Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

ESCAPING THE CYBER STATE OF NATURE: CYBER DETERRENCE AND INTERNATIONAL INSTITUTIONS

Ryan T. KAMINSKI[1]

Columbia University, New York, USA

Abstract: The existing literature related to cyber security tends to conclude that states cannot rely on so-called 'cyber deterrence' to prevent cyber attacks. A little analysis, however, discusses why this is the case and if cyber deterrence can ever be a practical national or international security strategy. Analyzing four cases of cyber attacks against states, this paper isolates three variables acting to hinder cyber deterrence including the lack of a cyber legal lexicon, difficulty in tracing cyber attacks, and too low levels of transparency when establishing national cyberwarfare policies. It is argued such factors can be manipulated via the use of international institutions as evidenced by the existence of the Chemical Weapons Convention, Nuclear Non-Proliferation Treaty, and certain aspects of the post-9/11 Bush Doctrine. The task before states then, is to re-think purely domestic approaches to cyber security.

Keywords: cyber warfare, international institutions, cyber deterrence, international organizations, national security

Disclaimer: This research was performed under an appointment to the U.S. Department of Homeland Security Scholarship and Fellowship Program, administered by the Oak Ridge Institute for Science and Education through an interagency agreement between the U.S. Department of Energy and DHS. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE, or ORAU/ORISE.

1 Columbia University School of International and Public Affairs, 420 West 118th Street, New York, New York, 10025, Email: rtk2107@columbia.edu.

INTRODUCTION

In an editorial. David Tohn (2009), National Security Fellow at Harvard's Kennedy School of Government, compares cyberspace with Thomas Hobbes' chaotic state of nature arguing, "The world of cyber-crime, cyber-terrorism, and cyber-warfare is truly a wild, unruly, and ungoverned place" (p. 17). Another study from the Center for Strategic and International Studies (CSIS) argues that cyber security currently presents one of the "most urgent national security problems" facing the US (Lewis, Langevin, McCaul, Charney, & Raduege, 2008). A RAND Corporation commission concerning cyber security concludes, *"deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace"* (Libicki 2009). Overall, the majority of literature on the emerging concept of cyberwarfare seems to follow a more or less similar pattern of reasoning.

Specifically, articles and reports on the subject tend to sound the alarm, deploy a titillating term like 'cyber-vigilantes,' and pessimistically conclude that states cannot expect to rely on a Cold War-inspired state of deterrence. Other literature commonly focuses on cyber crime and cyber terrorism against the private sector, giving comparatively little attention to the possibility of cyber attacks among states. Given that the respected computer security company McAfee estimates that as of 2007 at least 120 countries were engaging in research to use the internet for war fighting purposes, the US and NATO, if not the entire world, faces a growing threat (Takeda, Ferraro, Edwards, Blum, & Vaile, 2007, p. 12). Unfortunately, a scant amount of literature discusses in detail what specific factors act to preclude grafting the notion of deterrence onto the concept of cyberwarfare. Consequently, only minimal discussion has emerged concerning whether such variables can be manipulated.

To fill this conceptual gap, I examine four cases of cyber attacks and how they highlight the difficulties of relying on deterrence to prevent or mitigate the use of cyber attacks between states.[2] The cases include cyber attacks against Estonia in April 2007, cyber attacks against Georgia in August 2008, the worldwide 'GhostNet' attacks occurring between May 2007 and March 2009, and the string of cyber attacks against South Korea–US interests in July 2009.[3] Analyzing these cases, I find three main factors currently preventing states from relying on cyber deterrence. They include: the lack of a comprehensive legal lexicon regarding cyber attacks; no return address for those individuals, groups, and states committing cyber attacks; and too little transparency and public debate when crafting national cyberwarfare policies.

---

2 The term "cyber attack" is used in order to remain as neutral as possible concerning what is and what is not an act of cyberwar, cyber espionage, etc.

3 Most computer servers remain unaware they have been infected by GhostNet. The March 2009 date refers to the last *recorded* infiltration.

It is argued that while such factors present significant obstacles for creating an international strategic environment where cyber deterrence is possible, they are not insurmountable. Specifically, past international accords and norms such as the Chemical Weapons Convention (CWC), Nuclear Non-Proliferation Treaty (NPT), and particular aspects of the post-9/11 Bush Doctrine provide convincing evidence that an international institutional approach, rather than the conventional 'one-state one-policy' framework, presents the most efficacious path for establishing a foundation for cyber deterrence.

1. FOUR CASES

1.1 ESTONIA – APRIL 2007

Beginning on April 27, 2007, a series of coordinated distributed denial of service (DDoS) attacks were launched primarily against Estonia's government-run websites. Many analysts have speculated that the Estonian government's decision to move a Cold War-era statue motivated the cyber attack ("Estonia Fines," 2008). With Estonia's Parliament declaring online access a human right in 2000 as well as Estonia being considered "one of the world's most wired countries," the attack carried the potential to severely disrupt everyday cyber activity in the country (Brookes, 2008).

Despite Estonia's considerable emphasis on its citizens having internet access, however, the April 2007 DDoS attacks did not cause significant damage to Estonia's infrastructure or government websites. Rather, the attack caused temporary access-related problems for Estonians attempting to view webpages such as the website of the Prime Minister's political party (Sanger, Markoff, & Shanker, 2009, p. 1). A fake apology for relocating the Cold War memorial was also allegedly posted on the Prime Minister's webpage (Wickramarathna, 2009). Elsewhere, other government-sponsored links were corrupted to misdirect users to iconic pictures of Soviet soldiers and quotations from Martin Luther King, Jr. about fighting evil (Wickramarathna, 2009).

Later, Estonian Foreign Minister Urmas Paet would publicly accuse Russia of sponsoring the attack, but would later admit that neither Estonia nor NATO had any direct evidence to support such a claim (Wickramarathna, 2009). In January 2008, an ethnic Russian-Estonian college student was tried and convicted for carrying out part of the attack on the Estonian Reform Party's website and fined around $1,350 ("Estonia Fines," 2008).

1.2 GEORGIA – AUGUST 2008

Early in its August 2008 war with Russia regarding the breakaway territories of South Ossetia and Abkhazia, Georgia was a victim to a host of cyber attacks also allegedly emanating from Russia. Specifically, two rounds of DDoS attacks were launched against Georgian government websites as well as respected Georgian media outlets. Several private websites such as *StopGeorgia* were also established complete with easy-to-use software for caring out DDoS attacks ("Marching," 2008).

According to the *Economist*, however, the "actual damage done was minimal: some e-mail was disrupted and targeted websites were rendered unavailable to the public" ("Marching," 2008). The genuine significance of these acts, however, is hard to measure as other countries including the US, Estonia, and Poland mirrored Georgia's original government websites (Korns & Kastenburg, 2009). Absent such assistance, the official US Army website found that Georgia risked becoming "cyber-locked" or having no access to the internet (Korns & Kastenburg, 2009).

Once again, Russia would claim it was not involved in the attacks ("Georgia Targeted", 2008). Most analysts seem to agree that Russian nationalists were responsible for the attack using BOT or "zombie" networks to facilitate the DDoS campaign ("Georgia Targeted," 2008). Whether such individuals received assistance directly from Moscow remains unclear.

1.3 GHOSTNET – MAY 2007 THROUGH MARCH 2009

Contrasting from the attacks on Georgia and Estonia were the massive so-called 'GhostNet' attacks which occurred globally over a 22-month period between 2007 and 2009. According to researchers at Toronto University's Munk Centre for International Studies 1,295 computers in 103 countries were allegedly infiltrated ("Chinese Ghost," 2009). Unlike the cyber attacks targeting Estonia, however, most analysts conclude that one of the most important features of the GhostNet attacks concerned its power to whisk away potentially sensitive information using a combination of phishing and malware strategies.

One study conducted at the University of Cambridge Computer Laboratory firmly points the finger at Chinese authorities for operating GhostNet, as the Tibetan government in exile was a key target of the cyber attacks ("Chinese Ghost," 2009). A joint Toronto University and Ottawa think-tank research group also reportedly found evidence that the Tibetan government's computer system had been corrupted to send relevant Tibet-related information back to servers in China, but did not di-

rectly accuse the Chinese government of carrying out the attack (Jacobson, 2009).

In response, an official from the Chinese government declared, "I will not be surprised if this report is just another case of their recent media and propaganda campaign" (Harvey, 2009). Another problem with putting the blame for the GhostNet attacks on China is the fact that the software used to infiltrate various foreign websites and government officials' email accounts was discovered to be available online using a Google Search (Kelly, 2009). It is also unclear what strategic motivation China would have to steal information from states and entities targeted in the attack such as Barbados, Malta, Cyprus, Portugal and Hong Kong.

1.4 SOUTH KOREAN & US INTEREST ATTACKS – JULY 2009

The last case concerns a concentration of attacks in July 2009 overwhelmingly targeting South Korean and US government and military interests. Beginning on July 4th, the attacks occurred in three waves primarily relying on a DDoS strategy. Specifically, the websites of the US White House, National Security Agency, Federal Aviation Administration, State Department, Secret Service, Treasury, Federal Trade Commission, and South Korea's National Intelligence Service were targeted (Siobhan & Ramstad, 2009). Compared to other small-scale cyber attacks, the *Wall Street Journal* notes that the July 2009 cyber attacks "were among the broadest and longest-lasting assaults perpetrated on government and commercial Web sites in both countries" (Siobhan & Ramstad, 2009).

Once again, general expert opinion seems to conclude that damage associated with the attacks was minimal. Jose Nazaro (2009), manager of security research at Arbor Networks, notes, "The code is really pretty elementary . . . I'm doubting that the author is a computer science graduate student" (Sang-Hu & Markoff, 2009). A White House spokesperson also claimed the attacks had "absolutely no effect on the White House's day-to-day operations" (Sang-Hu & Markoff, 2009). It is worth noting, however, that the US Treasury Department's, Trade Commission's, and Department of Transportation's websites were all briefly shut down during the attack ("US Eyes").

While a recent South Korean investigation cites North Korea as the perpetrator, an opposition South Korean political party claims such findings are little more than a callous attempt by one agency to increase its power and influence within the South Korea government (Sang-Hu & Markoff, 2009). Although some officials have noted the attacks almost perfectly overlapped with North Korean missile tests and a UN Security Council resolution passed against the country, there is little conclusive evidence linking North Korea to the attacks (Siobhan & Ramstad, 2009). One North

Korean embassy official claimed that rumors of North Korea's involvement in the cyber attacks were baseless (Siobhan & Ramstad, 2009).

2. VARIABLES AFFECTING CYBER DETERRENCE

The four cases consistently point to three key variables that preclude states from relying on cyber deterrence. They include the absence of a cyber legal lexicon, difficulty in determining the source of cyber attacks, and low levels of transparency and genuine public discussion on the subject of cyberwarfare strategy and defense. In this section each variable will be clarified.

2.1 LACK OF A UNIVERSALLY ACCEPTED CYBERWARFARE LEXICON

Anyone reading lay articles, think-tank studies, published manuscripts, or even government reports on cyber attacks is likely to find a dizzying array of terms sometimes referring to the same concept. For example, should a DDoS attack that causes disruptions to a government website, yet does not steal any sensitive information, be considered an act of cyberwar, cyber espionage, or cyber vandalism?

The implications of lacking a generally accepted vocabulary in this area are twofold. First, depending on what lexical framework is used, international and customary law can be interpreted to permit vastly different reactions to the same cyber attack. For example, if two states have contrasting lexicons concerning cyberwarfare, one could view a cyber attack as an act of war, while the other could conceptualize it merely as an act of cyber vandalism ("Marching Off," 2008). Second, given that some states even lack a universally accepted cyber glossary among their various domestic civilian and military agencies, the possibility of misinterpreting a potential cyber attack on the national level also remains high (Shanker & Markoff, 2009).

Looking at the Estonian and Georgian cases, this problem is uniquely apparent. Tohn (2009), for one, hyperbolizes the attacks against both states as "cyber-blitzkriegs," regardless of such a term's connotation with an all-out military attack from World War II (p. 17). Former US Deputy Assistant Secretary of Defense Peter Brookes (2008) even classifies the attack on Estonia as a "pre-emptive digital strike" despite the lack of any significant evidence that Estonia was planning a cyber attack on Russia. Jaak Aaviksoo, Estonia's Defense Minister, also declared that the cyber attack against his country "cannot be treated as hooliganism, but has to be treated as an attack against the state" ("Marching Off," 2008). Even though Estonia did not end up

invoking Article V of the NATO charter which commits states to treat an attack on one member as an attack on themselves, the defense minister's comments nonetheless illuminate major problems associated with the lack of a comprehensive cyberwarfare lexicon. While Estonia did construct a NATO-sponsored facility in its capital to study cyber security, this also may do little good if non-NATO members like China and Russia are relying upon an entirely different cyber language.

Similarly, while many respected media outlets referred to the cyber attacks against Georgia as acts of 'cyberwar', other analysts have concluded that this is not the case, as the attacks did not cause any "physical harm" ("Marching Off," 2008). Others, however, counter that the attacks on Georgia can still be considered 'cyberwarfare' as they were accompanied by a military offensive ("Marching Off," 2008).

In a similar vein, classification of the GhostNet attacks as activity related to a "global spy network" or as an act of 'cyber espionage' remains in dispute (Jacobson, 2009). For example, a critical legal difference may exist between a cyber attack that merely downloads information or one that actually takes control of sensitive computers. Arguing GhostNet was capable of the latter, the Information Warfare Monitor (IWM) group clarifies, "The GhostNet system directs infected computers to download a Trojan known as Ghost Rat that allows attackers to gain complete, real-time control" (Harvey, 2009, p. 29).

While the cyber attacks committed against South Korea and the US raise issues similar to the Estonian and Georgian cases, the former case also posits questions concerning what a proportional response to a cyber attack should be. Given that several government websites went down in the US, it is difficult to hypothesize what an appropriate US response would have been had it known with certainty that North Korea committed the attacks. A recent high-level US panel on the subject of cyber attacks, for example, noted its concern over a disturbing 2004 Pentagon statement on a similar scenario. Notably, the Pentagon statement claimed that in the event of a cyber attack, "on US commercial information systems or attacks against transportation networks" the US should consider the use of nuclear weapons (Shanker & Markoff, 2009). Additionally, while the 2010 US nuclear strategy rules out nuclear retaliation in response to cyber attacks, it delineates exceptions for certain states including Iran and North Korea (Sanger & Baker, 2010, p. A1).

2.2 DIFFICULTY IN DETERMINING THE ORIGINS AND/OR PERPETRATORS OF CYBER ATTACKS

Another inherent problem with cyber deterrence concerns difficulty in determining who is committing the cyber attack. If the attacker is not a state, another question to

answer concerns to what extent states have a responsibility to prevent or investigate attacks committed by non-state actors operating within their sovereign territory. According to US Deputy Defense Secretary William J. Lynn III, "Deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace, where it is so easy for an attacker to hide" (Waterman, 2009, p. B01).

While many signs seem to point to Moscow in the Estonia and Georgia cases, there is still no hard public evidence that Russia committed the attacks ("Marching Off," 2008). James Lewis (2009), Director of the CSIS Technology and Public Policy Program, disputes the notion that countries—including Russia—cannot stop cyber attacks from being executed within their territory:

> *We should not forget that many of the countries that are havens for cyber crime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept.*

Similar charges have been made against China regarding GhostNet. In, *Tracking GhostNet,* Robert Deibert notes, "The most significant actors in cyberspace are not states. In China, the authorities most likely perceive individual attackers [i.e. teenagers in internet cafés] as convenient instruments of national power" (Jacobson, 2009). Another headache for determining who was responsible for the GhostNet attacks concerns the fact that the software associated with GhostNet was easily accessible to virtually any internet user. One cyber security analyst told a reporter, "It's a nice piece of software – easy interface . . . You can do it yourself" (Kelley, 2009).

Finally, the July 2009 attacks on South Korea and US interests raise complex issues regarding infected 'zombie' computers around the globe inadvertently participating in cyber attacks against other countries. Specifically, South Korea's spy agency concluded computers from 16 different countries participated in the DDoS attacks. Rafal Rohozinski, an investigator for IWM, further notes, "Attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local" (Sanger et al, 2009).

2.3 INADEQUATE TRANSPARENCY AND PUBLIC DISCUSSION ON CYBERWARFARE

Further precluding the possibility of cyber deterrence is the high amount of secrecy concerning cyberwarfare-related policymaking. Overall, this has especially been true for the US. Many international security analysts, for example, have noted a growing hypocrisy on the part of the US in criticizing the stealthy cyberwarfare policies of other states like China and Russia while remaining incredibly secretive about US cyber policy (Glenny, 2008). Marcus Sachs, who helped to establish one of the first government cyberwarfare units in the US, argues, "We need to have a public debate, not a classified conversation" (Waterman, 2009).

The US Cyber Consequences Unit also conducted a comprehensive study of the cyber attacks targeting Georgia. Problematically, though, only certain portions of it were made public (Fulghum, 2009).[4] The group's conclusions—as described by an anonymous IT official familiar with the group's work—included the idea that the cyber attacks against Georgia had "direct" benefits for Russia's military (Fulghum, 2009). Given such a revelation, it is unfortunate the report was not made public and able to contribute to the already limited public literature on the implications of integrating cyber attacks with traditional military operations.

Next, while no firm evidence has solidly linked China to the GhostNet cyber attacks, many have nonetheless faulted China's lack of military transparency especially in the area of cyber security. Bill Gertz (2008), a journalist with the *Washington Times*, claims anonymous Pentagon sources have discovered that "There is growing evidence ... that rather than simply adopting Western-style military secrecy, China's military is engaged in a wider effort at denial and deception." The same Pentagon officials further clarified that one of the most non-transparent areas of the Chinese military concerns cyberwarfare (Gertz, 2008).

On the other side of the Pacific, the US has been critiqued for lacking a public and coherent cyber doctrine in the wake of the July 4th cyber attacks. According to a *Washington Post* editorial published eights days after the attacks began, "lack of a guiding vision has implications beyond mere inefficiency. The nation's cyber-defenses are being developed without any structure to guarantee transparency and accountability" ("Cyber czar," 2009, p. A10). Another report conducted by a high-level panel organized by the National Academy of Sciences entitled "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities,"' also finds that a lack of open discussion about cyberwarfare within the US could have significant negative effects for US military policy (Shanker & Markoff, 2009). Moreover, while the South Korean National Intelligence Service claimed it was

4 A summary of the US Cyber Consequences Unit report on the 2008 cyber attacks against Georgia was made public and can be found in the bibliography under Borg and Bumgarner.

extremely likely that "North Korea" or "North Korean sympathizers" were behind the attacks, and no evidence was provided as it had been deemed "classified" ("U.S. Eyes," 2009).

3. THE CASE FOR AN INTERNATIONAL APPROACH

This section shows that the three cyber deterrence variables have successfully been manipulated in the past through the CWC, NPT and Bush Doctrine. It will also present evidence that the current approach to cyber security is problematically overwhelmingly centered at the national level, particularly in the US.

3.1 A NATIONAL SECURITY ISSUE

By and large, the world's preeminent military power, along with other major powers, has focused on the development of a cyberwarfare strategy on the national level rather than the international. This, however, must change if the possibility of cyber deterrence being a reasonable option for states—rather than a scenario where states just attempt to dominate the cyberwarfare landscape or engage in cyber arms races—is to exist. One US military officer argues, "The fortress model simply will not work for cyber . . . Someone will always get in" (Sanger et al, 2009, p. 1). While bilateral or regional agreements toward this end should generally be considered a step in the right direction, they carry similar problems associated with the current one-state, one-policy approach to cyber attacks.

At the UN, the US and its allies have balked at Russian attempts to construct a cyber attack treaty from a belief that such an accord would merely protect states lacking the capacity to engage in cyberwarfare (Adams, 2001, p. 104). Larry McKee, an adviser to US Strategic Command, however, believes such reluctance may be more logistics-related. He notes, "There are so many stakeholder organizations and individuals in the cyberdomain it is difficult to know exactly where to start the collaboration, information sharing, and integration" (Waterman, 2009). On the other hand, the existence of a UN Convention on Cyber crime and a comparable EU accord show the notion of a cyberwarfare treaty is not entirely without precedent. Additionally, Geoffrey Darnton (2006), Head of Knowledge Transfer for the Institute of Business and Law, finds that the 1977 Geneva Protocol may provide a foundation for the regulation of cyberwarfare as it specifically expands the jurisdiction of the accord to include "new weapons . . . means or method[s] of warfare" (p. 147).

Others, however, have posited that it may be best to start regionally. Duncan Hollis,

a law professor at Temple University, finds regional organizations like NATO or the EU should first formally clarify a set of cyber attack standards amongst themselves ("Marching Off," 2008). Again, while such a development would not be negative per se, problems could still arise if different regional organizations or states have clashing cyber lexicons. Several Russian military officers have reportedly endorsed the doctrine that "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself" (Hildreth, 2002, p. 13-15). James Lewis (2009) clarifies the implications of the national versus international cyber security problem:

> *We have, at best, a few years . . . to modernize our laws to allow for adequate security . . . The United States will need to define doctrine for the use of the cyber attack as a tool of national power. It would benefit from an effort to reshape the international environment for cyber conflict in ways that could reduce risk, to win consensus (as we did with proliferation) on a set of norms and constraints for cyber conflict ("Korean Cyber attacks").*

3.2 CHEMICAL WEAPONS CONVENTION

Opened for signatures in January 1993, the CWC presents startling evidence of the success of the international community's ability to regulate specific types of warfare. Regarding the accord's global effect, James Caroll (2008) with the *Boston Globe* eloquently summarizes, "The 1993 convention has been ratified by almost every nation on Earth . . . Their [chemical weapons] legitimacy has been entirely removed, their permanence rejected. The poison gas realists of 1919 have been proven wrong" (p. A15). According to David Cooper (2002) in *Competing Western Strategies against the Proliferation of Weapons of Mass Destruction*, "the mere existence of a legal prohibition provides a meaningful disincentive for covert possession by participants, despite a low probability of detection" (p. 27).

Beyond mere symbolism, the CWC contains a tri-level lexicon for understanding what can and cannot be considered a chemical weapon subject to the convention's regulations. This includes Schedule 1, 2, and 3-type weapons, along with criteria for determining what chemicals fall under what Schedule and specific disarmament- related obligations ("Article 1 Obligations"). Article II of the CWC also lays out accepted interpretations for chemical weapons-related components as well as for verification instruments ("Definitions and Criteria").

Next, the CWC contains provisions not only regarding what acts are prohibited by the treaty, but also obligations for states not to transfer chemical weapons to non-state actors. In particular, the convention demands that state-parties actively work

to prevent the use of chemical weapons. Article I, for example, orders members of the convention not "to develop, produce, otherwise acquire, stockpile or retain chemical weapons, or transfer, directly or indirectly, chemical weapons to anyone" as well as not "to assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State Party under this Convention" ("Article 1 Obligations").

3.3 NUCLEAR NON-PROLIFERATION TREATY

Opened for signatures in July 1968, the NPT has been signed by 189 countries and constitutes the foundation of the international nuclear non-proliferation regime. US President Obama's recent demand for renewed efforts towards universal nuclear weapons disarmament at a special session of the UN Security Council presents a testament to the strength and durability of this accord (Kessler & Sheridan, 2009). Overall, the NPT provides substantial evidence that establishing a cyber legal lexicon as well as increasing transparency concerning cyberwarfare is possible.

For example, the NPT distinguishes "nuclear weapon states" from "non-nuclear weapon states" while also clarifying what sorts of nuclear technology the latter are and are not entitled to receive (IAEA, 1970). Another little discussed norm associated with the treaty concerns nuclear weapon states agreeing not to employ their weapons against non-nuclear states unless the latter allies with a nuclear state or uses a nuclear weapon which it recently acquired (Kimball, 2005). While some nuclear states have recently stretched this perceived rule in regard to the targeting of nuclear weapons and declaratory policies, Kimball (2005) notes that this has only been done for 'rogue' states (2005).

Another growing norm associated with the NPT concerns obligations to prevent terrorists from acquiring nuclear weapons. The effect has been the establishment of new multilateral agreements like the 2003 Proliferation Security Initiative (PSI) designed to prevent the proliferation of nuclear materials and other weapons of mass destruction. Mark Shulman, (2006) with the Strategic Studies Institute, notes that the PSI "has received widespread support . . . United Nations Secretary-General Kofi Annan has explicitly endorsed it . . . at least 60 nations are participating in it."

Pertaining to transparency, the NPT calls upon non-nuclear weapon states to submit to IAEA inspections. While critics will likely point out that certain countries have ignored such provisions, the IAEA nonetheless has been able to carry out investigations in Iraq, Iran, and North Korea in the past. While the occasional nuclear weapons breakout scenario has occurred, the normative power associated with the IAEA and NPT has still inarguably invalidated former President Kennedy's prediction that there would be 15-20 new nuclear weapon states by 1970 (Allison, 2004).

3.4 THE BUSH DOCTRINE

While international scholars continue to debate the efficacy of the Bush Doctrine, in terms of US foreign policy, one aspect of it as declared in September 2001 before a joint session of the US Congress, is uniquely applicable to the second variable acting to preclude cyber deterrence. President Bush stated,

> *"We will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime" (Whitehouse, 2001).*

This statement places an affirmative obligation on states to prevent non-state actors from operating and launching attacks from within their territory. While many US foreign policy experts and historians have critiqued this part of the Bush Doctrine as representing a radical departure from previous international law, it seems for better or worse to have been accepted by many key players at the international level. Russia, for example, has invoked the doctrine in its ongoing struggle with Chechnya, and Israel has used it to justify its numerous incursions into Palestinian territories (Diehl, 2002, p. A21). Some political pundits in the US have even argued that the Obama Administration's recently enunciated policy towards Pakistan resembles a tacit endorsement of the Bush Doctrine ("Matalin," 2009).

4. CONCLUSION

While Tohn offers a pessimistic view of contemporary cyber security reminiscent of Hobbes' hellish state of nature, he forgets that Hobbes ultimately concludes that individuals lacking any sense of industry or justice will eventually come together and empower a Leviathan to rescue them from such chaos. There is no doubt that neither the UN nor any other currently existing intergovernmental organization remotely resembles a Hobbesian Leviathan, but this is not to say that a cooperative international approach is entirely impractical when linked to cyber attacks.

On the contrary, factors inhibiting the implementation of cyber deterrence strategies including the lack of a cyberwarfare lexicon, difficulty in tracing cyber attacks to their state or non-state origins, and a lack of transparency can and must be addressed at the international level rather than merely the national. Past international agreements and norms such as the CWC, NPT, and certain aspects of the Bush Doctrine provide convincing evidence that cyber deterrence can be a possibility given that states are willing to commit the political muscle to do so. If an international

cyber security regime with widely accepted norms and procedures concerning cyberwarfare can be built, the costs of 'cheating' will radically increase, making the execution of shadowy cyber attacks a less and less tantalizing option for states. The probability of a cyberwar instigated by miscalculations or accidents will also drop as nations will have a forum to discuss their disputes. Finally, states will also have an incentive to preemptively detect, target, and neutralize non-state groups wishing to carryout cyber attacks from within their territory rather than just looking the other way. The challenge now is for states to recalibrate their cyber security policies from the national to international arena.

REFERENCES

- A Chinese Ghost in the Machine: Cyberwarfare. 2009, April 4. *Economist.*
- A. Guidelines for Schedules of Chemicals . (n.d.). *Organisation for the Prohibition of Chemical Weapons.* Retrieved February 4, 2010, from http://www.opcw.org/chemical-weapons-convention/annex-on-chemicals/a-guidelines-for-schedules-of-chemicals/
- Adams, J., 2001. Virtual Defense. *Foreign Affairs, 80*(3).
- AFP. (2008, August 12). AFP: Georgia targeted in cyber attack. *Google*. Retrieved February 4, 2010, from http://afp.google.com/article/ALeqM5iRuGsssizXAKVgmPqAXOxqB5uHsQ
- About the Convention. (n.d.). *Organisation for the Prohibition of Chemical Weapons*. Retrieved February 4, 2010, from http://www.opcw.org/chemical-weapons-convention/about-the-convention/
- Allison, G. 2004, January 1. Nuclear Terrorism - FAQs. *Nuclear Terrorism: The Ultimate Preventable Catastrophe - Home*. Retrieved February 4, 2010, from http://www.nuclearterror.org/faq.
- BBC, 2008, January 25. *Front Page*. Retrieved February 4, 2010, from http://news.bbc.co.uk/2/hi/technology/7208511.stm
- Borg, S. & Bumgarner J., 2008. Overview of the US-CCU of the Cyber Campaign Against Georgia in August of 2008. US Cyber Consequence Unit. Retreived April 5, 2010, from http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf
- Brookes, P., 2008, March 4. The Cyber Challenge. *The Heritage Foundation - Conservative Policy Research and Analysis*. Retrieved February 4, 2010, from http://www.heritage.org/press/commentary/ed031008c.cfm
- Carroll, J., 2008, June 23. If Poison Gas Can Go, Why Not Nukes. *Boston Globe.*
- CNN, 2009, December 6. Matalin: With AfghanistanSurge: Obama Resembles George W. Bush. *CNN*. Retrieved February 4, 2010, from politicalticker.blogs.cnn.com/2009/12/06/matalin-with-afghan-surge-obama-resembles-george-w-bush/.
- Cooper, D. A., 2001. *Competing Western Strategies Against the Proliferation of Weapons of Mass Destruction: Comparing the United States to a Close Ally.* Westport, CT: Praeger Publishers.
- Diehl, J., 2002, April 29. Free Pass on Chechnya. *Washington Post.*
- Fulghum, D., 2009, September 14. Cyberwar is Official . *Aviation Week & Space Technology, 171,* 0.
- Geoffrey, D., 2006. Information Warfare and the Laws of War. In D. Webb Ed. *Cyberwar, Netwar and the Revolution in Military Affairs* (pp. 139-151). New York: Palgrave Macmillan.
- Gertz, B., 2008, August 21. Plugged In--National Security. *Washington Times.*
- Glenny, M., 2008, June 26. Cyber armies are gearing up in the cold war of the web. The Guardian.
- Harvey, M., 2009, March 30. Chinese hackers 'using ghost network to control embassy computers.' *Times Online*. Retrieved February 4, 2010, from http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece
- Hildreth, S., 2001. Terrorism and the Future of US Foreign Policy. In J. Blane Ed. *Cyberwarfare: Terror at a Click (*pp. 1-22). New York: Novinka Books.
- Jacobson, S., 2009, March 31. China denies involvement in GhostNet cyber-attacks *The First Post*. Retrieved February 4, 2010, from http://www.thefirstpost.co.uk/46883,news-comment,news-politics,china-denies-involvement-in-GhostNet-cyber-attacks
- Kelley, C., 2009, March 31. Cyberspies' code a click away. *Toronto Star*. Retrieved February 4, 2010, from http://www.thestar.com/article/610860
- Kessler, G., & Sheridan, M. B., 2009, September 24. Security Council Adopts Nuclear Weapons Resolution. *Washington Post*. Retrieved February 4, 2009.
- Kimball, D., 2005, February 15. The Future of the Nuclear Non-Proliferation Regime. *Arms Control Association* . Retrieved February 4, 2009, from https://www.armscontrol.org/events/20050219_AAAS

- Korns, S., & Kastenbeg, J., 2009. Georgia's Cyber Lefthook. *Parameters, 38(*4). Retrieved February 4, 2010, from http://74.125.93.132/search?q=cache:http://www.usamhi.army.mil/USAWC/Parameters/08winter/contents.htm
- Levy, C., 2009, May 27. In Siberia, the Death Knell of a Complex Holding a Deadly Stockpile. *New York Times.*
- Lewis, J., Langevin, J., McCaul, M., Charney, S., & Raduege, H., 2008. Securing Cyberspace for the 44th Presidency. *Center for Strategic and International Studies.* Retrieved February 4, 2009, from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
- Lewis, J., 2009, October 1. The "Korean" Cyber Attacks and Their Implications for Cyber Conflict | Center for Strategic and International Studies. *Center for Strategic and International Studies.* Retrieved February 4, 2010, from http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict
- Libicki, M., 2009, December 1. Cyber deterrence and Cyberwar. *RAND Corporation.* Retrieved February 4, 2009, from http://www.rand.org/pubs/monographs/2009/RAND_MG877.sum.pdf
- Marching off to cyberwar., 2008, December 6. *Economist (US).*
- Membership of the Biological Weapons Convention. (n.d.). *The United Nations Office at Geneva.* Retrieved February 4, 2010, from www.unog.ch/80256EE600585943/(httpPages)/7BE6CBBEA0477B52C12571860035FD5C?OpenDocument
- MSNBC., 2009, July 2. U.S. eyes N. Korea for 'massive' cyber attacks. *MSNBC.* Retrieved February 5, 2010, from http://www.msnbc.msn.com/id/31789294
- President Declares "Freedom at War with Fear", 2001, September 20. *Welcome to the White House.* Retrieved February 4, 2010, from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html
- Sanger D., Baker, P., 2010, April 6. Obama Limits When US would Use Nuclear Arms. *New York Times.*
- Sanger, D., Markoff, J., & Shanker, T., 2009, August 28. US Plans Attack and Defense in Web. *New York Times.*
- Sang-Hu, C., & Markoff, J., 2009, July 9. Cyber attacks jam government and commerical websites in U.S. and South Korea. *New York Times.*
- Siobhan, G., & Ramstad, E., 2009, July 9. Cyber Blitz Hits US, South Korea. *Wall Street Journal.*
- Shulman, M., 2006, April 1. The Proliferation Security Initiative as a New Paradigm for Peace and Security. *Strategic Studies Institute.*
- Takeda, K., Ferraro, M., Edwards, G., Blum, R., & Vaile, D., 2010, February 5. 2007 Virtual Criminal Report: The Next Wave. *McAfee Corporation.* Retrieved February 1, 2010, from http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_en.pdf
- Tohn, D., 2009, June 11. Digital Trench Warfare. *Boston Globe.*
- Treaty on the Non-Proliferation of Nuclear Weapons. (1970, April 22). *International Atomic Energy Agency.* Retrieved February 4, 2010, from http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf
- Waterman, S., 2009, July 2. U.S. takes aim at cyberwarfare. *Washington Times.* Retrieved February 5, 2010, from http://www.washingtontimes.com/news/2009/jul/02/us-takes-aim-at-cyberwarfare/
- Wentworth, T., 2008, August 23. How Russia May Have Attacked Georgia's Internet. *Newsweek.* Retrieved February 4, 2010, from http://www.newsweek.com/id/154965
- Where is our Cyber czar?, 2009, August 12. *Washington Post.*
- Wickramarathna, W., 2009, August 27. Online edition of Daily News. Retrieved February 4, 2010, from http://www.dailynews.lk/2009/07/27/fea02.asp