveillance, which some consider to be a threat to citizens and to the security of states, and which some authors have even considered, figuratively, to be a form of cyber war, even if it is inappropriately justified as a means of combating terrorism. And they resist calls to end mass surveillance. This paper argues that the positions taken by key developed countries could have grave negative consequences in the future, in particular for those very countries. The time has come to take steps to prevent this, which include more discussions and engagement in various forums, including ITU.

Keywords: *cyber security, cyber warfare, ITRs, ITU, WCIT*

1. INTRODUCTION

Cyber security can be defined as the collection of tools and procedures that ensure availability, integrity, authenticity and confidentiality of information and communications.[1] Both computer systems and networks can be attacked to prevent their use (denial of service), to compromise and alter the data they store or transport, to compromise ("spoof") the identification of the originator, and to read data without authorization (eavesdropping). In this paper, we will refer to all such attacks as cyber attacks.

The structural and technological changes arising from telecommunications privatization, liberalization, and the growth of mobile and Internet Protocol based networks (the Internet) have resulted in a degradation of network security (and consequent facilitation of cyber attacks), increasing cyber crime, proliferation of viruses, worms and other malware, and proliferation of spam (Talbot, 2006; WGIG, 2005, para. 17-18; Deibert, 2013; Brunton, 2013; Hill, 2014). And the situation will get worse, not better (Jeffers, 2013). In particular, as discussed in some detail below, confidentiality is not ensured, due to mass surveillance.

It is worth outlining the key reasons for this situation. The Internet was initially deployed to connect a handful of large, expensive computers operated by a small group of trusted entities. Security was not a major design goal: security was achieved by securing the end-devices connected to the network. The situation changed dramatically with the emergence of personal computers, whose security is mostly very weak (despite attempts by manufacturers to improve the situation) and with the connection of those insecure devices to the Internet (Hill, 2014, pp. 24 and 32). As Robert Khan, co-creator of Transmission Control Protocol/Internet Protocol (TCP/IP), puts the matter (Khan, 2011): "At present, the Internet environment is tilted in favor of those with adverse motives, while the rest of the community must be on constant vigil to defend against harmful interference."

It is well known that the cost of entry into cyber space is relatively low (Schreier, 2015, p. 12) and that cyber capabilities are relatively inexpensive: with a computer and Internet access anyone can engage in cyber attacks, and many states can even envisage cyber warfare (Lewis, 2010, p. 2; Schreier, 2015, pp. 26 and 27). It is important to note here that there are differing definitions of the term "cyber warfare", resulting in different understandings of consequences and preventive measures. Strictly speaking, it refers to massive state-organized assaults, akin to conventional warfare, but it is also used more generally. Indeed, the term "war" is often used figuratively, as in economic war (Freeman, 2015), the war on drugs, and the war on terrorism. The Inter-Parliamentary Union has recently adopted a resolution that states (Inter-Parlimentary Union, 2015): "Considering that cyber warfare may encompass, but is not necessarily limited to, operations against a computer or a computer system through a data stream as a means and method of warfare that is intended to gather intelligence for the purpose of economic, political or social destabilization or that can reasonably be expected to cause death, injury, destruction or damage during, but not exclusively in, armed conflicts". A recent academic work uses "cyber war" figuratively to refer to utilization of digital networks for geopolitical purposes, including covert attacks against another state's electronic systems, but also the variety of ways the Internet is used to further a state's economic and military agendas (Powers and Jablonsky, 2015). But

1 This is a simplified version of the definition found in Recommendation ITU-T X.1205 and it is consistent with other older definitions of security, such as that found in Recommendation ITU-T E.408.

this figurative use of the term "cyber war" predates academic writings, see for example an article by a former director of the US National Security Agency (McConnell, 2010). We note that the figurative use of the term is consistent with what is found on the web sites of some private companies active in the area (Rand, 2015). But it has also been said that the figurative use of the term is inappropriate, see Singel (2010), who quotes the US "cyber security czar".

Various states have been accused of practicing cyber espionage or even of conducting cyber attacks. Not surprisingly, the USA accuses China (Sanger, 2013) and Russia (AP, 2011) of actively engaging in cyber attacks or at least in commercial cyber espionage. However, it is generally accepted that the USA and Israel conducted an apparently successful secret cyber attack on Iranian nuclear facilities, through the Stuxnet virus (Sanger, 2012), and that the US has invested significantly in cyber espionage (Gellman and Miller, 2013; Poulsen, 2015) and in offensive and defensive cyber capabilities (Harris, 2015). Separately, Chinese government researchers have published in the open literature accounts of some of their work (Stone, 2013).

It is generally agreed that conventional laws apply online as well as offline[2], so certain types of cyber attacks are surely illegal. However, this paper argues that additional agreements are needed regarding cyber operations: if there is no common agreement regarding the appropriate level of cyber operations by states, then cyber attacks may become more common and could escalate out of control. In particular, mass surveillance programs may become more widespread and more intensive. The paper argues that there should be some agreement on how to respond appropriately to cyber attacks, and how to distinguish the responses to cyber attacks originating from states, from commercial organizations, or from criminal organizations.

Concern regarding the lack of security of the Internet is widespread (Talbot, 2006). Vint Cerf, Khan's TCP/IP co-creator, agrees that a change is needed (Cerf, 2011): "We can't let it sit the way it is now, it is simply not adequate. We're depending too heavily on the Internet, for too many different things to allow it not to be evolved to a more secure state." As Schreier (2015, p. 14) puts the matter: "modern society's overwhelming reliance on cyberspace is providing any attacker a target-rich environment, resulting in great strain on the defender to successfully defend the domain". That is, the situation regarding cyber threats is not as bad as most people think it is: it is worse than most people could imagine it could be.

Unless limits are internationally agreed, state-led cyber attacks threaten the trust required among stakeholders for effective internationally agreed cyber security goals, such as security of electronic commercial transactions and privacy of personal communications. The establishment of trust through agreed limits in state-led cyber attacks and agreed ways to respond to cyber attacks (whether originated from states, commercial organizations, or criminal organizations) could be achieved through increased international cooperation. Increased international cooperation could also facilitate the development and implementation of appropriate technical measures to improve cyber security, which might include greater use of encryption (Internet Architecture Board, 2014), and stronger encryption.

Indeed, the 2013 Seoul Conference on Cyberspace stressed the benefits of such international cooperation (Seoul Conference, 2013). Richard Haass, President of the Council on Foreign

2 For example, UN General Assembly Resolution A/RES/68/167 "*Affirms* that the same rights that people have offline must also be protected online, including the right to privacy". And there is a long line of court decisions applying conventional law to the Internet (Hill, 2014, p.18).

Relations, suggests (Haass, 2010): "Cyber is exactly at the point today where nuclear was maybe 50 years ago, where people are beginning to think, what sort of rules do we set up? What sort of arrangements do we put into place?" The East West Institute's 2012 Cybersecurity Summit called for greater collaboration on cyber security between both the private and public sectors and international actors, noting (East West Institute, 2012): "securing cyberspace is a global challenge – one that cannot be solved by a single company or country on its own." And no doubt it cannot be solved by a single instrument, or type of instrument, either: a combination of voluntary codes of conduct, soft law, and law at both the national and international levels will likely be required.

Similar concerns and calls for cooperation are found in international agreements such as Resolution 130 of the ITU, which recites various threats and trends and notes "the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memorandums of understanding, etc)". Calls for cooperation and action are also found in ITU World Telecommunication Standardization Assembly (WTSA) Resolutions 40 and 52.

In this light, it is not surprising that the matter of improving cooperation regarding cyber security was discussed at the ITU's 2012 WCIT. WCIT-12 was convened in December 2012 at the request of the ITU members in order to revise the International Telecommunication Regulations (ITRs), a treaty which had been agreed in 1988 and which opened the way for the privatization and liberalization that has since characterized the telecommunications sector (Hill, 2013; Hill, 2013b).

The purpose of the ITRs is to establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services. The ITRs provide the groundwork from which the ITU promotes the development of telecommunication services and their most efficient operation while harmonizing the development of facilities for worldwide telecommunications.

The issue of Internet security had already surfaced in 1988 at the ITU's World Administrative Telegraph and Telephone Conference (WATTC), which was the predecessor of WCIT and which approved the 1998 version of the ITRs. When the WATTC was convened on 28 November, the Morris Internet worm (Eisneberg et al., 1989) was still a topic of concern. Although the worm itself was not explicitly mentioned in the ITRs, the "avoidance of technical harm" provision of Article 9 is generally considered to have been inspired by a desire to take steps that would prevent a reoccurrence of problems of this type (Hill, 2013b, p. 8). This is possibly the first treaty provision dealing with the security of telecommunication networks, a form of cyber security[3]. A similar provision was subsequently added to what is now Article 42 of the ITU Convention[4]. In

3 Actually the original predecessor of the ITRs, the 1865 treaty that created the ITU, included a provision regarding the use of encryption, and such provisions are also found in later versions. But those provisions were as much about costs (they prevented the use of private short-codes which reduced the number of words in a telegram) as about national security, so they cannot be considered to be security provisions in the modern sense of the term. See Headrick (1991).

4 A detailed discussion of the evolution over time of provisions related to security in the various instruments of the ITU (including the "technical harm" provision of Article 9 of the ITRs) is given in Rutkowski (2011).

the author's opinion, those provisions have not had any significant practical effect, but this does not necessarily mean that new provisions agreed today would not be effective.

2. DISCUSSIONS AT WCIT

A. Preparations for WCIT

Some of the proposals submitted to WCIT were motivated by an underlying goal to increase sovereign control over some portions of the Internet (indeed a late submission from the Russian Federation explicitly called for that – this proposal was never placed on the agenda so it was not discussed at the conference (Hill, 2013b, pp. 60-62)). Such proposals must be seen in light of a perceived erosion of national control and a perceived domination of the Internet by the United States and its dominant private companies (Hill, 2013c). Be that as it may, some of the proposals could have facilitated state control over some aspects of the Internet, including censorship. This understandably raised concerns in many quarters and resulted in unbalanced press coverage which stressed those proposals while ignoring the many other proposals which addressed commercial matters, such as reduction of mobile roaming prices, transparency of pricing in general, etc. (Hill, 2013b, pp. 35-48 and 65-66; and 59 and 63, respectively). Several of the pro-consumer provisions were supported by developing countries but opposed by developed countries (Hill, 2013b, pp. 59-63).

The issues of security and spam had long been discussed in various ITU meetings[5]. Thus it was not surprising that various proposals were presented to WCIT regarding security and spam. All called for increased international cooperation, but differed in other respects. Some of the proposals were characterized as more-or-less disguised attempts to impose or to favor censorship (see below), but the true intent of the more elaborate proposals was to likely limit state-sponsored cyber attacks (Mueller, 2012; Hill, 2013b, pp. 41-42)[6]. The USA made it clear that it was opposed to any text on security or spam in the ITRs[7], refusing even to consider a proposal that was essentially copy-pasted from one of USA President Obama's Presidential Declarations[8]. While some European and other countries were initially willing to consider some text related to security and spam (Hill, 2013b, pp. 29 and 33), the USA was successful in influencing their positions with the result that there were strong differences of views going into the conference (Hill, 2013b, p. 54). The main reason given by the USA for opposing cooperation to improve security and combat spam was a concern that a treaty provision to that effect could be used by authoritarian countries to justify censorship or other restrictions on freedom of speech or human rights (Majority Committee Staff, 2012; Rizo, 2012; US Congress, 2012).

5 For example, Resolution 130 "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies" has been revised at every Plenipotentiary Conference since it was adopted in 2002; cyber security and spam have been topics of study in ITU-T Study Group 17 since, respectively, 2001 and 2009.

6 Hill (2013b, p. 42) concludes, on the basis of a legal analysis of the proposals and the ITU Constitution, that a Russian proposal could be construed as an attempt to authorize blocking of state-originated cyber attacks, and to bind all states to cooperate to prevent transmission of such cyber attacks.

7 See WCIT document 9 "United States of America Proposals for the Work of the Conference", August 3, 2012, which notes that cyber security should be treated by member states primarily as a sovereign issue, and opposes "any effort to interfere with those rights."

8 See ITU documents CWG-WCIT12/C-60 for the proposal, and CWG-WCIT12/TD-62 for the US opposition, expressed as "cybersecurity should not be included in the ITRs in any way, shape or form." The proposal is CWG/4/225 in the publicly-available "Draft of the future ITRs" <http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf>

However, a legal analysis of the ITRs does not support the allegation that it could threaten freedom of speech (Hill 2013; Hill 2013b)[9], see below. And the USA's arguments appear incongruous in light of its pervasive domestic and foreign surveillance – as Brazilian President Dilma Rousseff has pointed out: "In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy" (Borger, 2013)[10] –, and that at least some of the foreign surveillance appears to be done without meaningful judicial oversight (Hill, 2013c; National Security Agency, 2013; Bowden, 2013). Be that as it may, the discussions at WCIT were difficult.

B. Outcome of WCIT

Strong objections were raised by the USA regarding certain proposed provisions of the new treaty (Hill, 2013; Hill, 2013b). These objections were supported to some extent by other countries and resulted in the preparation of a compromise text (Hill, 2013b, pp. 55-65). The compromise text was acceptable for most countries – albeit not for the USA – (Hill, p. 54) but, at the last minute, a vote was called to introduce a controversial provision in the preamble of the treaty. That provision was not related to security or spam, it was related to unilateral actions by some countries to block access by other countries to certain web sites (Hill, 2013b, p. 65). The inclusion of that controversial provision in the preamble resulted in most developed countries refusing the sign the treaty, on the grounds that they needed more time to consider the implications of the provision in question. In what follows, we will focus only on the provisions regarding security and spam since these appeared to be acceptable to a majority of states; a full account of the discussions and issues regarding the other provisions is found in Hill (2013b).

The treaty provisions approved at WCIT include two new articles on security and spam. These articles state:

> "6: Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public."

And

> "7: Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense."

These articles have been heavily criticized in the USA, in particular in relation to freedom of speech (Hill, 2013; Hill, 2013b, p. 70, footnote 5). However that criticism is not valid from a legal point of view, in particular because the Preamble and Article 1 of the treaty make it clear that these provisions cannot be invoked to justify restrictions on freedom of speech (Hill, 2013; Hill 2013b, pp.86-89). In the author's view, the real motivation for the USA resistance to article 6 appears to be a desire to avoid international agreements on improving cyber security, as such agreements might restrict the USA's ability to carry out cyber attacks and mass surveillance (Hill, 2013b). For example, apparently no judicial approval is required in some cases for surveillance of non-US persons; this was not publicly known when WCIT took place and presumably would have had to be revealed in the context of cooperation on cyber security matters; such practices might have been found objectionable by some countries (Hill, 2013b, p. 42). As noted above,

9 The author is not aware of any other peer-reviewed legal analysis and has been told privately by both legal scholars and representatives of certain states that his analysis is sound.

10 The same point is made in paragraph 14 of High Commissioner for Human Rights (2014)

most of the states that did not sign the treaty referred to the new clause in the preamble as the main reason for not signing. One can speculate regarding other reasons, which might be similar to those posited above for the USA. And one can speculate that, at the time, the US has greater cyber capabilities than other countries (Harris, 2014), so other countries were more willing to accept restrictions.

As noted above, lack of security favours cyber attacks and mass surveillance is a form of cyber attack (and, figuratively speaking, perhaps even cyber war). Consequently, as Schreier (2015, p. 7) puts the matter: "In fact, there is a stunning lack of international dialogue and activity with respect to the containment of cyber war. This is unfortunate, because the cyber domain is an area in which technological innovation and operational art have far outstripped policy and strategy, and because in principle, cyber warfare is a phenomenon which in the end must be politically constrained."

A continuing resistance to improve cyber security and to curtail mass surveillance could have negative consequences for the Internet (Naughton, 2013; Morozov, 2013). Mass surveillance is often justified as a means to combat terrorism. But the number of potential terrorists present in developed countries is very small, so from a statistical point of view a mass surveillance program cannot be effective at detecting them: there will be too many false positives (Rudmin, 2006). However, mass surveillance programs can collect information that is useful for economic and political purposes, and reportedly some countries are using them for such purposes (Poitras, Rosenbach and Stark, 2013; Gellman and Miller, 2013; CBS News, 2014; Price, 2014; Tribune de Genève, 2015[11]). Thus, figuratively, mass surveillance can be viewed as a form of cyber warfare, even if it is not cyber warfare in the legal sense of the term. And calls to continue it are not justified: mass surveillance violates human rights, and it is not effective (Harding, 2015; Powles, 2015). Nobody would accept to put mass surveillance into place to prevent violent bank robberies, because everybody can see that it would not be effective. The same holds for the terrorist threats in developed countries, which share many of the characteristics of violent crime.

3. THE FUTURE

A persistent refusal by developed countries to envisage cooperation with developing countries and emerging economies on terms that are acceptable to them to improve cyber security might have undesirable consequences. For sure there are many cooperation mechanisms and it is easier to negotiate non-binding agreements. But non-binding agreements are just that, and forums that do not include all states tend to make decisions that are consistent with the interests of the participating states, but not necessarily with the interests of non-participating states. In the absence of global agreements, states may choose to enter into bilateral or regional arrangements. At present, it is impossible to say whether those bilateral or regional arrangements might set the stage for future global agreements, or whether they might be detrimental to the global interconnectivity of today's telecommunications systems. As a Canadian think-tank put the matter referring to overall governance, which includes the security issues outlined above (Raymond and Smith, 2013):

11 Citing a proposed new French law that would authorize certain types of surveillance in cases of major economic or scientific interests, as well as national defense, prevention of terrorism, etc.

> "the larger problem [of the split between signatories and non-signatories of the 2012 ITRs] in the long term is the overall degree of complexity introduced into the governance of international telecommunications, the potential for increased transaction costs and the eventual possibility of significant divergence between the two treaty regimes over time. Given the similarity between the two treaties [1988 versus 2012], as well as the long history of routine cooperation on international telecommunications and the resulting business relationships and accumulated social practice, there are reasons to believe that this complexity may be manageable, if suboptimal. This assessment may not apply, however, in the event that the parties to the new ITRs engage in subsequent negotiations, building on the accompanying resolutions to erect a parallel institution for Internet governance. … Further, since routing is currently done without regard for international borders, the existence of parallel Internet governance regimes that may evolve with very different privacy protections poses challenging questions about the sustainability and desirability of legacy routing practices."

Cyber security issues are only one part of the overall governance of international telecommunications. But they are an important part (Eichensehr, 2014). And if there is uncertainty regarding global governance, then it is difficult to predict how the situation will evolve with respect to cyber security. On the one hand, private companies appear to favor improved cyber security in the interests of their customers, for example by improving encryption (McCarthy, 2015). On the other hand, some states appear to resist those improvements, because they are of the view that mass surveillance is an effective means to protect their citizens (United States of America, 2014; Ball, 2015; McCarthy, 2015; Sanger, 2015). In the absence of international agreements, the most likely outcome would appear to be the emergence of a "federated Internet": one in which national networks are interconnected, but remain under local control to some extent. This is already largely the case for China, and for the internal networks of large private companies. A more detailed discussion of this scenario is given in Hill (2015).

Despite rhetoric to the contrary, the USA government supports greater state involvement in improving cyber security. Similarly, former CYBERCOM and NSA Director Keith B. Alexander has argued that securing private networks cannot be achieved through voluntary mechanisms alone (Alexander, 2012): "Recent events have shown that a purely voluntary and market driven system is not sufficient. Some minimum security requirements will be necessary to ensure that the core, infrastructure is taking appropriate measures to harden its networks." Indeed, state involvement can be justified in light of the externality effects of security – or rather, lack of security – which effects are well explained by Schneier (2007). While it has proven possible to reach agreements to limit certain types, or certain uses, of conventional weapons, it is not clear whether it will be possible to reach similar agreements regarding cyber attacks (Eichensehr, 2014).

Some may take the view that there is no need for a treaty regarding cyber security or even international telecommunication matters in general: any matters requiring inter-governmental coordination can be handled by soft-law, or bilateral or regional agreements. But the divergence of views expressed at WCIT indicates that there is a need to agree some basic principles at a high level even if it is not clear which, if any, to enshrine formally in a treaty (Eichensehr,

2014). In the author's view, lack of treaty-level agreement regarding cooperation with respect to network security issues in effect favors the current practices of secret (and unacknowledged) cyber attacks and mass surveillance, because there are no agreements on how to interpret and to apply existing international law. In particular, the USA takes the view that its obligations under international human rights law with respect to privacy do not apply to non-USA persons (United States of America, 2014). Treaty-level agreements would presumably affect such activities, because treaties should be enacted into national law, which laws would be enforced nationally (but it should be noted that treaties are not always respected).

International agreements to improve cyber security would likely make mass surveillance more difficult, if not impossible. Agreements could be envisaged for many different aspects, for example to allow pervasive strong encryption[12]. It will surely be difficult to discuss all topics at the same time, and to envisage their inclusion in a single instrument. Thus a first step could be an agreement in principle to cooperate and to agree on forums in which to carry out more detailed discussions in line with some agreed principles, for example, limits on mass surveillance, and limits on the means used to carry out authorized surveillance.

Reportedly, states whose private companies are producers of telecommunications hardware have programs in place to intercept some shipments of such hardware so that the hardware can be modified to facilitate monitoring of communications and even to allow the hardware to be attacked (Greenwald, 2014; Paganini, 2014). Such modifications might escape detection by the end-user and might enable monitoring or attacks even if the hardware is used for a private network that is not connected to the public Internet[13] (Perlroth and Sanger, 2015; Kaspersky Lab, 2015). Thus, nobody can ensure secret communications unless they manufacture their own hardware and software. But this is beyond the reach of all but a few states. Further, sophisticated techniques can be used to implant spyware no matter who manufactured a system (Gallagher and Greenwald, 2014; Sanger and Shanker, 2014), and encryption keys can be obtained through indirect attacks against manufacturers of equipment with embedded keys (Scahill and Begley, 2015).

As already noted above, anybody can conduct cyber attacks: developed countries, developing countries, very small states, as well as criminal organizations. A continuing lack of concrete action to improve cyber security and to limit and control state-sponsored cyber attacks is a serious threat to the developed countries who, at present, are the least willing to take such actions.

As one human rights advocate puts the matter (Donahue, 2014): "Furthermore, by engaging in tactics that undermine digital security for individuals, for networks and for data, governments trigger and further inspire a hackers race to the bottom. Practices that undermine digital security will be learned and followed by other governments and non-state actors, and ultimately undermine security for critical infrastructure, as well as individuals users everywhere. Strengthening digital security for individual users, for data, for networks, and for critical infrastructure must be seen as the national and global security priority that it is."

12 There are numerous restrictions at present on import, export, and even use of certain encryption methods, see for example Saper (2013).

13 For example, the hardware might emit radio signals, or be able to receive radio signals.

Portions of critical national infrastructures are increasingly linked to and dependent on the Internet (McGuinn, 2004). If they can be disrupted by cyber attacks, that can have a significant effect on the national economy. The purpose of a national military is to protect the nation against external threats. How many military forces today are capable of protecting the civilian infrastructure against a determined cyber attack? And how many could perform effectively their traditional defense mission of using physical force if the civilian infrastructure (electrical power distribution, roads, manufacturing, etc.) is severely disrupted by a cyber attack?

4. CONCLUSIONS

Global trade and economic interdependence create incentives for nation-states to come together and agree to additional rules, or treaties, that collectively bind behavior and ensure the protection of shared resources[14]. If one considers the Internet as a microcosm of society, then its natural progression from an infant, specialized technology to the global network of networks would likely follow the path of any highly complex and interdependent community. This is to say, it is both natural and predictable that, as the Internet becomes more and more integral to the collective welfare of citizens around the world, governments will act to protect this shared resource from the abuse of malicious actors.

States should agree to cooperate to improve cyber security and to limit cyber attacks and reactions to cyber attacks. They have managed to agree to limit the types of munitions used in small arms, to limit the use of some types of mines, to limit the proliferation of nuclear weapons, and to prohibit the use of chemical weapons. A first step in the direction of cooperation to improve cyber security might be to accede to the 2012 ITRs. For sure this would not result in an immediate reduction in the number of incidents, but it would hopefully result in increased discussion and cooperation. This in turn could lead to increasing trust, thus decreasing the perceived need to engage in unilateral cyber operations. An analogy to discussions on chemical weapons and the related treaties might be appropriate. Such weapons are relatively inexpensive to develop and their use can cause severe collateral damage. Without those discussions and treaties surely there would be a greater risk of use of chemical weapons than there is at present.

Discussions on international cooperation to improve cyber security would be complex and arduous, for technical, political and social reasons (for example, improving encryption can favor both free speech and criminal activities), but every journey starts with the first step. In this case, several first steps could be taken simultaneously: the technical issues can be discussed in forums such as the ITU, the social issues in forums such as the United Nations Human Rights Council, while the political issues could be discussed at a summit to be convened by a group of willing states.

From this point of view, the results of the 2014 ITU Plenipotentiary Conference are disappointing: in order to avoid controversies and an open split within the membership, sensitive topics were not discussed in any depth (Ermert, 2014). For example, a proposal from India that included provisions that could have had the effect of improving the privacy (and hence the security) of

14 See for example the World Trade Organization (WTO) agreements, the many treaties relating to international commerce, the treaties administred by the World Intellectual Property Organization (WIPO), the ITU treaties, etc.

domestic communications was only discussed (and dismissed) in a small group and not in the larger groups that are publicly webcast (Hill, 2014b).

Fundamentally, either we recognize that the Internet has become a global public good, and govern it accordingly (French Senate, 2015), or we continue to pretend that it is not a critical infrastructure, and we allow cyber crime and cyber attacks to flourish, which will result in medieval-style pervasive crime, violence, fear, and terror. Nobody would accept a world in which almost any criminal organization could acquire a Predator unmanned aircraft equipped with laser-guided missiles. Why should we accept the cyber-equivalent of such a situation? And if we do not wish to accept such a situation, then shouldn't we require states to cooperate to prevent its coming to pass?

The time has come to agree to cooperate to improve cyber security and to limit cyber attacks. And to focus on peaceful uses of telecommunications, which is the mission of the ITU.

ACKNOWLEDGMENT

This paper is partly based on Hill, Richard and Powers, Shawn, "Cybersecurity and spam: WCIT and the future", World Cyberspace Cooperation Summit IV, 5-6 November 2013 <http://www.hill-a.ch/EWI%20final%20rev2%20clean.pdf>. The author wishes to thank the reviewers for their helpful and constructive comments, and in particular Anna-Maria Osula for her patience and persistence.

REFERENCES

Alexander, Keith (2012), "U.S. Cyber Command Cybersecurity Legislation Position Letter", United States Cyber Command, 3 May 2012 <http://publicintelligence.net/u-s-cyber-command-cybersecurity-legislation-position-letter/>

AP (2011), "U.S. report blasts China, Russia for cyberattacks", *USA Today*, 3 November 2011 <http://usatoday30.usatoday.com/news/washington/story/2011-11-03/china-russia-cybersecurity/51065010/1>

Ball, James (2015), "Cameron wants to ban encryption – he can say goodbye to digital Britain", *The Guardian*, 13 January 2015 <http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror>

Borger, Julian (2013), "Brazilian president: US surveillance a 'breach of international law'", *The Guardian*, 24 September 2013 < http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>

Bowden, Caspar (2013), "The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights", Note for the European Parliament (2013) <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf>

Brunton, Finn (2013), *Spam: A Shadow History of the Internet*, MIT Press

CBS News (2014), "Snowden: NSA conducts industrial espionage too", *CBS News*, 26 January 2014 <http://www.cbsnews.com/news/snowden-nsa-conducts-industrial-espionage-too/>

Cerf, Vint (2012), "Can We Make the Internet Safer?" Lecture delivered at the University of Maryland's A. James Clark School of Engineering, 7 April 2011 <http://lecture.umd.edu/detsmediasite/Play/4feab66caa824cafae6d01798b4849e51d>

Deibert, Ronald J. (2013), *Black Code: Inside the Battle for Cyberspace*, Signal (McCelland and Stewart)

Donahue, Eileen (2014), "Human Rights in the Digital Age", *Just Security*, 23 December 2014 <http://justsecurity.org/18651/human-rights-digital-age/>

East West Institute (2012), "Building Trust in Cyberspace." 3rd Worldwide Cybersecurity Summit in New Delhi, 2012

Eichensehr, Kristen (2014), "The Cyber-Law of Nations", *The Georgetown Law Journal*, vol. 103, p. 317, 8 January 2014 <http://ssrn.com/abstract=2447683>

Eisenberg, Ted et. al. (1989), "The Cornell Commission: On Morris and the Worm", *Communications of the, ACM*, June 1989, Volume 32, Number 6, p. 706

Ermert, Monika (2014), "ITU Plenipotentiary Conference: Internet Governance Diplomacy On Display", 5 November 2014, *Intellectual Property Watch* <http://www.ip-watch.org/2014/11/05/itu-plenipotentiary-conference-internet-governance-diplomacy-on-display/>

Freeman, Kevin D. (2015), "Financial Warfare Threatens America", Global Economic Warfare, 6 March 2015 <http://globaleconomicwarfare.com/2015/03/financial-warfare-threatens-america-2/>

French Senate (2015), Proposition de resolution sur la nécessaire réforme de la gouvernance de l'Internet, Foreign Relations Committee, 22 February 2015 <http://www.senat.fr/rap/l14-102/l14-1022.html>

Gallagher, Ryan, and Greenwald, Glenn (2014), "How the NSAPlans to Infect 'Millions' of Comupters with Malware", *The Intercept*, 12 March 2014 <https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/>

Gellman, Barton and Miller, Greg (2013), "'Black budget' summary details U.S. spy network's successes, failures and objectives", *The Washington Post*, 29 August 2013 <http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html>

Greenwald, Glenn (2014), "Glenn Greenwald: how the NSA tampers with US-made internet routers", *The Guardian*, 12 May 2014 <http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden>

Haas, Richard (2010), Interview with Eric Schmidt and Jared Cohen at the Council on Foreign Relations, 29 November 2010 <https://www.youtube.com/watch?v=eJAMD5p5tQo>

Harding, Luke (2015), "Mass surveillance is a fundamental threat to human rights, says European report", *The Guardian*, 26 January 2015 <http://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe>

Harris, Shane (2014), *@War: The Rise of the Military-Internet Complex*, Houghton Mifflin Harcourt

Headrick, Daniel R. (1991), *The Invisible Weapon: Telecommunications and international Politics 1851-1945*, Oxford University Press, p. 45

High Commissioner for Human Rights (2014), "The right to privacy in the digital age", Report, A/HRC/27/27, 30 June 2014 <http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc>

Hill, Richard (2013), "WCIT: Failure or success, impasse or way forward?" *International Journal of Law and Information Technology*, Vol. 21 No. 3, p. 313

Hill, Richard (2013b), *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History*, Schulthess/Springer

Hill, Richard (2013c), "Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?", in Weber, R. H., Radu, R., and Chenou, J.-M. (editors) *The evolution of global Internet policy: new principles and forms of governance in the making?*, Springer/Schulthess

Hill, Richard (2014), "The Internet, its governance, and the multi-stakeholder model", *Info*, Vol. 16 No. 2, pp. 16-46

Hill, Richard (2014b), "Inside Views: What Is Happening At The ITU Plenipotentiary Conference?", *Intellectual Property Watch*, 5 November 2014 <http://www.ip-watch.org/2014/11/05/what-is-happening-at-the-itu-plenipotentiary-conference/>

Hill, Richard (2015), "The Future of Internet Governance: Dystopia, Utopia, or Realpolitik?", in Pupillo, Lorenzo (ed.), *The global Internet governance in transition*, Springer (forthcoming)

Inter-Parliamentary Union (2015), Cyber warfare: a serious threat to peace and global stability, resolution adopted by the 132ns IPU Assembly, Hanoi, 1 April 2015 <http://www.ipu.org/conf-e/132/Res-1.htm>

Internet Architecture Board (2014), IAB Statement on Internet Confidentiality, Internet Architecture Board, 14 November 2014 <https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/>

Jeffers, Dave (2013), "Security prediction for 2014: It will get worse", *PC World*, 16 December <http://www.pcworld.com/article/2080802/security-prediction-for-2014-it-will-get-worse.html>

Kaspersky Lab (2015), "Kaspersy Lab Discovers Equation Group: The Crown Creator of Cyber-Espionage, Press Release, 16 February 2015 <http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-discovers-equation-group-crown-creator-cyber-espi>

Khan, Robert (2011), "The Role of Architecture in Internet Defense," in Kristin M. Lord and Travis Sharp (editors), *America's Cyber Future: Security and Prosperity in the Information Age*", Center for a New American Security, Washington, DC., June 2011

Lewis, James A. (2010), "Thresholds for cyberwar", Center for Strategic and International Studies <http://csis.org/files/publication/101001_ieee_insert.pdf>

Majority Committee Staff (2012), "Hearing on International Proposals to Regulate the Internet", *Memorandum to the Committee on Energy and Commerce*, 29 May 29 2012 <http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CT/20120531/HMTG-112-HHRG-IF16-20120531-SD001.pdf>

McCarthy, Tom (2015), "NSA director defends plan to maintain 'backdoors' into technology companies", *The Guardian*, 23 February 2015 <http://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies>

McConnell, Mike (2010), "Mike McConnell on how to win the cyber-war we're losing", *The Washington Post*, 28 February 2010 <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063>

McGuinn, Martin (2004), "Prioritizing Cyber Vulnerabilities", Final Report and Recommendations, National Infrastructure Advisory Council, 12 October 2004 <http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf>

Morozov, Evgeny (2013), "The Price of Hypocrisy", *Frankfuter Allgemeine*, 24 July 2013 <http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html>

Mueller, Milton (2012), "Threat Analysis of the WCIT: Part IV: the ITU and Cybersecurity", Internet Governance Project, 21 June 2012 <http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/>

Naughton, John (2013), "Edward Snowden's not the story. The fate of the Internet is", *The Guardian* 28 July 2013 <http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet>

National Security Agency (2013), "The National Security Agency: Missions, Authorities, Oversight and Partnerships", 9 August 2013 <http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf>

Paganini, Pierluigi (2014), "NSA intercepts US-made Routers to implant surveillance", Security Affairs, 14 May 2014 <http://securityaffairs.co/wordpress/24932/hacking/nsa-implant-surveillance-backdoor.html>

Perlroth, Nicole and Sanger, David E. (2015), "U.S. Embedded Spyware Overseas, Report Claims", *New York Times*, 15 February 2015 <http://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html>

Poitras, Laura, Rosenbach, Marcel and Stark, Holger (2013), "Ally and Target: US Intelligence Watches Germany Closely", *Der Spiegel*, 12 August 2013 <http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html>

Poulsen, Kevin (2015), "Surprise! America Already Has a Manhattan Project for Developing Cyber Attacks", *Wired*, 18 February 2015 <http://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/>

Powers, Shawn, and Jablonsky, Michael (2015), *The Real Cyber War: The Political Economy of Internet Freedom*, University of Illinois Press

Powles, Julia (2015), "Charlie Hebdo and the Security State", *Wired*, 23 January 2015 <http://www.wired.co.uk/news/archive/2015-01/23/charlie-hebdo-security-state>

Price, David (2014), "The NSA, CIA, and the Promise of Industrial Espionage", 28 January 2014, *Counterpunch* <http://www.counterpunch.org/2014/01/28/the-nsa-cia-and-the-promise-of-industrial-espionage/>

Rand Corporation (2015), "Cyber Warfare" <http://www.rand.org/topics/cyber-warfare.html> accessed 11 February 2015

Raymond M., and Smith, G. (2013), "Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance," Centre for International Governance Innovation, Internet Governance Papers, Paper No. 1, July 2013 <http://www.cigionline.org/sites/default/files/no1_4.pdf>

Rizo, Chris (2012), "Int'l proposals for U.N. Internet regulations draws bipartisan rebuke", *FierceOnlineVideo*, 20 June 2012 <http://www.fierceonlinevideo.com/story/plans-un-internet-regulations-draws-bipartisan-rebuke/2012-06-20>

Rudmin, Floyd (2006), "Why Does the NSA Engage in Mass Surveillance of Americans When it is Statistically Impossible for Such Spying to Detect Terrorists?", *CounterPunch*, 24 May 2006 <http://www.counterpunch.org/2006/05/24/why-does-the-nsa-engage-in-mass-surveillance-of-americans-when-it-s-statistically-impossible-for-such-spying-to-detect-terrorists/>

Rutkowski, Anthony (2011), "Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850", *Info*, Vol. 13 No. 1, pp.13-31

Sanger, David (2012), "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012, p. A1

Sanger, David (2013), "U.S. Blames China's Military Directly for Cyberattacks", *New York Times*, 6 May 2013 <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0>

Sanger, David and Shanker, Tom (2014), "N.S.A. Devises Radio Pathway Into Computers", *New York Times*, 13 January 2014 <http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0>

Sanger, David (2015), "President Tweaks the Rules on Data Collection", *The New York Times*, 3 February 2015 <http://www.nytimes.com/2015/02/03/world/president-tweaks-the-rules-on-data-collection.html?_r=1>

Saper, Nathan (2013), "International Cryptography Regulation and the Global Information Economy", Northwestern Journal of Technology and Intellectual Property, Fall 2013, vol. 11, p. 673 <http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/5/>

Scahill, Jeremy and Begley, Josh (2015), "The Great SIM Heist: How spies stole the keys to the encryption castle", *The Intercept*. 19 February 2015 <https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>

Schneier, Bruce (2007), "Information Security and Externalities", *Schneier on Security*, January 2007 <https://www.schneier.com/essay-150.html>

Schreier, Fred (2015) "On Cyberwarfare", DECAF Horizon 2015 Working Paper No. 7 <http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf>

Stone, Richard (2013), "A Call to Cyber Arms", *Science*, vol. 339, 1 March 2013, p. 1026

Seoul Conference on Cyberspace (2013), *Results*, <http://www.seoulcyber2013.kr/en/media/View.do?media_id=2242>

Singel, Ryan (2010), "White House Cyber Czar: 'There is no Cyberwar'", *Wired*, 4 March 2010 <http://www.wired.com/2010/03/schmidt-cyberwar/>

Talbot, D. (2006), "The Internet is broken" *MIT Technology Review*, December 2005/January 2006, p. 62 <http://www.technologyreview.com/news/405318/the-internet-is-broken/>

Tribune de Genève (2015), "De nouveax droits pour le renseignement français", *Tribune de Genève*, 17 March 2015 <http://www.tdg.ch/monde/europe/nouveaux-droits-renseignement-francais/story/14690017>

United States of America (2014), "United States Response to OHCHR Questionnaire on 'The Right to Privacy in the Digital Age'", Office of the High Commissioner for Human Rights <http://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf>

US Congress (2012), *Congressional Record*, vol. 158, no.116, Wednesday, August 1, 2012, House, pp. H5599-H5602 <http://www.gpo.gov/fdsys/pkg/CREC-2012-08-01/html/CREC-2012-08-01-pt1-PgH5599-3.htm>

WGIG (2015), *Report*, Working Group on Internet Governance, 3 August 2005 <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0>