Project Minerva Working Paper Series

CONTROLLING BEHAVIOR – NOT ARMS:

MOVING FORWARD ON AN INTERNATIONAL CONVENTION FOR CYBERSPACE

By,

Ramtin Amin
2010 Google Public Policy Fellow | Citizen Lab

Submitted to:

Professor Jack Goldsmith
Harvard Law School

Professor Ronald Deibert
University of Toronto

Masashi Nishihata
Citizen Lab, Toronto

Rafal Rohozinski
The Sec Dev Group

September 2010

Abstract: *The rapidly increasing occurrence of cyber attacks and the growing use of the cyber domain for politically motivated purposes during both times of war and peace by both state and non-state actors has precipitated a dire need of an international convention to control behavior in cyberspace. While arms control conventions exist for the nuclear, chemical, and biological modes of warfare occurring at land, sea, space, and air, no such treaty is in place for the latest domain, whose tactical importance is now of vital importance for the global communication infrastructure and domestic military capabilities. In this paper, I will first extrapolate upon the current legal landscape pertinent to cyber arms and crime, and explore the limitations of current international laws that have been most often cited during past instances of cyber attacks. I will further explore a number of arms control drafts that have been proposed over the years, and highlight some of the lessons learned, with the aim of providing a constructive analysis to aid international lawmakers and affiliated institutions who are less familiar with the meta-physical cyber domain, and the unique challenges it presents. Finally, I will analyze the following five essential elements of a future global cyber convention: terms and definitions regarding cyber arms; peaceful use of cyber technology; signatory obligations regarding private actors; attribution; and mechanisms for deterrence. In exploring these fundamental themes, I will demonstrate why and how a future convention for cyberspace should focus on controlling behavior, rather than dwelling on a counterproductive goal of arms control.*

INTRODUCTION

> "History has shown that when nations agree upon a common malicious threat, be it piracy on the high seas centuries ago or aviation terrorism of the 20th century, a cooperative, treaty-mediated regime can contribute substantially in addressing the problem." – *The Stanford Proposal*, August 2000.

The historical record reflects that laws presiding over information and communication technology have rarely been able to keep up with the rapid rate of innovation. Newly penned statutory codes have often demonstrated a tendency to be apropos of the past, and somewhat nescient of the future. The arduous lawmaking process is also riddled with administrative hurdles and political obstacles, further mitigating the value of a sewn up legal doctrine. Over the years, continuous and disruptive leaps in science and technology have emphatically forced lawmakers – along with their policymaking brethren – to reconsider extant statutes, or formulate entirely new codes in order to maintain relevancy and promulgate order in the realm of information and communication technology. Yet time and time again, newly signed laws that have been established to administer the latest innovations in technology have fallen heavily short – or worse, become entirely obsolete.

With the twenty-first century well underway, the most challenging and crucial – not to mention, most latent – domain of war left for lawmakers to administer is cyberspace. Since its inception, cyberspace was never designed to be secure, closed, or hierarchical, and as a result, it has always been weakly governed.[1] Consequently, a diverse set of contentious issues has permeated throughout the cyber sphere, ranging from concerns over user privacy to freedom of expression and content censorship. But the most malign issue manifesting within the cyber domain is the potential for, and proliferation of, cyber arms and cyber warfare. For a number of years now, a handful of legal scholars and policy makers have attempted to find ways to extend well-established international laws of war – governing land, air, sea, and space – to the cyber domain. Provided that the computing and networking technology that cyberspace is predicated on is far more dynamic than technology in other domains – evolving at a rapid, exponential rate – the annals of technology law suggests that future rules established to govern this new domain could become antiquated and nugatory much sooner. Thus far, the international legal landscape that governs cyberspace lies in a feeble – if not entirely absent – state of affairs. But this should not mitigate the pervasive need for an international legal regime to administer the use of cyber arms, governing both state and non-state actors, during both times of war and peace. Nor do adverse technical characteristics manifest within the cyber domain represent a predicament that earlier international arms control regimes have not had to deal with, whether it was biological, chemical, or nuclear.

An international treaty for cyber arms will of course be afflicted with the same plights of other international conventions, at both the planning and execution phases. Indeed, since the Peace of Westphalia, innumerable international treaties have been concocted, yielding many lessons to be learned for today's lawmakers and policy-planners hoping to construct a viable convention to control the proliferation and use of cyber arms around the globe. But one does not need to go back to the founding of the modern nation-state to unearth analogous treaty proposals

[1] Lewis 2010, 1

akin to a future cyber regime. An introspective analysis of the planning and execution of international arms control doctrines in the twentieth century, whose regulation spans traditional war domains of land, sea, air, and space, provides substantial insight for contemporary lawmakers and policymakers keen to design a durable global cyber arms treaty focused on controlling behavior, rather than arms.

In what follows, I will first extrapolate upon the current legal backdrop pertinent to cyber arms – and to a lesser extent, cyber crime – and explore the limitations of current international laws that are have been most often cited during past instances of cyber attacks. As I will show, these laws are mostly ensconced within the *Geneva Conventions* and the first two of its three additional protocols, and to a lesser extent, the *Charter of the United Nations*. I will further assess some of the draft proposals that have been formulated over the years by cyber experts and legal scholars in order to highlight what a future cyber arms control treaty should include in order to be effective for controlling behavior and conduct, viable for multi-party cooperation, and dynamic enough to maintain relevancy in the face of rapidly evolving technology and tactics. Finally, I will then delve deeper into five fundamental themes that manifest in the cyber domain, whose execution will be essential for a future global cyber treaty to be successful. These five elements include terms and definitions regarding cyber arms; peaceful use of cyber technology; signatory obligations regarding private actors; the question of attribution, and mechanisms for deterrence. In exploring these fundamental themes, I will demonstrate why and how a future convention for cyberspace should focus on controlling behavior, rather than dwelling on a counterproductive goal of arms control.

GROWING NEED FOR CYBER ARMS CONTROL TREATY

Cyber arms and cyber warfare are two separate yet intertwined concepts, and it is worth spending some time differentiate between the two non-interchangeable terms before proceeding. Cyber arms are more or less defined as the weapons used to carry out attacks through cyber media. These weapons include software, hardware, and methods used to sabotage information and communication data and systems, which range from the creation of botnets and the delivery of malware and denial-of-service attacks to the launching of computer viruses and worms.[2] Cyber warfare on the other hand, also referred to as digital warfare or information warfare, describes the omnipresent, networked domain in which attacks are carried out, and include various threats, ranging from information gathering and espionage to offensive attacks like vandalism and sabotage. Cyber arms are the means to carryout cyber warfare, much like chemical and nuclear weapons – inclusive of their supply chains – are the means used to conduct chemical or nuclear warfare, respectively. While these definitions are quite contentious in the literature, and their precise definition continues to evolve overtime in tandem with the latest technological and tactical strategies in the cyber domain, their inter-twined relationship remains steady and unwavering.

Despite the rapid proliferation of cyber arms and cyber attacks – during both times of war and peace – there still is no international cyber arms control treaty or convention. Today's legal landscape presiding over cyber arms and cyber warfare is similar to the 1950s-60s, an uncertain

[2] Denning 1

and unnerving time in which nuclear technology was beginning to proliferate across the globe with few control mechanisms or legal bodies in place. Today, perhaps the most relevant extant law presiding over the cyber domain comes from the Council of Europe's *Convention on Cybercrime*.[3] The protocol – which was signed in Budapest in 2001, with the United States, Canada, South Africa, and Japan acting as official observers, is a regional agreement amongst European states to harmonize national laws related to the growing threat of cyber crimes.[4] While this treaty was a monumental step forward at the time in the international law arena (although long overdue), it was not formulated to administer and govern the use of cyber attacks or tactics for purposes of war, and it also falls deficient of fully adjudicating over state-sanctioned cyber attacks. Instead, its design was more motivated by the need to coordinate efforts to control the dissemination of online child pornography, restrict the proliferation of racist web content, and mitigate the use of cyberspace as a medium for bank fraud and identity theft.

In the absence of an international convention for cyber arms, the law governing conventional warfare has traditionally been used to apply towards cyber warfare.[5] Making this substantive analogy for purposes of legal jurisdiction is tremendously misleading for a variety of reasons. The discordance becomes vividly clear when considering the *information* aspect of cyber warfare, as opposed to the *kinetic* or offensive facet of the term, in addition to the tactical defensive and offensive approaches taken by players. Nonetheless, the prevailing laws most commonly cited derive from the *Geneva Conventions*, the *Charter of the United Nations*, and regional treaty organizations. Not only were today's international legal regimes formulated and signed well before the advent of sophisticated cyber arms and digital tactics, but they were also designed with more conventional weapons in mind.

Application towards some real world examples will readily demonstrate why such conventions are unequipped to deal with the unique peculiarities manifesting within cyber space. One lucid example includes the oft-cited Estonian case, where a barrage of cyber attacks had bombarded the websites of banks, government agencies, and media organizations, effectively shutting down much of the nation's economy temporarily. Delivering an earnest declaration, the Estonian defense minister boldly claimed: "the attacks cannot be treated as hooliganism, but have to be treated as an attack against the state."[6] However, had the appropriate legal action been taken, as stipulated by Article 5 of the North Atlantic Treaty Organization's (NATO) statutes and Article 51 of the Charter of the United Nations, collective defense among all NATO states could have theoretically been summoned.[7][8][9] Naturally, nothing of the sort materialized in

---

[3] A full English language translation of the *Convention on Cybercrime* is available at <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>

[4] Canada, Japan, South Africa, and the United States later signed on to the convention. The United States later ratified the Convention on Cybercrime in August 2006, and it entered into force January 1, 2007.

[5] Brown 181

[6] Morozov 1

[7] Morozov 1

[8] The North Atlantic Treaty, singed in Washington, DC in 1949, is available at <http://www.nato.int/cps/en/natolive/official_texts_17120.htm>. Article 5 states: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

the aftermath, despite the crippling nature of the attacks on Estonia's state websites, and the detrimental impact on day-to-day functions of the state.

Over the last few years, the prevailing opinion among government and military leaders has begun to shift towards an enhanced awareness of the growing cyber dilemma, and an increased willingness to take action. It should, however, be noted that some cyber experts have expressed serious doubt about cyber war, perhaps most notably Evgeny Morozov, who declared fears of digital warfare to be highly exaggerated, with the literature rich in loaded metaphors, ranging from "digital Pearl Harbors" to "cyber Katrinas."[10] Highlighting the proprietary interests of individuals and corporations who stand to gain from enhanced cyber security contracts to protect both public and private infrastructure, gross hyperbole is indeed pervasive throughout the rhetoric and literature, particularly within industry white papers. Boeing, Raytheon, and Lockheed Martin, are just a few examples of companies that have ventured into the booming business of securing the government's vital information and communication networks.[11] In addition to the potential for profiteering, others have highlighted the interests of national security and intelligence agencies. Marc Rotenberg of the *Electronic Privacy Information Center* is one such advocate, who remarked that:

> "the threat of cyber war is part of a long running campaign here in Washington to move control of the Internet, the technical standards, and the openness that we have enjoyed away from its current model to one that would give the intelligence community ant the National Security Agency much great authority to decide what people may or may not do on the Internet."[12]

Other Internet experts and political scientists have strongly countered this cynicism. In what seems like a direct rebuke to Morozov's *Boston Review* article, Ronald Deibert, Director of the Citizen Lab in Toronto, notes in his own piece published across the river by the MIT Press that while it has become "fashionable" to express skepticism about 'cyber war, the threat still remains, and the militarization of cyberspace is indeed "very real" – particularly in the absence of international rules of engagement in the cyber domain.[13] Deibert's argument is also propagated to varying degrees among America's top military leaders. In the 2010 *Joint Operating Environment*, published by the United States Joint Forces Command, the authors acknowledged that America's opponents will use cyber space to "attack, degrade, and disrupt communications and the flow of information," and further note that "other nations without the

---

[9] The Charter of the United Nations is available at <http://www.un.org/en/documents/charter/index.shtml>. Article 51 states: Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain inter- national peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

[10] Morozov 1

[11] Morozov 1

[12] Intelligence Squared U.S. 4

[13] http://www.technologyreview.com/computing/25570/

legal and cultural restraints found in the U.S. may excel at capturing, assessing, or even manipulating this information for military purposes..."[14]

There are a myriad of cases, some more widely cited than others, that supports this latter argument which prioritizes the consistently increasing threat of cyber warfare. Some of the more notable cases of cyber warfare include the 2006 Israel-Hezbollah War, cyber attacks against both belligerents in the 2008 Russian-Georgian war over South Ossetia, the 2009 cyber attacks against government, media, and financial websites in the United States and South Korea, and ongoing attacks against the United States, presumably from computers in China and Russia.[15] The most recent case unveiled in late September was a malware program dubbed Stuxnet – a worm that penetrated industrial computer programs around the world. Stuxnet – suspected to have been concocted by a government organization or intelligence agency due to its technical complexity – is thought to have been targeted towards the Iranian nuclear program, considering the disproportionate penetration rate within the Islamic republic.[16] If this were found to be true, the recent Stuxnet cyber attack would be the first worm targeted towards an industrial system and having global reach.[17]

Interestingly enough, the aforementioned cases include attacks carried out during both times of declared war and ongoing peace. The precise origin of the command and control centers and identity of the attackers in each of these cases is still a contentious issue, which may include both state and/or non-state actors, underscoring perhaps the most difficult aspect of cyber crime investigations: attribution. Yet, with each successive cyber attack, tactics and digital strategy have evolved considerably, always hovering a step ahead of the cyber security industry. The open and dynamic character of cyberspace and coding has rendered the security industry reactive rather than proactive. This dim reality has thus far ensured that cyber attackers, whether state or non-state actors, continue to have an upper hand over cyber monitoring teams.

Unlike the other domains of war – land, air, sea, and space – cyberspace is an artificially created entity, created to store and transmit data and information. Nonexistent a century ago, this artificial cyber domain is still in its infancy. The traditional four domains of war were physical realms with stable, measurable, areas composed of tangible parts. One or more of these domains have hosted the battleground of every war ever fought, and belligerent actors have become very skilled and adept to performing both defensive and offensive maneuvers within these interdependent domains for purposes of achieving some predefined endstate.[18] Although the electromagnetic spectrum of cyberspace is bounded, the cyber medium is an abstract, complicated domain to measure, or even merely observe. Further, the links across the cyber medium are dynamic and constantly evolving, with innumerable links forming at each positive time increment. This makes mapping out a traditional cartogram extremely difficult, if not impossible. The near-infinite potential for new links and layers to take shape in cyberspace make this domain a playground for computer programmers, who are able to modify and develop

[14] 2010 Joint Operating Environment 34
[15] To keep up to date with the latest developments in global cyber attacks the Information War Monitor, published by the Citizen Lab at the Munke Center for International Studies headquartered at the University of Toronto maintains an continuously updated record. See <http://www.infowar-monitor.net/>
[16] Falliere et al 1
[17] Markoff 1
[18] Kelley 28

its anatomy by interfacing at a physical terminal using coded programming language. This hyper-dynamic environment not only plays to the offense, but also allows anyone with the technical know-how to play a role in shaping and directing the action that takes place within this domain. The open and dynamic architecture of cyberspace did not come by chance; its design was enabled by the of course was the original intent of early Internet evangelists, who advocated for open source and open standards for software applications. Ironically, this same golden philosophy that enabled the computer and Internet industry to thrive for so many decades is the same credo that provides the upper edge to computer hackers, and other entities who wish to employ attacks in cyberspace.

PROPOSED DRAFTS FOR INTERNATIONAL CYBER ARMS CONTROL

While there is still no international cyber arms control convention or treaty, there have been some attempts at the global level to move in this direction. At the First Committee of the United Nations meetings in 1998 and 1999, Russia proposed that the committee "explore an international agreement on the need for arms control for information warfare weapons," and a few years later in 2002, the G-8 Government-Industry Conference on High Tech Crime also sought ways to form an international framework to "classify and control malicious computer code."[19] Other major players, including China, the United States, and Israel, have maintained a quieter voice, and generally expressed a penchant for pursing bilateral agreements, rather than signing onto global accords.

There are some notable international scholars who have also put forth their own ideas for what should be included within an international cyber arms control treaty. Perhaps the most detailed draft was published by a group of scholars through Stanford University, collaborating under a jointly sponsored grant funded by the Hoover Institution, the Consortium for Research on Information Security and Policy (CRISP), and the Center for International Security and Cooperation (CISAC). The proposal, penned in August 2000, specifically addressed both cyber crime and terrorism. The Stanford Proposal argued in favor of more international cooperation in combating cyber attacks, noting: "the speed and technical complexity of cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks."[20] To administer the proposal, the committee recommended the creation of an international Agency for Information Infrastructure Protection (AIIP), intended to serve as a forum where groups can cooperate through independent experts around the world to develop standards and practices concerning cyber security.[21] The proposal would be modeled on other global regimes, such as the International Civil Aviation Organization (ICAO) and the International Telecommunication Union (ITU), and would have similar procedures for election to a governing assembly, along with a set of administrative duties ascribed to a Secretariat. It is difficult to imagine an arms control regime operating in the absence of such an international, independent body. Independent experts selected from signatory states would not only serve to

[19] Wilson 9
[20] Sofaer ii
[21] Sofaer iv

mitigate potential bias, but also enable a more democratic process which could incorporate different perspectives on some of the more subjective issues manifesting within the cyber realm.

The Stanford Proposal demonstrated a laudable effort to address a problem that was off the radar for most legal and arms control scholars at the time, having been published just months after the dot com bust in 2000. Like the Council of Europe's *Convention on Cybercrime*, the proposal is well equipped for detecting and responding to crimes committed across a myriad of states and zones of jurisdictions. Furthermore, the proposal notes the difficulty of getting so many countries with varying levels of technology and Internet penetration rates to collaborate; a quandary faced by earlier arms control conventions in other domains. In developing a future international convention to control cyber warfare, these countries will have to reach a compromise over key elements of a treaty, such as what constitutes cyber warfare, and what degree of retaliatory measure should be appropriate following a cyber attack. Already there exists widespread disagreement amongst nation states on many of these fundamental issues. The successful implementation of the *Convention on Cybercrime* suggests that regional cooperation might be the best-case scenario in this domain, in the shadow of burgeoning unilateral programs. As of late-2010, this is in fact the situation the world finds itself in, with major cyber players like the United States, China, Russia, and Israel continuing to administer robust domestic cyber crime regimes, in contrast to the Europeans who have formed a regional cyber crime regime (although not all members of the European Union have ratified).

One key flaw of the Stanford committee's draft is their proposal's lack of obligations, or even clear recommendations, for member states to harmonize their domestic laws, in order to enhance harmonized practices across the entire cyber regime. A harmonized set of laws would not only eliminate a large amount of duplicate processes, but also yield significant cost savings for all member states. Instead of recommending a harmonizing scheme to capitalize on these benefits, the Stanford proposal concludes by denoting a unique priority for jurisdiction:

> "...first, the State Party in which the alleged offender was physically present when the alleged offense was committed; second, the State Party in which substantial harm was suffered as a result of the alleged offense; third, the State Party of the alleged offender's dominant nationality; fourth, any State Party where the alleged offender may be found; and fifth, any other State Party with a reasonable basis for jurisdiction."[22]

At first glance, this order comes across as an essential prerequisite for the cyber domain, considering that different stages of an attack can and often are routed through intermediaries across wires and networks in multiple states. However, conflicting laws across national boundaries would have the potential to contradict one another, and cyber criminals could easily use this order of jurisdiction to their advantage when coordinating a multi-routed cyber attack. The implications for cyber warfare are clear: A stipulation that emboldens states to harmonize their own domestic laws would not only make questions of attack location, command and control origin, and citizenship non-issues, but it would also avoid one state – through obligations of the international legal regime – from encroaching upon the sovereignty of another when crimes and cyber attacks cross boundaries.

[22] Sofaer 29

In his efforts to develop a treaty more geared towards cyber warfare, Davis Brown, an American legal scholar, developed his own project for a global cyber arms treaty, entitled *Draft Convention Regulating the Use of Information Systems in Armed Conflict*. Brown's draft is much more relevant to cyber arms and warfare than the Stanford Proposal, which was more pertinent to cyber crime and terrorism. With thirty-two articles, his proposal includes a detailed set of definitions of information systems and attacks – an important element of any treaty dealing with cyber arms and dual use technology. Brown's draft refers specifically to attacks carried out during armed conflict, which limits its application to a significant number of cyber attacks that have already transpired, or will transpire in the future. Brown's version is reminiscent of the first Additional Protocol to the *Geneva Conventions*, highlighting a code for conduct and set of rules for belligerent and neutral states during times of war. One interesting point worth noting is Brown's stipulation regarding noncombatants. In § V Article 31, he states:

> "States shall enact legislation to prohibit noncombatants within its jurisdiction from engaging in information attacks against other States and shall prescribe criminal penalties for the same. States shall take all reasonable and appropriate measures to prevent and punish noncombatants within its jurisdiction from engaging in information attacks against other States."[23]

One unique facet of the cyber domain that Brown is referring to is the relative ease at which a dedicated person can deploy a cyber attack. This reality opens up the battlefield to civilians and other noncombatants in ways that other earlier forms of conventional arms and warfare could not, due to a variety of reasons that include higher cost, obstacles to arms acquisition in the global market, and training experience.

In the cyber domain, each of these factors is attenuated by a significant degree. In the age of cyber warfare, the only prerequisites for an interested participant include a sufficient knowledge of coding language (or at least the means to acquire malicious code from others), and network access for purposes of deployment. The key driver in noncombatant cyber attacks is political motivation, social status amongst a hacker community, and to a lesser degree, financial gain. Cross-national attacks, directed by citizens affiliated with or maintaining an affinity for a particular nation-state and its stance towards perceived antagonists affiliated with an opposing nation-state or political and/or religious inclination has proliferated over the years. Non-state actors have fewer infrastructures that can be threatened in a retaliatory response, and their greater capacity to accept risk – compared with nation-states – renders them more likely to attempt an attack in cyber space.[24] Even within states, affiliates of opposing political groups and ideologies can and have carried out cyber attacks against websites affiliated with their own countrymen. Nationality alone is not sufficient in determining the source of a politically motivated cyber attack, as national affiliations cross state boundaries, and can be maintained by citizens of different countries. One can think of American-born citizens who have fled to Afghanistan to fight against their own national brethren. Unfortunately, an inclination amongst political observers and media voices, particularly in the immediate aftermath of a targeted attack, has been to highlight "key suspects" – which more often than not are a list of two or three states

[23] Brown 221
[24] Lewis 1

where attacks were launched, rather than a list of individuals. This is of course a dangerous precedent, and can hamper the efforts of a cyber forensics team, who may be inclined to stop somewhere along the path of a routed attack before reaching the actual command and control center.

The EU's Convention on Cybercrime, the *Stanford Proposal*, and Brown's *Draft Convention Regulating the Use of Information Systems in Armed Conflict* all provide useful blueprints for a future global convention on cyber arms and cyber warfare. Key lessons to be learned from these preliminary drafts include the importance of defining fundamental terms, allowing for flexibility in definitions to anticipate for evolving technologies and tactics in cyber arms and warfare, and maintaining a process for truly multi-lateral collaboration – in both the treaty development phase, and the execution and verification stages which would commence following a cross-national cyber attack.

CONTROLLING BEHAVIOR IN CYBER SPACE

With a goal of controlling behavior, as opposed to the proliferation of arms – in cyberspace, there are a few requisite elements that a future international convention must include. Most of these elements are analogous to those found in other treaties, and will be familiar to intentional law scholars with a limited understanding of the unique cyber domain. The five most pertinent themes covered here include:

1. Terms and definitions regarding cyber arms
2. Peaceful use of cyber technology
3. Signatory obligations regarding private actors
4. The tricky question of attribution
5. Deterrence mechanisms

This set of *jus cogens* principles begins with definitions of key terms.

1. Terms and Definitions Regarding Cyber Arms

New terms unique to the cyber domain that will have to be universally defined include the three types of information weapons: code, computer systems, and operators.[25] In the context of cyber war, these three elements are logically interrelated and codependent, given that an operator uses a computer system to deliver a code for attack. This is analogous to a nuclear or chemical weapon, delivered by a missile system, guided by a soldier under command. A nuclear or chemical weapon sitting idly will by and large not cause any damage (less it malfunctions and detonates unexpectedly); nor will a missile, or a complex delivery system. The operator, a soldier in this instance, is a requisite element needed to facilitate an attack.[26]

[25] Brown 185

[26] Davis Brown offers another useful analogy describing a bullet, being fired from a gun, by a shooter. The gun and bullet alone are not enough to cause harm; the operator element is essential for bringing the elements together and creating an attack. See Brown 185

This analogy will make definitions of terms within a cyber arms treaty much more lucid for signatories. The mere acquisition of computer infrastructure or technical capacity for delivering an attack is not and should not be cause for alarm. Instead, the focus should be on the behavior of actors within this domain. Therefore, the act of cyber warfare will also have to be defined, whether it is dubbed "information warfare" or "cyber-assaults." The definition of the term, for the purposes of an arms control treaty, will have to be broad enough to include all forms of actual attacks, whether kinetically or economically damaging, while excluding information acquisition for purposes of espionage, keeping inline with the standing international laws governing arms and warfare.[27]

Additionally, the language of an international cyber arms control convention must consider the distinction between official combatants and non-combatants during war time, and render unique forms of sanctions for each. Current international humanitarian laws rooted in the *Geneva Conventions* and *Additional Protocols* clearly stipulates the proper treatment of both official combatants and noncombatants. However, in the cyber context, the line between the two can be very obscure. Coordinated cyber attacks carried out through military facilities, or codes delivered by military command and control centers during a time of war, are the easiest group to classify, as they are most analogous to a state-affiliated group engaging in a war across conventional domains. Noncombatants include both private citizens and corporations, and this latter category can be further subdivided into government-sanctioned or contracted corporations, and entities pursuing cyber attacks against competitors and/or national governments for proprietary purposes. Defining each type of player in a cyber attack will permit a convention to include more appropriate avenues for prosecution. Additionally, there should be a clear distinction made regarding neutral parties in a cross-national cyber war. Such a distinction will become more important when the question of attribution arises, and also provide some legal cover in the face of re-routed cyber attacks originating from non-neutral territory. Ultimately, these mechanisms will serve to control behavior, rather than the acquisition and proliferation of arms.

Relative to nuclear and chemical weapons technology, cyber technology has evolved considerably more, and in a shorter period of time. Consequently, definitions for cyber related terms devised in the present might not be applicable in the future, as no one can anticipate or administer unpredictable developments in technology or tactical strategy within this unique, ever evolving domain. It is therefore paramount for any cyber treaty – especially in the section defining key terms – to consider the unpredictability of developments in cyber technology and tactics. Given the exponential rate of growth in this industry, the authors of any cyber-based treaty – written to control crime or warfare – will face a considerable challenge with definitions. With this in mind, it will be essential for a global cyber treaty to include an efficient and graceful amendment process that has fewer administrative hurdles than earlier arms treaties.

The final definitions will also have to be mindful of the duel use capability of cyber armament, including tactics used for defense. One potential way to incorporate this is to classify cyber attacks by intent, or "potential effect," rather than by technical features.[28] By focusing on

[27] Brown 186
[28] Keys 3

the effect, a treaty will be able to exercise much greater flexibility, and sanctions will be able to be applied much more evenly across different types of cases. The set of categories include a diverse set of motives, ranging from espionage and brute force attacks to mere nuisance. The next section will delve deeper into the dual use aspect of cyber technology.

2. Peaceful Use of Cyber Technology

Given the dual use capability of computing and network infrastructure, any future cyber arms control treaty will have to include a section differentiating between the two uses. Under the NPT, the delivery systems alone do not need to be classified as nuclear delivery systems, and controlled amounts of nuclear research and material can be developed, purchased, and maintained by party signatories. However, this has not precluded signatory states from getting inches away from developing all the elements necessary to create a capacity for nuclear weapons deployment, should they choose to do so. The case of Iran illustrates a vivid example of this treaty's exploitable weak point, given their clever acquisition and development of duel-use technologies that can be converted, overtly or covertly, from a nuclear medicine and energy research program into a full-fledged nuclear weapons program. The only element missing from this potential scenario is an operator's orders.

Applying this lesson learned to a future cyber arms convention implies that careful distinctions will have to be made between cyber tools and tactics used for legitimate, non-malicious purposes – primarily for network security – and those used to engage in offensive cyber warfare. Naturally, any dedicated cyber armament facility should be controlled under a treaty, as any dedicated nuclear weapons program consisting of highly enriched uranium would be controlled, despite free trade in many primary nuclear components. However, in the cyber context, much of the systems used to carry out attacks are not embedded within dedicated military bases, or even dedicated privately contracted facilities. Indeed, cyber attacks can be carried out from just about anywhere. Richard Clarke once noted that the North Koreans were known to rent out hotels in China and set up under cover cyber centers to carry out attacks.[29] And in reality, the origin of the command and control responsible for directing a cyber attack can be lost in the fog of war. Under a reigning cyber arms control regime, such malicious, covert activity by member states would be cause for sanctioning, and legal recourse could be taken. This again highlights the importance of controlling behavior, and not arms, in the cyber domain.

3. Signatory Obligations Regarding Private Actors

One unique characteristic of the cyber domain is that most of the space is privately owned and administered, unlike other domains of war. Since the inauguration of a commercial Internet market in the early 90s, the private industry has always advocated for self-administration and governance. This libertarian mindset not only emanates throughout the Silicon Valleys of the world, but, ironically, also is credited with spawning the rapid development and innovation in information and communications technology. However, private actors around the world have also expressed concern over establishing legally mandated obligations in the form of an international arms regime, fearing detrimental effects to their business, and their capacity for

[29] Greenberg 2

growth.[30] At the same time, the record reflects an inability and/or unwillingness for private actors to voluntarily implement effective control. Although, it would be misleading to see the private industry as entirely careless or imprudent when it comes to controlling the spread of cyber attacks across their networks, as such negligent behavior would yield serious ramifications from a user experience and customer satisfaction viewpoint. Customers afflicted with an onslaught of cyber attacks through their email and Internet activities, not to mention, slower Internet speeds, would be quick to switch Internet service providers, or worse, adjust their level of consumption. Both scenarios would have major implications for the private Internet market, and also negatively impact the markets for related or dependent technologies and services.

Consequently, network administrators and Internet service providers do work hard within their means to monitor and filter attacks. For instance, Dave McMahon from *Bell Canada Security* once noted that approximately 98% of email sent through their servers is blocked and classified as spam.[31] This content includes both cyber crime and malicious code that could be classified as cyber warfare. In these latter instances, the private industry should be given some credit for their voluntary efforts. But again, it should be emphasized that Internet companies are not in the business of protecting customers or state infrastructures; they are in the business of expanding profit margins for their shareholders. This premise does more than to provide an opening for a government to step in and regulate – it necessitates it. This regulation should include more than just a series of statutory mandates originating within a global arms treaty; it should also include wording that serves to close the gap in terms of required resources – whether physical or pecuniary – and ensure that the private sector is equipped to handle the surge in malicious code and malware attacks being disseminated around the world.

Like other arms treaties, a future international cyber arms convention should obligate signatories to create domestic statues where none exist to force domestic actors around the world to adhere to a common legal regime.[32] The *Convention of Cybercrime* does just that in Chapter 2 §1-3, Articles 1-22 with its provisions for harmonizing national laws related to cyber crime. Harmonized laws within the cyber domain are of far greater importance than in other arms control regimes, as code can be routed through a series of countries much more efficiently. Any cyber arms treaty that does not have 100% buy-in from nation-states will suffer from this dilemma, as a committed actor can route an attack through or against public or private entities within a state that lacks sufficient jurisdiction. While the same is technically possible with weapons of mass destruction across conventional domains of war, the physical attributes of cyber arms makes it much more difficult to successfully implement this key feature. Designing a global treaty that mandates state-governments to oversee domestic actors will also significantly aid in responding to the attribution problem.

[30] Sofaer 7
[31] "Cyber-Security and its implications for Canadian Foreign Policy? Does an open cyberspace make us more or less secure?" *Open Net Initiative Global Summit*, Conference panel in Ottawa, Canada, June 30, 2010.
[32] This is a key provision recommended by the Stanford Proposal.

4. Attribution

Of all the challenges of a cyber arms control regime, perhaps the greatest is the question of attribution. While elements of uncertainty and confusion have always been a part of warfare, "the fog of war is especially thick in cyberspace."[33] This reality makes deterrence particularly difficult in the cyber domain, as it is difficult to deter an unknown actor.

In traditional crime scenes, when a crime is committed, a forensics team is called in to investigate the case and determine the criminal. Similarly, when a cyber attack is carried out, a cyber forensics team attempts to determine the original command-and-control center that delivered the attack. In other words, attribution here is the ability to link an actor with an action.[34] Like a traditional crime scene, a cyber attacker can leave many loops and holes in their trail, or mask their identity altogether. Only, it is much easier to do in cyber space. As mentioned earlier in this article, a number of well-known cyber attacks that have transpired over the last few years still remain unsolved. Cases where recent political events drive motivation are much easier to decipher, although the majority of the time, all "verification" is merely speculative. It generally takes a careless computer hacker to get caught, given the wide gap in sophistication between cyber attackers and cyber security tactics and technology, and the constant cat-and-mouse game that manifests between the two.

During the Cold War, attribution was a much easier question, thanks to the limited number of nuclear powers, and the very tangible destruction that was certain to immediately follow an attack.[35] In the contemporary cyber world however, attacks transpire at a much higher rate, and can be just as easily deployed by state and non-state actors from all over the world, in sharp contrast to nuclear or chemical warfare. Richard Clarke, co-author of Cyber War, points out that while many say that verification will never be 100%, there are still viable alternatives that should be considered:

> "say that every country has the responsibility to stop botnets [PCs hijacked with malware] attacking from within its borders. If every country that signed a treaty had a legal obligation to set up an enforcement mechanism to stop cyberattacks [sic] in their country, you wouldn't have to worry about whether an attack originally started in Brooklyn or Moscow. Just shut the [expletive] server off....With more time, I think we can solve the attribution problem. You can't find the origin of an attack in real time. But ultimately you can do the forensics if you can hack into all the servers. The NSA can do that. And the NSA tells me that attribution isn't really a problem.

Others have echoed this point, noting that the problem of attribution is particularly over-stated in high-end threats.[36]

---

[33] Lewis 1
[34] Goodman113
[35] Owens 294
[36] Knake 2

The EU's *Convention on Cybercrime* attempts to take on the problem of attribution, but falls heavily short of detail. It merely mandates a prompt response (deemed the "24/7 network") to incidences of cyber crime and requests for cooperation among member parties, as stipulated in Chapter 3 § 2 Article 31-35. In reality, the tremendous difficulty of enforcing existing criminal laws that pertain to computer network attacks has been widely noted, as many attacks go undetected, while others are never fully attributed, and investigations often end midway at an intermediary transfer point.[37]

Unlike the EU's *Convention on Cybercrime*, a future global cyber treaty will have to tackle the attribution question head-on. The provision must be flexible enough to anticipate and withstand evolving cyber tactics and technology, yet rigid enough to ensure a standard level of proof. This standard level of proof must also be robust enough to embrace and preempt botnets, a system used for many years now to route attacks through innocent bystanders. It is therefore essential for an effective cyber treaty to differentiate between the source of an attack, and the actual origin of the command and control center. To accomplish this, Jeffrey Carr – a renowned cyber intelligence expert – recommends that the onus be places on Internet services providers, and enforced at the national level.[38] Requiring nation states to police their own territory is of course analogous to current laws governing land and sea. In the cyber context, private actors would be responsible for more closely verifying the identities and actions of their customers and clients.[39] While this will allow for easier attribution, it is important to consider how these stakeholders might respond after being assigned with this new burden, and to what extent they are currently capable of carrying out the task.

As mentioned earlier, the interests of private actors in cyberspace does not necessarily coincide with the *national* interest of their host government. Furthermore, customers of Internet service providers may reject the expanded authority of the providers, which could be perceived as an encroachment upon their privacy and other civil liberties. Mechanisms that enable attribution ipso facto require enhanced collection and dissemination of private, identifiable information. This flavor of resentment would no doubt most vocally manifest within the West, and particularly within the United States, where the Fourth Amendment of the *Bill of Rights* provides protection against "unreasonable" searches. Achieving some level of balance between respect for privacy and the need to determine attribution is essential, and reaching a compromise amongst global powers might prove to be the most contentious subject during the negotiation stages. One only needs to consider the vastly different convictions surrounding privacy rights and democratic values in China and the United States – across cultural and statutory paradigms – to appreciate just how tempestuous this discussion will be.

It's also worth noting that, in the era of cloud computing, assigning private actors and the governments hosting them with the responsibility for attribution may already be antiquated. The cloud – an omnipresent space that hosts remote computing services – crosses national borders and multiple regions of jurisdiction, and represents the "ultimate example of globalization."[40]

[37] Denning 2
[38] Carr 1
[39] Ibid
[40] Schjolberg 12

The existence and growing popularity of the cloud underscores the importance of globally harmonized laws, pursuant to the provisions of an international treaty for cyber space.

One final consideration for the attribution provisions of a future global cyber treaty is regarding transparency; or more clearly, whether or not methods and procedures should be hidden. Transparency is a virtuous goal in any democratic society, but in the world of cyber warfare, too much transparency could prove counterproductive. Access to attribution methodology could be used by would-be computer hackers to exploit loopholes and evade cyber forensic experts and investigators. A unique relationship between national security agencies and private actors (i.e. Internet service providers) may be necessary to maintain an appropriate and constructive level of asymmetrical information between these entities and citizen-customers.

A closer look at the relationship between Google Corp and the National Security Agency (NSA) in the United States is useful for exploring the dynamics of a private/public partnership in the cyber domain. After announcing that Google's corporate infrastructure (along with at least twenty other large corporations from a wide range of industries) was the target of cyber attacks which appeared to have originated in China, the Internet company declared that they had taken an unprecedented step to share information surrounding the attack with relevant authorities.[41] This sharing of information eventually morphed into an alliance. Anonymous sources with knowledge of the relationship stated that "the alliance is being designed to allow the two organizations to share critical information without violating Google's policies or laws that protect the privacy of Americans' online communication," and further emphasized that "the deal does not mean...that Google will be sharing proprietary data."[42] This was a radical turn-around in Google's relationship with the NSA, as they had previously (and vocally) eschewed cooperation in its *Terrorist Surveillance Program*. One of the most clever aspects of this arrangement, whatever its final details may be, is the way in which it conceals details regarding the attribution process which could be exploited by a future cyber attacker, while simultaneously ensuring consumers that Google's "Do No Evil" ethos will not be violated. While there was some outcry amongst consumer groups, few customers dared to boycott Google products and services. Further, the series of attacks that precipitated this unlikely marriage illustrate the incentive for private Internet related companies to cooperate with government agencies, despite the various costs incurred. Legal scholars keen to draft an international cyber treaty to control attacks should continue to explore how this relationship between Google and the NSA continues to evolve. Although, it is worth emphasizing that the lessons learned from a public/private partnership in the United States will not be applicable in all non-American contexts.

5. Deterrence

It is difficult to discuss the issue of attribution without considering the question of deterrence. While the concept of deterrence is limited to some extent in cyberspace due to the interdependence of operators and combatants in this truly global and interconnected domain, it still has an important and constructive role. Deterrence in the form of "Mutually Assured

[41] "A New Approach to China," Official Google Blog. January 12, 2010. <http://googlepublicpolicy.blogspot.com/2010/01/new-approach-to-china.html>
[42] Nakashima 1

Destruction" and second-strike capability is an oft-cited rationale for the avoidance of a nuclear war during the post World War II era of bi-polarity.[43] Yet applying this premise to cyber warfare become rather murky, especially when considering the aforementioned question of attribution, in addition to the complicated issue of proportionality.[44] Determining what type of measures will be effective in deterring actors in cyber space to not carry out malicious attacks will be a difficult task. Rather than delving deeper into what specific deterrence mechanisms should be used, I will instead highlight how these mechanisms should be designed in a global cyber treaty to enhance effectiveness.

First and foremost, different deterrence measures will be needed for different types of actors, as the interests and motives of traditional state-actors can contrast sharply with those of non-state actors. Depending on the scenario and the intent, non-state actors may have much less to lose, even if apprehended, than state-actors. International sanctions and even litigation in the World Court may be in order for the latter, while a trial by jury and extensive fines are a more appropriate deterrent for the former. Furthermore, due process for non-state actors should parallel that prescribed by the Stanford Proposal, as highlighted earlier in this paper.

Second, in addition to attribution regulations, a deterrence mechanism will also require some sort of global verification system. Ronald Deibert, a renowned cyber scholar based at the University of Toronto, has prescribed a system that is predicated on earlier arms verification systems, such at the Comprehensive Test Ban Treaty (CTB) Verification System.[45] This extant system consists of 321 monitoring facilities strategically located around the globe to help detect possible violations to the CTB.[46] The stations cover various domains, and stretch across oceans and uninhabited lands as well. The networked system allows for monitoring facilities to notify a central server in the case of suspicious activity that sets of warning signals, and adheres to a rigid set of standardized procedures for verification and attribution. Applying this system to cyber space would not require as many monitoring facilities around the world, or even that they be geographically dispersed to encompass land, air, and sea. Instead, there would have to be enough facilities to handle the swath of digital data that would come through its servers, and a degree of geographic coverage that parallels information and communication technology penetration rates around the world. The point here would not be to have facilities as close to potential cyber war actors as possible, but instead, to ease access to Internet service providers. As one would expect, the most difficult problem with developing an effective verification system will be gaining trust and cooperation from not only private actors like Internet service providers and telecommunication companies around the world, but also national governments who may have tactical reasons – on the basis of national security – to not cooperate with a global verification system in certain cases. But ultimately, the creation of a global verification system will not only ease the process of attribution, but also enable a degree of deterrence.

While deterrence will never be full-proof, the inclusion of some sort of standardized, international system will be far superior to the status quo, which is ineffective at best at and counterproductive at worst. In addition to deterrence, the other four elements described in this

[43] Knake 2
[44] Ibid
[45] Deibert Presentation at MIT
[46] Ibid

section – terms and definitions, peaceful use clauses, signatory obligations regarding private actors, and attribution – should all be carefully considered by international lawmakers when hammering out a final draft for a global cyber treaty. Appraising these five elements will allow the global community to focus its limited resources on the much more logical goal of controlling behavior in cyber space, rather than trying to control the proliferation of arms in this quickly evolving domain.

CONCLUSION

It is likely that the world of 2040 will be as odd to an observer from 2020, as today's world would seem to a spectator from 1920. This reality makes the lawmaking process significantly more difficult, particularly in the continuously evolving domain of cyberspace. In a recent interview, Richard Clarke, America's terrorism czar under three administrations, boldly noted: "Around the world 20 to 30 nations have formed cyber war military units. Everything we were talking about 10 or even 20 years ago in terms of cyber war is happening, except for the development of relevant international law."[47] It is difficult to argue with Clarke's astute observation, particularly in the shadow of highly publicized cyber attacks around the world, from Estonia to Iran and from United State to China. The sooner an international convention for cyberspace is formulated, the sooner states can avoid duplicating security efforts, and begin to more efficiently monitor and protect this vital, global network, instead of just stopping at their domestic borders. But considering the historical record of other international arms control conventions to form in traditional domains of warfare, there will likely be a few remaining states that refuse to join, and a few more that refuse to ratify, a future convention on cyberspace.

To compensate for this lack of global convention on cyberspace, cyber powers around the world have invested to varying degrees to defend their national infrastructure, while others have gone further to invest in offensive and kinetic capabilities. Some countries now have dedicated divisions within their military and intelligence agencies to defend against and engage in cyber warfare. China, Russia, Israel, and the United States are the most heavily cited countries active in this new domain of war. Of all the world cyber powers, Russia has led the way for attempting to engage in multilateral talks, and bilateral talks with the United States for many years now. In the past, the United States has either refused, or left the Russians with a cold shoulder in response. However, there are some indications that the tides may have shifted following the Goolge-China fiasco that commenced in late 2009. In June 2010, General Keith B. Alexander – head of the newly inaugurated U.S. Cyber command, noted: "I do think that we have to establish the rules and I think what Russia's put forward is, perhaps, the starting point for international debate – not at my level, but at levels above me."[48] This admission is a promising step forward, even if it only resolves in the creation of a bilateral agreement. Such an agreement between two of the worlds most powerful national actors in cyberspace could be a stepping stone towards a all-encompassing global treaty to control behavior in cyberspace. In the shadow of the recent Stuxnet worm – an attack that permeated around the globe and still remains un-attributed – underscores the importance of establishing a global cyber arms regime sooner rather than later.

[47] Greenberg 1
[48] Talbot 2

REFERENCES

"2010 Joint Operating Environment." (2010) *United States Joint Forces Command*. <http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf>

Abbott, Kenneth W. (1993) "Trust But Verify: The Production of Information in Arms Control Treaties and Other International Agreements." *Cornell International Law Journal*, Vol 26, No 1: 1-58.

Adler, Emanuel. (2009). "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control." *International Organizion*, Vol. 46, No. 1: pp.101-145.

Brenner, Susan W. Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford, UK: Oxford University Press, 2009.

Brown, Davis. (2006) "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict." *Harvard International Law Journal*. Vol. 47, No 1. Winter 2006, pp 179-221.

Carr, Jeffrey. (2009) "Projecting Borders into Cyberspace." *Security Focus*. Published April 28, 2009. <http://www.securityfocus.com/columnists/500>

Chayes, Antonia. (Summer 2008). "How American Treaty Behavior Threatens National Security." *International Security*. Vol. 33, No. 1, pp 45-81.

Clarke, Richard A. and Robert K. Knake. Cyber War: The Next Threat to National Security and What to do about it. Ecco. 2010.

Deibert, Ronald J. (2010) "Militarizing Cyberspace," *Technology Review*. MIT Press. July/August 2010. <http://www.technologyreview.com/computing/25570/>

Deibert, Ronald.J. (2003) "Unfettered Observation The politics of Earth Monitoring from Space" In W Henry Lambright (Eds). Space Policy in the Twenty-First Century.

Deibert, Ronald J. (2010) "The Geopolitics of Cyberspace: From Militarization to Arms Control." Presentation at MIT, Cambridge, MA. May 13, 2010.

Denning, Dorothy. (2007) "The Ethics of Cyber Conflict." *Draft of March 27, 2007*.

Denning, Dorothy E. (2001). "Obstacles and Options for Cyber Arms Controls." Presented at *Arms Control in Cyberspace*, Heinrich Boll Foundation, Berlin, Germany. June 29-30, 2001.

Maclean, William. (2010). "Spies and hackers exploit world cyber rule void." *Reuters.* Published February 22, 2010. Accessed September 8, 2010. <http://www.reuters.com/article/idUSTRE61L37B20100222>

Falliere, Nicolas et al. (2010). "W32.Stuxnet Dossier." *Security Response*. Symantec. September 2010, version 1.0. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>

Fearon, James. (1998) "Bargaining, Enforcement, and International Cooperation." *International Organization.* The MIT Press. Vol. 52, No. 2: pp269-305.

Goodman, Seymour E. and Herbert S. Lin, (eds). (2007) Toward a Safer and More Secure Cyberspace. National Academies Press, 2007.

Gorman, Siobhan. "U.S. Backs Talks on Cyber Warfare." *The Wall Street Journal Online.* Dow Jones and Company. June 4, 2010. <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html>

Greenberg, Andy. (2010). "Security Guru Richard Clarke Talks Cyberwar." *Forbes.com* – Magazine Article. April 8, 2010.

Hughes, Rex. (2010). "A Treaty for Cyberspace." *International Affairs.* Blackwell Publishing Ltd/The Royal Institute of International Affairs. 86: 2(2010). 523-541.

Intelligence Squared U.S. Debate. "The cyber war threat has been grossly exaggerated." Transcript prepared by National Capitol Contracting. June 8, 2010.

Janczewski, Lech J. and Andrew M. Colarik (eds). (2008). Cyber Warfare and Cyber Terrorism. IGI Global 2008.

Kelsey, Jeffrey T.G. (2008). "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." *Michigan Law Review.* Vol. 106, No. 7:1427-1455.

Keys, Ron, Charles Winstead and Kendra Simmons. (2010) "Cyberspace Security and Attribution." *Improving the Future of Cyberspace...Issues, Ideas, Answers*. National Security Cyberspace Institute. July 20, 2010.

Knake, Robert K. (2010) "Untangling Attribution: Moving to Accountability in Cyberspace." Prepared Statement. Hearing on *Planning for the Future of Cyber Attack*. July 15, 2010.

Koremenos, Barbara, Charles Lipson and Duncan Snidal. (2001) ""The Rational Design of International Institutions." *International Organization.* Vol. 55, No. 4: pp761-799.

Lewis, James A. (2010). "Cyber War and Competition in the China-U.S. Relationship." Remarks delivered at the China Institutes of Contemporary International Relations, May 13, 2010. Center for Strategic and International Studies.

Lewis, James A. (2009). "The Fog of Cyberwar: Discouraging Deterrence." Center for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland.

Lipson, Charles. (2010). "Why are Some International Agreements Informal?" *International Organization*. The MIT Press. Vol. 45, No. 4: pp495-538.

Markoff, John. (2010). "A Silent Attack, but not a Subtle One." *New York Times*. Published September 26, 2010. Accessed September 30, 2010. <http://www.nytimes.com/2010/09/27/technology/27virus.html?>

Morozov, Evgeny. (2009) "Cyber-Scare." *Boston Review*. July/August 2009. <http://www.bostonreview.net/BR34.4/morozov.php>

Mueller, M., J. Mathiason, et al. (2007). "The Internet and Global Governance: Principles and Norms for a New Regime." *Global Governance*. 13(2): 237-254.

Muller, Harald. (2000) "Compliance Politics: A Critical Analysis of Multilateral Arms Control Treaty Enforcement." *The Nonproliferation Review*, Summer 2000: pp77-90.

Nagorski, Andrew. "Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway." East West Institute. April 2010.

Nakashima, Ellen. "Google to enlist NSA to help it ward off cyberattacks." The Washington Post. February 4, 2010. Accessed September 16, 2010. <http://www.washingtonpost.com/wpdyn/content/article/2010/02/03/AR2010020304057.html>

Owens, William A,; Kenneth W. Dam, and Herbert S. Lin, *Editors*. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington , D.C.: The National Academies Press, 2009.

Schear, James A. (1985) "Arms Control Treaty Compliance: Buildup to a Breakdown?" *International Security*, Vol. 10, No. 2: pp 141-182.

Schjolberg, Stein. (2010) "International Law as a Framework for peace and Security in Cyberspace." A presentation at the EastWest Institute 7th Worldwide Security Conference. February 17, 2010.

Schjolberg, Stein and Solange Ghernaouti-Helie. "Global Protocol on Cybersecurity and Cybercrime: An initiative for peace and security in cyberspace." Oslo: E-dit, 2009.

Schneier, Bruce. "U.S./Russia Cyber Arms Control Talks." *Schneier on Security Blog*. Published December 14, 2009. Accessed June 9, 2010. <http://www.schneier.com/blog/archives/2009/12/usrussia_cyber.html>

Setear, John K. (2010) "Responses to Breach of a Treaty and Rationalist International Relations Theory: The Rules of Release and Remediation in the Law of Treaties and the Law of State Responsibility." *Virginia Law Review*, Vol. 83, No. 1: pp.1-126.

Shackelford, Scott. (2010). "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law*. Vol 27, No 1: 191-251.

Sofaer, Abraham D. et al. (2000) "A Proposal for an International Convention on Cyber Crime and Terrorism." *Stanford University*.

Talbot, David. (2010). "Exposing Hackers as a Deterrent." *Technology Review*. Published at MIT. April 13, 2010. <http://www.technologyreview.com/computing/25060/>

Talbot, David. (2010). "New Cyber Chief Outlines Strategy." *Technology Review*. Published at MIT. June 10, 2010. <http://www.technologyreview.com/web/25526/>

Tanji, Michael. (2009). "Burying Nitze: Calling for an end to cold-war analogs for info-war situations." *Threatswatch.* Center for Threat Awareness. December 8, 2009. http://threatswatch.org/analysis/2009/12/burying-nitze/

Townsend, Kevin. "No first cyber strike? Time for an international cyber treaty?" Personal Blog. Published February 1, 2010. Accessed June 8, 2010. <http://kevtownsend.wordpress.com/2010/02/01/no-first-cyber-strike-time-for-an-international-cyber-treaty/>

"UN Chief Calls for Treaty to prevent cyber war." AFP. January 30, 2010. <http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4I4yAA>

Wheeler, David A., and Gregory N. Larsen. (2003) "Techniques for Cyber Attack Attribution." *Institute for Defense Analysis*. IDA Paper P-3792.

Wilson, Clay. (2006) "Information Operations and Cyberwar: Capabilities and Related Policy Issues." *CRS Report for Congress*. Congressional Research Service. Updated September 14, 2006.