Foreign Policy and Cyber Weapons

By Dylan Powers
Major Research Paper
Submitted to Prof. Richard French
Submitted to Prof. Michael C. Williams

Foreign Policy and Cyber Weapons[1]

Contents

[1] Title adapted from Henry Kissinger's seminal work, *Foreign Policy and Nuclear Weapons*

Abstract

This essay explores the challenges of ensuring cyber security internationally and what needs to be done for Western-aligned states to address cyber weapons internationally. At present, the prevailing approach by the major powers in cyber space is antagonistic and destabilizing. To address this situation and ensure international peace is maintained, a comprehensive approach is needed. This approach should draw upon the lessons learned during the early years of the Cold War. During this time, international norms concerning nuclear weapons were in their nascent stage and the international system was only just beginning to settle into a bi-polar structure. Today, by drawing an analogy between nuclear weapons and cyber weapons and utilizing the lessons learned during the Cold War, the international community can ensure that the introduction of cyber weapons does not threaten the stability of the international system.

Introduction

Cyberspace is the backbone of modern societies. Computer systems are responsible for running many aspects of daily life, from banking systems, electrical grids, and traffic systems. Utilizing cyber systems has allowed states to increase their productivity and improve the lives of their citizens. Today, many societies are completely dependent upon cyberspace to facilitate the smooth operation of their economies, ensure law and order, and provide basic services, such as power and water. However, cyber dependence has created national insecurity as these systems are open to attack and infiltration from foreign states' military and intelligence apparatus. The damage that can be done to a modern society through cyber operations is unfathomable. Many academics have suggested that cyber weapons may share parallels with weapons of mass destruction (WMDs). The world has already witnessed numerous conflicts in cyberspace and the weaponization of cyberspace is happening at a furious pace. Furthermore, the implications of an unchecked arms race in cyberspace can have dire consequences for international peace and stability, yet recent developments suggest that this race has already begun. Out-dated national security strategies must be reconfigured to accommodate the threat posed by cyber weapons.

This will have implications on how states' view their relative power and act internationally. Today, statesmen are faced with a challenge to reassess old doctrines of how to achieve international peace. However, the goal remains the same—to craft a lasting, stable international order. This will be even more challenging now than in the past as an international consensus on the use of cyber weapons has yet to emerge among the major powers, namely China, Russia, and the United States

This paper will explore the question of how modern statesmen can create international treaties to address cyber weapons. To begin, this paper will first outline the challenges for survival in a cyber age. This will be achieved by first describing the nature of cyberspace, cyber power, and cyber warfare, as well as the dilemmas for security that arise from society's dependence on cyberspace. These dilemmas will include an overview of the variety of threats and vulnerabilities in a cyber dependent society and an overview of the first usage of a cyber weapon by one state against another. The subsequent section will outline the similarities and differences between nuclear weapons and cyber weapons. Understanding how international treaties surrounding these weapons were crafted will provide an apt blueprint for how the world should respond to cyber weapons; this paper will therefore examine which past strategies can be replicated. Then, this essay will proceed to argue the world's traditionally understood large actors (US, Russia, and China) are pursuing divergent and conflicting strategies on cyber weapons, which that can have destabilizing consequences. Ultimately, this paper will argue that the international system needs an approach for cyber weapons that is drawn on the world's experience addressing nuclear weapons.

The Challenges of Survival in Our Time

Understanding Cyberspace and Cyber Power

History has shown that the "likelihood of a new arms race is high when disruptive technologies dramatically alter the means and methods of war… and as nations aspire to project power in cyberspace, a new digital arms race appears imminent".[2] The US, for one, is actively defending against cyber aggression from foreign nations.[3] This policy decision is based on the "diversity of potentially hostile entities building cadres of cyberwarriors, probing [their] systems for weaknesses, infiltrating U.S. government networks and making similar attempts against American businesses and critical industries – including defense systems".[4] Indeed, evidence suggests that states are utilizing cyber weapons to improve their strategy position vis a vis the US. This is because "asymmetrical responses have become easier to execute and difficult to defeat".[5] States no longer need to engage in decades of military build-up to improve their relative power. As the world moves from a unipolar order to an increasingly multi-polar world, the introduction of cyber weapons presents a potentially destabilizing and relatively unknown element with the ability to upset traditional calculations of power and capability. Indeed, it is important to understand cyber space and cyber weapons in order to incorporate them into any strategic considerations.

Cyberspace is a difficult concept to accurately define. It is ethereal in nature, yet it concretely affects peoples' lives every day. In rare instances it can be instrumental in toppling

---

[2] Hughes, Rex. "Towards a Global Regime for Cyber Warfare", *The Virtual Battlefield: Prospectives on Cyber Warfare* (IOS Press, 2009), p. 106

[3] Testimony by Mary Ann Davidson, Chief Security Officer at Oracle, to the United States House of Representatives Subcommittee on Emerging Threats, Cyber security, and the Science and Technology, Source: http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Davidson-Oracle-SFR_10Mar09.pdf

[4] Testimony by Mary Ann Davidson

[5] Fareed Zakaria, *The Post-American World* (WW Norton, 2008) [audiobook]

governments—as the world witnessed in Tunisia and Egypt—and reshaping the relations between the individual and society. Cyberspace is often defined as "the electronic world created by interconnected networks of information technology and the information on these networks… it is the global commons where more than 1.7 billion people are linked together to exchange ideas, services, and friendships."[6] Technically, cyberspace is an "evolving man-made domain for the organization and transfer of data using various wavelengths of the electromagnetic spectrum. The domain is a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information".[7] Thus, its key features are that it is man-made, designed to carry information, and operated through a partnership with government and private actors.

There are also several features of cyberspace which have implications for national security. It is not restricted by geopolitical borders, exists across the globe, and is readily accessible to all nations, if they choose to join. China and North Korea have been success at partitioning creating their own internet and erecting strong firewalls to curb unwanted content from reaching their citizens. Cyberspace is also more than just the internet; it includes financial transnational networks and networks which operate critical infrastructures, such as power grids, traffic lights, and nuclear facilities. As well, attributing cyber attacks to a responsible party and determining whether their actions were deliberate or accidental is extremely difficult.[8] The specific characteristics of cyberspace reduce power differentials between actors, and "thus

[6] Department of Public Safety Canada, *Canada's Cyber Security Strategy*, 5 October 2010 [online] available from http://www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.
[7] Major Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", in *Air Force Law Review* (2009), Vol. 64, p. 68
[8] Major Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", p. 68

provides a good example of the diffusion of power that typifies global politics in this century".[9] This is evident in the large number of actors operating on a level-playing field. Individual hackers and large government agencies are equally capable of doing damaging in cyberspace. It is difficult to speak about dominance in cyber space. Greater cyber power is often achieved through increasing dependence on cyber systems which in turn creates more vulnerabilities. While they have more resources to dedicate to the problem, power in cyber space does not favour the wealthy or large nations. For this reason, national responses have been dominated by offensive technology rather than defensive. These instruments can produce both hard and soft power. Soft power can be achieved through international statements in support of free internet, providing support to internet dissidents in cyber oppressive societies, or establishing international norms about the usage of cyber weapons. This could involve attracting software engineers to adhere to a specific idea of internet openness or supporting human rights groups fighting for free access to the internet. Hard power in cyber space can be used to attack the internet's infrastructure or nationally important facilities, such as critical infrastructures, services, or corrupting computers. Table 1 illustrates the various ways that information tools can be used to exert soft and hard power. [10]

TABLE 1: PHYSICAL AND VIRTUAL DIMENSIONS OF CYBER POWER

TARGETS OF CYBER POWER		
	WITHIN CYBERSPACE	OUTSIDE CYBERSPACE
Information Instruments	Hard: Launch denial of service attacks. Soft: Set norms and standards.	Hard: Attack SCADA systems. Soft: Initiate public diplomacy campaign to sway opinion.
Physical Instruments	Hard: Enforce governmental control over companies. Soft: Introduce software to help human rights activists.	Hard: Destroy routers or cut cables. Soft: Stage protests to name and shame cyber providers.

Power relations interact in a variety of ways in cyber space, providing many opportunities for states to exert power to guard their

[9] Joseph Nye, "Power and National Security in Cyberspace", in *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011) [available online] http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf

[10] Joseph Nye, "Power and National Security in Cyberspace"

national security. At the same time, however, it creates many vulnerabilities and explains why achieving security in cyberspace is so difficult.

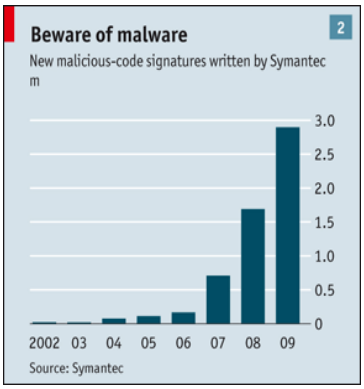
The threats are diverse and vulnerabilities many in a cyber dependent world. Yet, the most devastating threat to any state would be a concerted cyber attack carried out by a prepared nation. The greatest fear among US officials is an "electronic Pearl Harbor", where an adversary "could strike a sudden, crippling blow against the information systems on which the US military forces, financial institutions, and society depend. The result would be chaos and destruction."[11] In this scenario, phone systems would collapse, public transit systems malfunction and crash, and banks would become inaccessible. Ultimately, critical infrastructures would be disrupted to a point where normal functioning of society would be impossible. While this scenario is theoretically possible, the US Naval War College has concluded that it is highly unlikely for a non-state actor to accomplish. [12] This assuages fears of cyber terrorism, however state cyber attacks will always have the potential to be the most disruptive

Hard power usage of cyber weapons by national governments can fall into two categories: attacks against the physical infrastructure of cyber systems and attacks against the information stored on cyber systems. Often, even when the physical infrastructure is the main target, a degree of information compromise forms part of the operation. Attacks on information can take many forms. They can include data attacks, which occur when an opponent inserts data into an information system to make the system malfunction or tricking it into performing unauthorized

[11] Center For Strategic and International Security, *Cybercrime, Cyberterrorism, and* Cyberwarfare, (The CSIS Press, 1998), p. 2

[12]Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", in *International Political Science Review* (2006), Vol. 27, No. 3. P. 226

actions.[13] Other attacks on information are jamming radio signals, corrupting system files, or simply broadcasting deceptive propaganda. Another form of attack is software attack, in which malware is inserted into a system to carry out functions or crash the system. The use of malware has grown exponentially in recent years, and the skills required to create these programs are widely taught over the internet to future hackers (see chart).[14]



Finally, hacking is an important tool for the attack of information systems. Hackers seize control of a system to disrupt, deny use, steal resources, steal data of value, gain intelligence of enemy movements, or to otherwise cause harm.[15] Security researchers have discovered a form of software attack, coined "advanced persistent threats",[16] which aim to steal confidential information over a prolonged period of time after establishing themselves in a target's cyber system.

Physical attacks on cyber systems take advantage of the inherent vulnerabilities of the internet and the physical and digital weaknesses of cyber space. Globally, the physical infrastructure is fragile. More than nine-tenths of internet traffic flows through undersea fibre-optic cables, which are dangerously bunched up into a few, small choke points around New York, the Red Sea, or the Luzon Strait in the Philippines.[17] Other areas of vulnerabilities are frequently arising; weakly-governed areas of Africa are being connected to fibre-optic cables, which can

[13] Center For Strategic and International Security, *Cybercrime, Cyberterrorism, and* Cyberwarfare, (The CSIS Press, 1998), p. 10
[14] The Economist, *The Threat from the Internet: Cyberwar*, 1 July 2010 [online] available from http://www.economist.com/node/16481504
[15] *Ibid*
[16] Ilias Chantzos, "Opinion: Joining Battle on the Cyber Warfare Front", in *Jane's Defence Weekly*, December 6, 2010 (IHS Global Limited, 2010)
[17] The Economist, *War in the Fifth Domain*, July 1st 2010, [online] available at http://www.economist.com/node/16478792?story_id=16478792

create new, easily accessible intrusion points.[18] Another important vulnerability is the speed at which digital attacks can strike. In 2004 the Sasser virus spread to every core Internet router in less than an hour, causing an estimated $3.5 billion in damages.[19] The ability of an attack to cripple a system at mindboggling speed means that reactive measures to counter cyber attacks are inadequate on their own. Proactive measures, such as automatic fail safes, must be in place to protect against an attack. Another glaring vulnerability comes from our critical and non-critical infrastructures, as the recent Stuxnet virus demonstrated.

Stuxnet Virus – The Shot Heard Round the World

In June 2010, a 'cyber worm' attacked Iranian nuclear facilities at Natanz. [20] Subsequently, the virus was detected within critical infrastructures in over 60,000 computers around the world, with more than half of them in Iran. While the virus continues to spread, its effectiveness bas been diminished due to known responses and a built in expiry date of June 24th, 2012. [21] After analyzing the virus, experts have concluded that the only likely developer was a national military, due to the unusual characteristics of the code and the specific nature of its mission The purpose and design on this worm opened the world's eyes to the fact states were creating cyber weapons to attack adversaries.

Stuxnet was only designed to render a specific part of the Iranian nuclear weapon development program inoperable.[22]. It is a specific program designed to penetrate and gain

[18] I*bid*
[19] *Ibid*
[20] In cyber talk, a 'worm' is a malicious program or code inserted into computer systems without user permission or knowledge. They spread automatically from computer to computer and can replicate themselves hundreds of thousands of times. See 'Worms', OnlineCyberSafety, http://www.bsacybersafety.com/threat/worms.cfm
[21] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", in *Survival* (2011)Vol. 53, No. 1. p. 27
[22] The Economist, *The Stuxnet Outbreak,* Sept 30th, 2010 [online] available at

control over systems semi-autonomously. Its targets were 'air gapped', which means they were not connected to the internet. Infecting 'air gapped' computers has occurred in the past, notably at the US CENTCOM, however, it is generally thought of as the surest way to protect a system from intrusion. Stuxnet began by hunting down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These drives are responsible for regulating the electric current that affects the power fed to motors operating nuclear centrifuges. As centrifuges must operate at very high speeds, Stuxnet altered the frequency of the electrical currents of the motors, causing them to vacillate between high and low speeds over a period of months. The key to Stuxnet is that it can attack both known and unknown centrifuges, thus the assailants hoped to damage secret nuclear enrichment facilities within Iran.[23]

The sophistication, specific function, and purpose of the virus suggests that national militaries are investing resources in developing offensive cyber weapons. The most likely culprit is the United States, in collaboration with Israel. This incident provides insight into the evolution of cyber warfare thinking within US security agencies. The code of Stuxnet was an amalgamation of hacker tools found all over the cyber crime black market. This allowed the creators to hide their own capabilities and made attributing who was responsible almost impossible. Consequently, this also made it easy to disarm. As well, Stuxnet provided a low-cost weapon capable of disrupting or destroying Iran's nuclear facilities. Air strikes against Iranian facilities would be highly expensive, carry huge political risk, and break international conventions. Yet, this virus was able to achieve the goal of significantly setting back Iranian activities at a low cost and without any overt political repercussions. The International Atomic

---

http://www.economist.com/world/international/displaystory.cfm?story_id=17147818

[23] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", p. 29

Energy Agency reported that Iran ceased feeding uranium into Natanz centrifuges for a week, along with an overall 23% decline in the number of operating centrifuges, which could indicate a major, temporary breakdown of the reactor.[24] Regardless of the true extent of the damage, Stuxnet provides a window into the future of cyber war.

In 2007 Estonia was attacked by patriotic Russian hackivists who were angry over a government decision to remove a Russian war monument. Their efforts shut down the Estonian state, from government websites to banking services. Often, this attack is regarded as the first cyber war. Stuxnet, however, is much better illustration of what a state-on-state cyber attack would resemble. Unlike the cyber attack against Estoina in 2007, this time it was clear that one state (or a coalition) was attacking another in cyber space. Stuxnet was designed as a 'cyber missile' aimed at specific targets, presenting a new dimension to cyber attacks in international conflict. Estonia featured a loose coalition of angry protestors exploiting easily accessible and unsophisticated computer weaknesses. Stuxnet, on the other hand, was a weapons designed in a government cyber agency with a sole purpose of disrupting the critical infrastructures of another nation. In such a circumstance, however, it is difficult to determine the scale of the damage or identify the participants. Declarations of war are not needed and there appears to be little consequence for actions. To carry out an attack such as this, no nation has to appeal to international conventions, request a UNSC resolution, or cite a case for self-defence. Moreover, there is no agreement in the international community about whether this even constitutes an attack. By taking advantage of this legal grey zone, the creators of Stuxnet utilized a new tool for exerting power over another state, but have also opened up the possibility of escalation. Iran, who is believed to have significant cyber capabilities, can capitalize on the same legal ambiguity

[24] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", p 25

and carry out its own attacks clandestinely.[25] Already, the US congress has been warned that Stuxnet could be adapted into a weapon to attack its own critical infrastructures. Once used, the knowledge of cyber weapons can easily spread to anyone.

Given the scale of these threats, securing information assets is becoming a crucial component of any national security strategy. Stuxnet could have created a massive meltdown in Iranian nuclear facilities. For those who doubt the impact cyber weapons could have outside the virtual world, one only needs to look at Japan's nuclear crisis and imagine it resulting from a cyber terrorists or intelligence agencies. Like any virus, Stuxnet could have spread beyond the creators control and with unintended consequences. States need to begin seriously thinking about how to manage cyber weapons in order to reduce the likelihood of a cyber attack going horribly wrong.

Back to the Future

Analogies are an important tool for making policy. The appropriate use of historical analogies "can clarify the present situation, offer strategic insights, and inform policy options".[26] When done in a systematic way, it can educate policy makers, clarify the goals of a comprehensive cyber security strategy and avoid the pitfalls that a muddy historical analogy can bring. However, the incorrect use of analogies can also create unclear policy objectives and restrict the range of policy options. Too often, policy makers invoke the historical analogy of appeasement and Hitler to justify military adventurism. Already, the cyber security debate is rife with analogies, from the prediction of a coming "electronic Pearl Harbor" to using the public

[25] *Ibid*, pg. 33
[26] Sulek, David and Moran, Ned, "What Analogies Can Tell Us About the Future of Cybersecurity", *The Virtual Battlefield: Prospectives on Cyber Warfare* (IOS Press, 2009), p. 119

health term "virus" to describe malicious software. These references make the technically complex language of cyber security easily accessible and convey meaningful messages; however their glib applications can gloss over important nuances that separate the current situation from the past.

Overall, better decision making "involves drawing on history to frame sharper questions [on challenges] and doing so systematically".[27] No historical event can be a perfect analogy to a present crisis because underlying conditions will always be different and kinetic. But a thoughtful selection of historical analogies can offer insight for policy makers and anticipate the implications of their choices.[28] The value that forming analogies brings to the discussion is an appropriate lens through which to view the problem. They do not, however, provide clear cut policy options that can be applied without understanding the differences and nuances of the present condition. Despite the many similarities, the challenges posed by cyber weapons are quite different from nuclear weapons and any cyber strategy would need to reflect this. However, the goal in creating such a linkage, and for this essay, is to argue that the emerging realm of cyber warfare needs to be managed with as much care and awareness as nuclear weapons. To achieve this, the international community can draw lessons from the past.

Nuclear Weapons and Cyber Weapons – Similarities

The challenges of developing an effective cyber weapons strategy mirror many similarities with the challenges that faced the crafters of early nuclear strategies. Both were considered novel technologies with vast military applications, while also creating significant fear

[27] Neustadt, Richard E. and May, Ernest R., *Thinking In Time: The Uses of History by Decision Makers*, (The Free Press, New York, 1986)
[28] Sulek, David and Moran, Ned, "What Analogies Can Tell Us About the Future of Cybersecurity", p. 119

and anxiety about their indiscriminate use.[29] Both technologies offered a promise of revolutionizing how wars are fought and raised questions about their proper role in conventional warfare. At the beginning of the Cold War, there were few rules governing how or when nuclear weapons should be used. Currently, the usage of cyber weapons and cyber spying is in a wild-west stage, with new breaches being disclosed monthly. Reminiscent of the desperate attempts many nations have made over the last century to acquire nuclear technology, rising powers are utilising cyber weapons in order to shift power imbalances.

Similar to nuclear weapons, cyber power has the ability to shift power balances through technological developments *within* one's own territory, rather than through acquisition of territorial gains or access to resources.[30] For instance, the ability of the USSR to end the US's nuclear monopoly changed the balance of power far more profoundly than if they had conquered all of Western Europe. Cyber weapons can be developed clandestinely and can attack a society's backbone from thousands of miles away with just the click of a mouse. Achieving substantial cyber capabilities will shift the power balance away from established world powers to emerging countries or coalitions. For instance, a recently discovered computer espionage network called "Shady RAT" uncovered a 5-year long history of data thefts from over 72 international organizations, including ASEAN, UN, the Olympic Organizing Committee, and various national governments. McAfee, who uncovered this espionage ring, labeled it the "largest transfer of wealth in terms of intellectual property in history".[31] The shift of power during the Cold War occurred within a sovereign state's territory rather through territorial acquisition, which

---

[29] Jonah Friedman, "Cyber Weapons vs. Nuclear Weapons", at *Center for Strategic & International Studies*, 26 July 2011 [available online] http://csis.org/blog/cyber-weapons-vs-nuclear-weapons

[30] Henry Kissinger, *Foreign Policy and Nuclear Weapons*, (W.W. Norton, 1969), pg. 9

[31] Jim Finkle, "McAfee says it has uncovered biggest-ever series of cyber attacks", *Globe and Mail*, August 3rd, 2011 [available online] http://www.theglobeandmail.com/news/technology/tech-news/mcafee-says-it-has-uncovered-biggest-ever-series-of-cyber-attacks/article2117891/

ultimately resulted in an arms race rather than war. Currently, the world is experiencing a cyber arms race as each country attempt to gauge the capabilities of the other, while increasing their own capabilities.

Furthermore, the consequence of using nuclear weapons is so catastrophic, it has been impossible to define a *casus belli* which would lay out a moral case for the use of these weapons.[32] "Thinking the Unthinkable" was a common practice during the Cold War, as many people tried to imagine how a conflict would unfold and what the consequences would be. Phrases like "nuclear winter" and "mutually assured destruction" were created through public debate and academic research but also existed in popular culture. They contributed to an understanding of the threat that a nuclear arms race poised to global security. The same ambivalence around determining when an attack is serious enough to launch a nuclear weapon is echoed in politicians inability to properly determine what constitutes a cyber attack. Currently, it has been impossible to determine a *casus belli* for responding to a cyber attack with physical force because strategists have been unable to determine the lines that separating spying, sabotage, an act of aggression, or a cyber assault.

As the infamous nuclear attacks on Hiroshima and Nagasaki did in their time, cyber attacks can also have catastrophic and crippling effects on a society's fundamental ability to function. In the worst case scenario, a large scale cyber attack could bring down air traffic control systems, power and telecommunications grids, and destroy financial services and information. If these attacks were coordinated professionally, as opposed to a lone hacker or terrorist cell, they could destroy a nation's economy and deprive its population of basic services, such as electricity, water, and police and fire protection. Ene Ergma, the Speaker of the Estonian

[32] Henry Kissinger, *Foreign Policy and Nuclear Weapons*, (W.W. Norton, 1969), pg. 3

Parliament who has a doctorate in nuclear physics, first drew this parallel between nuclear and cyber attacks in his description of the cyber attack on Estonia, "when I look at a nuclear explosion and the explosion that happened in our country… I see the same thing".[33] Similar to nuclear weapons, the use of cyber weapons would inevitably target civilians. However, it is important to note that cyber attacks could never match the destructive capabilities of nuclear weapons. There is no equivalent to the notion of overkill or nuclear Armageddon for cyber weapons. This does not, however, undermine the grave and devastating economic consequences and societal impacts that a cyber war would have.

The difficulty of attribution is another shared characteristic, as one can only retaliate against an attacker if the source of the attack is known. Today, a country can reliably attribute the source of a nuclear strike, however this capability was not always a given. In cyberspace, an attack that is orchestrated by a nation-state could appear to be originating from a remote location, or even from computers within one's own territory. Many critics have claimed that deterrence cannot be achieved with cyber weapons because of the problem of attribution. Since a state cannot definitively know who has attacked them, retaliation is impossible to justify. Consequently, without the threat of retaliation, deterrence breaks down. Countries were eventually capable of correctly attributing the source of a nuclear attack and it is likely that, in time, this will also be possible in cyber space. Until then, offensive capabilities will have an advantage over defensive ones. When inter-continental ballistic missiles (ICBMs) were first introduced, effective defence became impossible and the advantage heavily favoured offensive

[33] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", in *Berkeley Journal of International Law* (2009), Vol. 27, No. 1 , p. 11

capabilities.[34] The current emphasis on defence rather than proactive measures is misguided given the advantages of offensive operations.

The relative ease and effectiveness of cyber attacks could allow for these weapons to create their own version of the stability/instability paradox that is familiar to nuclear strategists.[35] During the Cold War, this paradox meant that "to the extent that the H-bomb reduces the likelihood of full-scale war, it increases the possibility of limited war pursued by widespread local aggression".[36] Some strategists have theorized that cyber warfare will be able to provide an alternative to traditional armed conflict between states.[37] This might mean that cyber weapons will be successful in helping states avoid conventional wars. However, if states began to believe that they can achieve their military objectives while minimizing the physical costs of these operations, they will be more likely to enter into cyber conflicts.[38] Once engaged in these types of operations, the chances for escalation into physical conflict increases. Thus, the stability gained from cyber weapons at a macro level could lead to further instability at lower levels.

Nuclear Weapons and Cyber Weapons – Differences

Yet, in order to develop an effective way of defending against, and deterring, cyber attacks, it is important to understand vital differences between cyber warfare and traditional conflicts. Again, the analogy with nuclear weapons willbe useful in highlighting these differences. A key difference is that cyber attacks are occurring already, while no state has used a

---

[34] Jonah Friedman, "Cyber Weapons vs. Nuclear Weapons", at *Center for Strategic & International Studies*, 26 July 2011 [available online] http://csis.org/blog/cyber-weapons-vs-nuclear-weapons
[35] *Ibid*
[36] Michael Krepon, " The Stability Instability Paradox", at *Arms Control Wonk*, 2 November 2010 [available online] http://krepon.armscontrolwonk.com/archive/2911/the-stability-instability-paradox
[37] Michael Riley & Ashlee Vance, "Cyber Weapons: The New Arms Race", at *Bloomberg Businessweek*, 20 July 2011 [available online] http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html
[38] Jonah Friedman, "Cyber Weapons vs. Nuclear Weapons", at *Center for Strategic & International Studies*, 26 July 2011 [available online] http://csis.org/blog/cyber-weapons-vs-nuclear-weapons

nuclear weapon since 1945. Therefore, the lack of any inherent taboo against the use of cyber weapons makes it difficult to draw a line between acceptable and unacceptable limits. This also creates difficulties for crafting an appropriate and proportional response.

This has not, however, stopped the US from laying out how it would respond to a cyber attack, or publicly stating that any computer-based attack that damages US critical infrastructures would be considered an act of war.[39] This preliminary doctrine clearly states that it will not respond to a cyber attack with a cyber attack, but with conventional weapons. Recently, an anonymous Department of Defense official stated that "if you shut down our power grid, maybe we will put a missile down one of your smokestacks".[40] However, it failed to outline a minimum threshold of evidence for attributing a cyber attack to a state, the boundaries of what constitutes an attack, or the line which distinguishes civilians from military targets. Military and civilian organizations share the internet and it is not easy to distinguish between, say, the militaries communications system and civilians. The unique nature of cyber attacks means that conventional norms of discrimination and proportionality cannot be easily applied.

As mentioned, cyber space has a *private* actor dimension that did not exist for nuclear strategists. Militaries do not control the internet, nor can they take command of strategic sites that come under attack. For cyber offense, states that can harness the energies of their own underground hacking communities to attack foreign targets will have an advantage over a state that has a military who owns a monopoly over cyber weapons. China and Russia, for instance,

---

[39] Mark Clayton, "A US Cyberwar Doctrine? Pentagon documents seen as first step, and a warning", in *The Christian Science Monitor,* May 31, 2011 [available online] http://www.csmonitor.com/USA/Military/2011/0531/A-US-cyberwar-doctrine-Pentagon-document-seen-as-first-step-and-a-warning

[40] Siobhan Gorman & Julian E. Barnes, "Pentagon: Online Cyber Attacks Can Count as Acts of War", *Wall Street Journal*, May 31, 2011 [available online] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=googlenews_wsj#printMode

have been successful at courting their countries' organized crime syndicates and hacking communities to carry out attacks of foreign nations. Conversely, the US and its allies are waging a war against underground hacking communities such as Lulzsec and Anonymous. Thus, unlike with nuclear weapons, power in cyber space is dispersed to the effectiveness of the individual hackers rather than remaining in a government-owned missile silo. Indeed, an additional dynamic is that governments can also become the targets by their own citizens if their policies do not match the desires of a de-centralized hacking community. Therefore, the source of a nation's cyber power can be unpredictable and volatile.

For defense, proper cyber security needs the collaboration of a plethora of actors working toward a common goal. In nuclear deterrent strategy, civilian population did not need to cooperate beyond a tacit acceptance that they were passive hostages. Conversely, internet security is often distorted by market forces. If a company admits their systems are insecure, they can lose customers and have an incentive to keep breaches hidden from the public. Also, investing in proper computer security measures is expensive and the immediate benefits are not easily seen. Additionally, regulating companies to purchase security products would be a tax and largely unpopular. Certainly, the military is unable to ensure safety to all private actors on the internet in the same way they were able to through the creation of a nuclear umbrella. The man-power and money required to achieve this would be impossible to organize for a single entity, not to mention they lack the mandate to determine for private firms and individuals an acceptable level of security. This inability to ensure defence complicates strategies and favours offensive capabilities. This increases the need for international cooperation as states are unable to fully rely on their own ability to protect themselves. Creating a "cyber missile defense" is almost

impossible, and computer security strategists are forced to grapple with similar dilemmas facing strategists in the early stages of the Cold War.

Another important distinction between the Cold War and now is that the digital age does not reward shows of force. In order for nuclear deterrence to work then one's ability to retaliate cannot be kept a secret. However, "cyber weapons fall into the category of 'brittle' technology, susceptible to the swift development of countermeasures…The best weapon is one an enemy never knows exists".[41] This will make creating treaties governing their use and development difficult to negotiate, as states will have a large incentive to keep their full capabilities hidden. This also creates problems for states that wish to make declarative statements or issue assurances to their citizens of how they will respond in the event of an attack because it could render their arsenal obsolete. This explains why all states have not revealed their counter measures to a cyber attack, and few states have outlined their targets for retaliatory strikes.

Moreover, while the Cold War was a conflict between the US and Russia, the current era is characterized by a diffusion of power to smaller and smaller actors.[42] While the US occupies a position of unrivaled military strength, a number of potential rivals are emerging to challenge its superpower status. Moreover, many non-state actors, namely organized criminal groups and terrorist organizations, are striving to acquire cyber weapons. The allure of cyber weapons for small, non-state actors is high because the "costs of entry" are quite low—it costs very little to develop and maintain cyber capabilities.[43] This is a strong contrast to the investments made by the US and USSR in nuclear weapons to retain technological parity. Meanwhile, nations need

---

[41] Michael Riley & Ashlee Vance, "Cyber Weapons: The New Arms Race", at *Bloomberg Businessweek*, 20 July 2011 [available online] http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

[42] Joseph S. Nye, "Facing up to cyber security challenges", in *Power & Politics – Harvard Kennedy School Blog*, (2011) [available online] http://belfercenter.ksg.harvard.edu/power/2011/06/13/facing-up-to-cyber-security-challenges/

[43] Sulek, David and Moran, Ned, "What Analogies Can Tell Us About the Future of Cybersecurity", p.125

only spend a fraction of this to become a "cyber power". In 2002, the Naval War College estimated that it would only take five years and $200 million to conduct a major cyber attack.[44] Since then, knowledge of malicious computer codes have spread rapidly and this projected cost and time frame has likely dropped dramatically.

During the Cold War, the US was leading the race, both economically and technologically. The US was able to outspend the USSR in developing and building greater capabilities and, by the end, the economic disparity between the US and USSR was very pronounced. Moreover, the US had no significant trade relations with its principal enemy. This allowed them to grow economically independent from the USSR. In the cyber age, the landscape is very different.. Today, the US is much less wealthy and its main opponent in the cyber arms race, China, is not only a major trading partner but also the main creditor for the US. Indeed, the US has fallen behind significantly in this race[45]—Congress has been repeatedly warned about their strategic disadvantages in cyber space, yet responses are still in a nascent stage.

Lessons Learned

The nuclear aspect of US policy would be formulated under Eisenhower, who developed the doctrine of "massive retaliation" in the event of a nuclear attack—otherwise known as the strategic doctrine of deterrence.[46] Eisenhower summed up the dilemma these weapons technology created in his view that "there is no alternative to peace".[47] This "suicide or surrender" doctrine lacked credibility, and the concept of "mutually assured destruction" arose in large part

[44] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", in *Berkeley Journal of International Law* (2009), Vol. 27, No. 1 , p. 11
[45] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p. 63
[46] Heather S. Gregg, "Crafting a Better US Grand Strategy in the Post-September 11 World: Lessons from the Early Years of the Cold War", p. 243,
[47] Henry Kissinger, *Foreign Policy and Nuclear Weapons*, (W.W. Norton, 1969), pg. 10

to address the credibility gap. The spread of these weapons created a tacit nonaggression treaty through a recognition that war between the two powers was not a viable instrument of foreign policy, while simultaneously increasing each power's ability to annihilate one another. As the Cold War progressed, the weapons become more and more powerful, while with each new generation of missiles the reluctance to use them increased. Therefore, deterrence depended on a psychological element; it works best when military strength is coupled with the willingness to employ it.

Deterrence was buttressed with diplomatic efforts, such as arms control treaties and open negotiations between the two belligerent powers. Spreading the belief that arms control treaties were necessary to ensure international peace was facilitated by open debate and academic research and represents a utilization of US' soft power. This research was done by epistemic intellectual communities that worked collaboratively with their counterparts across the Iron Curtain. When the concept of arms control was first introduced in the 1950s, nuclear weapons were not completely understood. Concepts of nuclear winter, nuclear fallout, and escalation were in their infancy. As academics began to understand the repercussions of a nuclear war and the vulnerabilities that nuclear weapons created for international security, scientists and security analysts that comprised the US epistemic community began to advocate to US policy makers that creating binding arms control commitment would increase the chances of avoiding nuclear war and would enhance US' security.[48] Through joint academic meetings, US academics were able to share these beliefs with Soviet counterparts. These discussions slowly created a consensus around the need to limit the use and production of nuclear weapons. Emboldened by their

[48] Emanuel Adler, *Communitarian International Relations: The Epistemic Foundations of International Relations* (Routledge, 2005), p142

common belief, these epistemic communities lobbied governments, providing the technical knowledge legitimizing arms control and ultimately transforming their ideas into national security policy and practice for both countries. The 1972 Anti-Ballistic Missiles treaty created an international regime because the superpowers were able to "converge on an American intellectual innovation as the key to advancing both their irreconcilable differences and their shared interest in avoiding nuclear war".[49]

The Cold War offers a powerful analogy for the current cyber age. The image of a national struggle between powers for military, economic, and ideological supremacy has resonance in today's world. The espionage battles that happened below the surface of public knowledge are mirrored now in cyberspace, as well as the proxy wars that may suddenly break out in cyberspace. Indeed, the need to maintain technological supremacy was an overriding concern both then and now. To be sure, there are obvious differences. The Cold War was a bipolar, ideologically motivated struggle and the fear of mutual assured destruction moderated the behavior between the two major actors. However, the Cold War is an analogy that can educate the present, precisely in the manner that an international response to curbing the spread and use of nuclear weapons was pursued throughout the conflict.

The most important lesson from the Cold War is the need to prepare for the eventual conflict in cyberspace, define the boundary conditions for these conflicts, and create an international framework for preventing escalation. As well, open debate and academic research must be conducted in order to properly frame national interests with all possible repercussions in mind. The state needs to answer serious questions, such as: "Will cyber deterrence work? Should there be an international treaty on the use of cyber weapons? What is the line between espionage

[49] [49] *Ibid,* p.143

and warfare in cyberspace?".[50] Currently, other states are taking the lead in defining the boundaries of cyber warfare.

An Emerging International Consensus

There are over 120 countries actively creating offensive cyber weapon capabilities.[51] These capabilities have been put into use on numerous occasions which is gradually resulting in the development of an international consensus on the usage of cyber weapons. While cyber weapons are being developed by dozens of countries, this paper will focus on China, Russia, and the US. These countries are the most active actors in the cyber realm and based on their actions an international consensus on cyber weapons usage has emerged.

China

The Green Army—a self-proclaimed hacker organization with 3,000 members from all over China—emerged on the scene in 1997. This loose confederation of Chinese hackers is now notorious for orchestrating the first cyber attack on a state government in 1998. Riots struck Jakarta, Indonesia as Indonesian citizens blamed the People's Republic of China (PRC) for their own out of control inflation. Indonesian Chinese nationals were the targeted and a massacre ensued. A virtual Chinese Hacker's Emergency Conference was called to address the situation, and the retaliation that ensued was a military-style campaign attacking Indonesian government websites.[52] While the Green Army was eventually disbanded in 2000 due to financial troubles, its actions awoke the Chinese government to the concept of "Comprehensive National Power",

[50] McAfee Inc., Virtually Here: The Age of Cyber Warfare (Virtual Criminology Report 2009), [available online] http://www.projectcyw-d.org/resources/items/show/129 p.24
[51] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", p. 201
[52] Jorge Muniz Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College (2009), [available online] http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA502899 p. 6

where both military and civilians' roles are integrated and act on behalf of the state.[53] Since this point, many Chinese hacker organizations have gladly filled the role of national protector and use cyber operations to defend China. These include a cyber attack on the US in 1999 following the accidental bombing of the Chinese embassy in Belgrade and a week-long attack on US government websites in 2001 following the mid-air collision of a US EP-3 and a Chinese AN-124.[54] To date, however, it has been impossible to identify whether these attacks were, in fact, sponsored by the Chinese state, whether they were the work of lone organizations in China acting unilaterally, or the actions of a different entity entirely that used Chinese networks to disguise their identity. Yet, due to the sophistication of the Chinese control and monitoring of its own internet system, it is possible to infer that the Chinese government was aware of the perpetrators activities and probably provided mechanisms for them to achieve their goals. This assumption is reinforced by the literature available from the Chinese government on its views towards cyber warfare.

An important window into Chinese military thinking on cyber warfare has been the publication of *Unrestricted Warfare* (超限战, literally "warfare beyond bounds") .[55] This book was published by the People's Liberation Army (PLA) Literature and Arts Publishing House in Beijing, which suggests it was endorsed by some elements of the PLA leadership.[56] An interview with one of the authors and a glowing review of the book in the party youth league's official

[53] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers* (Library of Congress, 2007) p. 103
[54] Jorge Muniz Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College, 7
[55] Jorge Muniz Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College, p.16
[56] Liang, Qiao and Xiangsui, Wand, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February, 1999) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7179&rep=rep1&type=pdf

daily Zhongguo Qingnian Bao have reinforced this perception.[57] Essentially, it is a document that "proposes tactics for developing countries, in particular China, to compensate for their military inferiority vis-a-vis the United States during a high-tech war".[58] It was written by two senior colonels in response to the US Gulf War, which demonstrated the full power of smart bombs and the ability for the US to utterly dominate a conflict with its superior fire power. According to the authors, China can overcome the US in a conflict through "total warfare", which includes technology warfare and network warfare. It would be impossible for China to win in a force-on-force conflict that incorporates "satellite reconnaissance, electronic countermeasures, large-scale air attack plus precision attacks, ground outflanking, amphibious landings, [and] air drops behind enemy lines".[59] Rather, "total warfare" would include trans-military and non-military capabilities. The authors suggest that:

> If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis.[60]

The first rule of "total warfare" is that there are no rules and no action is forbidden.[61] The electronic Judgement Day described above is subject to a fair amount of hyperbole and is reminiscent of the incorrect predictions nuclear strategist made about the effectiveness of first strike bombings to knock out an opponent's ability to retaliate. However, what is clear is that in

---

[57] *Ibid*
[58] *Ibid*
[59] *Ibid,* p. 34-31
[60] Liang, Qiao and Xiangsui, Wand, *Unrestricted Warfare* p. 40
[61] *Ibid,* p. 1

their theory of "total warfare", the cyber warrior is on the front lines of any conflict and is an essential component of any viable strategy to be used against the US.

Another high ranking proponent of pre-emptive cyber attacks is Major General Dai Qingmin, who has published his views in a number of Chinese periodicals and compilation books. In his essay in "Research on Information Warfare Issues in Our Military", Dai believes that battlefields have been transformed by their reliance on cyber space, which will result in new types of combat such as "hacker warfare, network warfare, and computer virus warfare".[62] In the new information age, there is a "fusing and sharing of military and commercial information facilities and technologies [so that] the boundaries between military, non-military, global and battlefield information environment will gradually become ambiguous".[63] Battle will be won by attacking the information systems of units on the field, as well as disrupting the cyber systems of a home country. Dai builds upon these views a year later in his work "Innovating and Developing Views on Information Operations", where he outlined 10 cyber strategies to be used to gain superiority in this new realm: "plant information mines, conduct information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information, organizing information defense, and establishing network spy stations".[64] One of these efforts (establishing network spy stations) has already been uncovered in the highly published and blatant Chinese cyber spying network called GhostNet.

---

[62] Jorge Muniz Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College, p.18

[63] Qingmin Dai "Flexibly Utilization of Battlefield Information Environments, to Gain Advantageous Positions in Combat, through the use of Information Conditions": submitted for inclusion in Peng Chencang‟s book, "Efforts to Explore Information Warfare Theory Applicable to our Armed Force's", (Beijing, AMS, 01 Jan 1999), p 40.

[64] Jorge Muniz Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College, p. 19

GhostNet is a network of compromised computers located within high-value political, economic, and media networks in a variety of countries.[65] Until it was uncovered, the computers of "diplomats, military attachés, private assistants, secretaries to Prime Ministers, journalists and others [were] under the concealed control of unknown assailants".[66] The infected computers had documents stolen, keystrokes logged, web cameras silently turned on, and audio inputs opened. The researchers that uncovered this network are quick to point out that directly attributing the network to China is difficult. However, they do conclude that the circumstantial evidence clearly points to the Chinese state. Many of the targets are linked to the Chinese military and foreign policy, while the IP addresses of the controlling computer has been traced back to Hainan Island, home of the Lingshui signals intelligence facility.[67] The significance of this network is that it demonstrates that layers of cyber space are being infiltrated clandestinely for reconnaissance, surveillance, and exploitation purposes.

Both the deeds and words of the Chinese state indicate that they have fully realized the strategic significance that domination of cyber space can have for emerging powers. As Qiao, the author of *Unrestricted Warfare*, states,

> Strong countries would not use the same approach against weak countries because strong countries make the rules, while rising ones break them and exploit loopholes… The United States breaks [UN rules] and makes new ones when these rules don't suit [its purposes], but it has to observe its own rules or the whole world will not trust it.[68]

China has taken the lead in defining the new boundaries of cyber space conflict and has fully incorporated it into their strategic doctrines. Recently, the *China Youth Daily* published an article

---

[65] Information War Monitor, *Tracing GhostNet*, March 29 2009, (SecDev Group, Munk Centre for International Studies) [online] available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
[66] *Ibid*, p.47
[67] *Ibid*, p. 48
[68] Liang, Qiao and Xiangsui, Wand, *Unrestricted Warfare*, p. 1

explaining why China might be forced to fight a cyber war in the future[69]. This because the US has been antagonizing Chine by providing tools and support to dissidents within China to break through the government's firewall. Through these actions, they are creating international norms about the acceptability of using cyber weapons during peace time to gain strategic advantage. Unlike the international norms surrounding nuclear weapons that were created through public debate and academic research, the norms surrounding cyber space conflict are being created by national militaries and foreign intelligence agencies. Moreover, through their words they have crafted a strategy for utilizing cyber space to facilitate their rise to great power status. China has clearly incorporated cyber space dominance into its grand strategy for national security. The most dangerous aspect about this consensus on the acceptability of using cyber space for war that is emerging within China, is that it is happening in an international environment that lacks a clear definition of what constitutes an attack in cyber space, as well as a lack of international agreement on the full repercussions of what a cyber conflict could entail. These international standards cannot be dictated, but need to grow organically from open dialogue, international summits, and collaborative academic work from international epistemic communities. What exists now is simply an understanding from many states that the future of conflict will involve attacks over cyber networks. Without standards and boundaries, however, these beliefs will not foster international security in a cyber age. As China's stance becomes more clear, so should an international response.

Russia

[69] Adam Segal, "Strategies for Engaging China in Cyber Space", at *Council of Foreign Relations* [available online – June 16, 2011] http://blogs.cfr.org/asia/2011/06/16/strategies-for-engaging-china-in-cyberspace/

For a closed society, China has been very open about its cyber war development. Russia, on the other hand, is considered a much bigger threat to cyber space, as little is truly known about their full capacities. US intelligence officials believe that "the Russians are definitely better, almost as good as we are".[70] Russia has taken a much different stance towards cyber warfare than the US or China. They have allowed criminal and hackivist (which are hackers motivated by nationalistic or ideological concerns) organizations to supply the state's cyber offensive capabilities, while tacitly sanctioning their behaviour and restricting international intervention to curb their activities. Publically, Russia has been pressuring for international treaties surrounding cyber space; yet privately, the Russian state sanctions criminal and nationalist hackers, while engaging in international cyber offenses. To date, their rhetoric internationally has been focused on different priorities than the US and its allies. Rather than focus on cyber security or cyber warfare, Russian policy makers use the terms "information security" and "information warfare".[71] To the Russians, these terms have broader philosophical and political implications; "information security" means protecting Russian culture and knowledge and guaranteeing the free flow of information, while "information warfare" is the use of foreign propaganda (i.e. rhetoric on human rights) and using cyber tools to undermine the legitimacy of the state.[72] Domestic and international critics challenge this last goal, claiming that improving "information security" is actually a veiled attempt to improve the Kremlin's ability to silence dissidents and protect their cyber criminals.

---

[70] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p 63

[71] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors,* (EastWest Institute, 2010 [available online] www.ewi.info.com p. 5

[72] *Ibid,* p. 5

The branch of government that handles Russia's cyber capabilities is the Federal Commission for Government Communications and Information, or FAPSI, a former division of the KGB.[73] While the KGB collapsed along with the Soviet Union, FAPSI merely relocated and changed its name to the Service of Special Communications and Information. To US intelligence officials, it is simply known as "Moscow's NSA".[74] Much like America's NSA, this department was formed to create code, break encryptions, intercept communications, and other forms of signals intelligence. When the internet was first introduced into Russia, the FAPSI quickly began asserting its dominance over this new space. It took over the largest ISP in Russia and began requiring all Russian ISPs to install monitoring systems that only FAPSI could use. Today, the FAPSI runs one of the largest and best hacker schools in the world, which specializes in producing world class cyber warriors.[75]

Russia is renowned as a haven for cyber criminals and hackers. In a country that actively harasses publications it deems unacceptable, *Xaker: Comupter Hooligan* magazine thrives and cyber crime is tacitly encouraged.[76] Many of the recent cyber attacks on other states that have been accredited to Russia appear political. These include the attacks on Estonia in 2007, as well as attacks on Georgia and Lithuania.[77] When the Russia-Georgia conflict turned into a war in 2008, software became available on the internet that allowed anyone to conduct cyber attacks on the Georgian capital. Later that year, Lithuania was subject to a similar cyber attack when it

---

[73] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p 83
[74] *Ibid*, p. 83
[75] *Ibid*, p. 64
[76] Khatuna Mshvidobadze, "Analysis: Is Russia on the wrong side of the net?", in *Jane's Defence Weekly*, Feburary 28, 2011 (HIS Global Limited, 2011)
[77] Newsweek, "The Evil (Cyber) Empire: Inside the World of Russian Hackers", December 20, 2009 [available online] http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html

vetoed negotiations between the EU and Russia at an EU Summit.[78] Experts on Russia believe that the country still views its security in terms of geography, spheres of influence, and realpolitik.[79] The Russian security policy elitists view the source of their vulnerability arising from adjacent regions and, similar to during the Cold War, seeks to dominate their activities.[80] In the current cyber age, this is being achieved through a compromise between Russian organized crime and the Kremlin—Russian authorities will turn a blind eye to organized criminal activities if they will engage in politically motivated cyber attacks when needed. Indeed, Russian authorities have vehemently denied all of these allegations. NATO conducted an investigation into the attacks on Georgia and concluded, "Although there is no conclusive evidence that the cyber attacks in Georgia were executed or sanctioned by the Russian government, there is no evidence that it tried to stop them, either".[81]

Yet, at the same time, Russia has been advocating for an international regime to limit the spread of cyber weapons and envisions a convention that would ban the development and usage of military information technologies.[82] They believe this is in their national interest due to their perceived inferiority in communications technology.[83] A recent report on Russian critical infrastructures explained that their rationale for pursuing this policy is national interest:

> Russia's international cooperation in ensuring information security has two distinctive features: International competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allows them to build up their potential for information warfare. Russia views this development with

[78] Newsweek, "The Evil (Cyber) Empire: Inside the World of Russian Hackers", December 20, 2009 [available online] http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html
[79] Oksana Antonenko and Bastian Giegerich "Rebooting NATO-Russian Relations", in *Survival*, Vol. 51, No. 2 (2009) .p 15
[80] *Ibid*,.p 15
[81] Newsweek, "The Evil (Cyber) Empire: Inside the World of Russian Hackers", December 20, 2009
[82] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors*, (EastWest Institute, 2010 [available online] www.ewi.info.com p. 6
[83] *Ibid*

> concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure.[84]

According to Russian statements, this would address the threat of a "cyber arms race" and create international definitions for aggression in cyber space and cyber weapons.[85] To advance this agenda, Russia chaired a UN working group of experts on cyber security in 2003 and played a similar leading role on expert groups up to 2010. Perhaps more importantly, it created a partnership on information security called the Shanghai Cooperation Organization.

However, all of these international efforts appear to simply be an effort to deter criticism and deflect attention away from their actual behaviour. The Signatories of the Shanghai Cooperation Organization (SCO) is a who's-who of human rights violators—China , Kazakhstan, Krygyzstan, Russia, Tajiistan, and Uzbekistan—and is simply an agreement to justify sovereign controls on the internet.[86] The debate about whether the internet should have sovereign boundaries or should be an open commons is the main obstacle to US and Russian cooperation on international treaties on cyber space. Moreover, the events in Estonia and Georgia highlight another problem with international collaboration on cyber space—how to identify the source of the attack and inspect a cyber arsenal to ensure all parties are keeping their end of the agreement. Russia wishes to promote a weapons-free internet publically, but is aware that erecting national borders in cyber space will allow them to continue their support of non-state, criminal hackers.

By piecing together strategic documents, official statements, and pronouncements on cyber criminals with Kremlin ties, a picture of Russia's cyber doctrine can be created. It includes:

---

[84] A. A. Streltsov, *Gosudarstvennaya informatsionnaya politika: osnovy teorii*, State Information Policy: The Basis of the Theory, (Moscow, 2010), p. 345

[85] *Ibid* p. 6

[86] The Economist, *The Future of the Internet*, Sept. 2nd, 2010 [online] available from http://www.economist.com/node/16941635

"monitoring people's activity on the internet, protecting the people from 'harmful' foreign information, spreading Russian propaganda, defending Russia's information assets, partaking in espionage and attacking enemy information systems and critical infrastructure."[87] Indeed, Russia is sending conflicting messages about its cyber weapons policy and may be routinely engaging in cyber attacks on the security structure of others.[88] Russia is maintaining a strong defensive-posture in cyber space. Consistent with their world view, cyber space is another tool to be used in their brand of realpolitik in their sphere of influence. Their behaviour is consistent with the emerging international consensus that cyber weapons are a legitimate tool of foreign policy and can be utilized during limited conflicts. But, as technology advances and as the two countries continue to develop close ties over nuclear reduction agreements, Russia and the US might begin to see their interests intersect. Russia has demonstrated a willingness to take a lead on creating international cyber weapons treaties and recognizes that a cyber arms race is not in their national interest. Despite Russia's past behaviour, the White House and the Kremlin should view each other as potential allies in cyber space. However, until the latter ceases to use cyber criminals to carry out political goals and as long as attribution of cyber attacks remains a problem, no treaty on cyber space will be effective.

United States

Policy thinking on cyber security in the United States has taken many forms. A central element to cyberspace policy making was the belief that the role of government in this new

[87] Khatuna Mshvidobadze, "Analysis: Is Russia on the wrong side of the net?", in *Jane's Defence Weekly*, Feburary 28, 2011 (HIS Global Limited, 2011)
[88] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors*, (EastWest Institute, 2010)

domain should be minimal.[89] The senior policy advisor for policy development under President Clinton, Ira Magaziner, believed that "the first principle is that this will be an environment or a world where private actors lead, not governments."[90] The tool of choice for President Clinton was law enforcement agencies, such as the FBI, and this directive created the National Infrastructure Protection Centre, which persisted until 2007. The changing nature of cyberspace quickly outpaced the ability of the NIPC to properly function and cyber warfare was quickly gaining headlines and policy attention.

President Bush therefore revised the US' strategy with the publication of The National Strategy to Secure Cyberspace in 2003 (NSSC03) and the Comprehensive National Cyber Security Initiative in 2007. NSSC03 repeatedly stresses that the goal of the US is to deter cyber attacks and will respond appropriately to any acts of cyber aggression. It states that "when a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner".[91] Both of these documents discuss efforts to deter cyber attacks, with mention of the techniques to achieve deterrence residuals as well as an embryonic full-blown deterrence strategy. Pieces of a US cyber deterrence strategy emerged within these two documents; however it was fragmentary and unresolved. Within the 2007 document, for one, the term cyber warfare was introduced alongside a repetition of the US strategy for deterrence. However, most of the references to cyber war concerned securing the cyber realm with only

[89] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace", in *Brown Journal of World Affairs*, Vol. 16, Issue. 2 (Spring/Summer, 2010 p. 55- 65), p. 55
[90] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace", in *Brown Journal of World Affairs*, p. 55
[91] Callaghan, John P.; Kauffman, Rudi. Building Cyber-Security: The Prospects of Deterrence. Conference Papers -- Midwestern Political Science Association; 2008 Annual Meeting, p. 8

passing reference to where the threats in cyber space will come from and how they could actually be deterred.[92]

The Obama administration has since worked diligently to secure cyber space. It conducted a 60-day Cyberspace Policy Review and created the unified Cyber Command at the Department of National Defense which is "responsible for addressing the growing array of cyber threats and vulnerabilities…. and to secure freedom of action in cyberspace".[93] The first US Cybercom Commander was appointed in May 2010, with a press release stating his objectives:

> The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the DoD information security environment.[94]

Placing the new Cyber Comm in DND will allow cyber security to be viewed through a more military focused lens. Yet, the new head, Lt. Gen. Keith Alexander was the Director of the NSA. This demonstrates that there is still tension between the national security concerns and the public/private dynamic in the US' thinking towards cyber security. National security cannot be achieved in cyber space without working extensively with private firms, citizens, all government departments, the military, and other states. The US has fully acknowledged the extent of the problem and has promised heavy investment and the creation of new agencies.

The two main branches of government dealing with cyber issues are intelligence agencies and national defense. Law enforcement agencies only play a small role in the US cyber security policy approach as the threat of persecution is not a deterrent to state-sponsored cyber espionage. This heavy reliance on intelligence and defense agencies to provide security in cyber space is reminiscent of the Cold War era, and suggests that the Cold War analogy for the current cyber

---

[92] Callaghan, John P.; Kauffman, Rudi. Building Cyber-Security: The Prospects of Deterrence. Conference Papers -- Midwestern Political Science Association; 2008 Annual Meeting, p. 8
[93] *Ibid*, p. 10
[94] *Ibid*, p. 60

age is apt. Diplomatic international engagements on cyber norms, on the other hand, is the least developed aspect of US policy.[95] There has been little effort for the US to work with its perceived adversaries on creating acceptable boundaries and rules of engagement for cyberspace. This is due to the fact that these other countries have fundamentally different cultural norms on democratic values, such as free speech, human rights, and privacy issues. The US is opposed to any effort that would create borders in cyberspace or enshrine the norm that a state has sovereignty over the cyber systems within its country. Rightly so, the US is highly skeptical of Russian overtures for international treaties on cyberspace because they believe these proposals will provide cover to totalitarian regimes to censor the internet.[96]

On May 16th 2011, the Obama administration published its *International Strategy for Cyberspace,* which is an overarching statement to guide government bodies and define the administration's objectives. The US will work to enhance security, while ensuring a space for economic activity and protecting the freedom of users. The recent political events of the Arab Spring are praised in the strategy, which the Egyptian government's move to shut its citizens off from the internet to quell the dissent is condemned. The US guarantees to protect internet access to all people and support groups within countries that face a censored or restricted internet connection. Moreover, the document outlines the US's deterrence strategy. It states that the US reserves the right to protect its nation and will respond to any cyber attack as an attack on its national security. The document, however, fails to address three key questions: what constitutes an attack of cyber warfare, when would a military response be appropriate, and what are the rules

---

[95] James A. Lewis, "Securing Cyber Space for the 44th President", *A Report on the CSIS Commission on Cyber security for the 44th President,* (2008), [available online] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf p. 23

[96] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors,* (EastWest Institute, 2010)p. 8

of engagement.[97] This lack of clarity has already led to confusion in the application of the strategy in light of recent events.

On June 2nd, Chinese hackers broke into the gmail accounts of White House employees looking for government information.[98] While the US stated it would respond to attacks with force, it is unclear if this attack meets the governments criteria for warranting an attack, nor is it clear what would. Furthermore, the US states in the strategy that it "reserved the right to use all necessary means—diplomatic informational, military, and economic—…in order to defend our Nation".[99] Indeed, this indicates that the US is prepared to use all instruments of statecraft to defend its security; however the document fails to outline details of such a grand strategy. The *International Strategy for Cyberspace* is full of overarching statements on the need for securing cyberspace, however it does not address cyber weapons, indicate the boundaries of a cyber attack, or outline how it will protect civilians in a cyber conflict.

Overview

This section has outlined the emerging views on cyber warfare between the three largest adversaries in this realm. Indeed, there are several intersecting themes that are similar between the US, China and Russia. First, there is an emphasis on the role of intelligence agencies and militaries in cyber space and each country has delegated all authority for cyber space operations to these agencies. Thus, each state is taking a strong defensive posture towards cyber security. This is because each state's actions are unknown to one another, creating a type of prisoner's dilemma. Co-operation would benefit each party more than cheating, however it is impossible to

---

[97] Editorial, "A U.S. strategy for fighting cyberattacks", in *Los Angeles Times*, June 3 2011, [available online] http://www.latimes.com/news/opinion/opinionla/la-ed-google-20110603,0,5087778.story

[98] Zapler, Mike, "FBI Investigates Gmail Hack", in *Politico*, June 2 2011 [available online] http://www.politico.com/news/stories/0611/56103.html

[99] White House, *International Strategy for Cyberspace*, May 2011 [available online] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

guarantee cooperation or know if the other party is cheating. Therefore, rather than co-operate, states are clandestinely probing and infiltrating one another's systems to the detriment of each party. Second, each state has openly recognized the devastating impact that cyber weapons can have on a society and have begun to build cyber offensive capabilities. China's view is that the internet will provide it with asymmetric power capabilities to undermine the US' military dominance. Russia views the internet as a key tool to be used in military operations and ensuring its ability to influence periphery states. The US has recognized that the internet is a possible Achilles' heel and there needs to be proactive safeguards to prevent attack. The introduction of cyber weapons is offsetting traditional calculations of power capabilities and allowing states to quickly achieve parity, where they were previously thought to be decades away. Third, there has been an inability to reconcile state identities with a common understanding of what the identity of the internet should be. Authoritarian and illiberal democracies wish to create borders within cyber space to censor internal dissidents and infringe on free speech. The US, on the other hand, believes that the internet should be open to all and free from sovereign influence. This is setting the stage for a future international confrontation, especially since cyber space has been articulated as intrinsically linked to state security.

The battle lines have been drawn in the current cyber age. The world is witnessing the beginnings of an ideological battle over the future form and shape of the internet. Moreover, states are aggressively producing cyber weapons that can have societal wide impacts and re-shape the international balance of power. As states vie for mastery of the internet, tensions are rising and conflict looms on the horizon. If states refuse to reassess their strategic doctrines and neglect the impact that cyber weapons will have on international security, this conflict will become inevitable.

Foreign Policy and the Way Forward

A successful international response must incorporate many elements and use all of the instruments of statecraft. This section will outline recommendations for international agreements on cyber weapons. Ultimately, these recommendations to address cyber threats will be based on a sound deterrence strategy and engaged multi-literalism and diplomacy. Achieving this will demand the courage to be a leader for the international community.

Diplomacy

The diplomatic efforts of states should focus on the creation of an arms control treaty for cyber space. The experiences during the Cold War have taught many lessons for future statesmen about the potential successes and pitfalls of such treaties. When arms control is successful, it is capable of reducing uncertainty and can create a more stable and predictable international environment. By classifying some actions as illegal and others as legitimate, arms control negotiations can establish what another state's intentions may be. However, arms control treaties are not valuable when they are "largely hortatory, or when negotiation is seen as an end in itself or a platform for propaganda, when its limitations are vague and also when violations are without cost to the violator".[100] If a state is capable of moving from compliance to violation with no warning time, then the qualities of stability and predictability are lost.[101] Creating arms control treaties for cyber weapons faces all of these problems. For example, Russia's suggestions for an international treaty are largely for propaganda's sake. Their proposals go as far as banning cyber espionage, which is, in fact, neither a desirable nor reasonable end state for them. They propose

[100] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p 225
[101] *Ibid*, p. 225

stopping something that they really want to keep around and the proposal is a deceptive means of attempting to constraining their adversaries in an area they feel they might be outclassed.[102] Moreover, inspection and verification of compliance are impossible and, even when states are in compliance, they are capable of violating the terms of the treaty in seconds and without warning. Therefore, unlike other arms treaties that destroy weapons, a cyber weapons treaty could not ban capabilities and would be more successful at focusing on constraining actions.

Espionage was an effective tool of statecraft during the Cold War and will continue to play a prominent role in any state strategy, Banning cyber espionage would hurt a state's national interest, be nearly impossible, and it is extremely doubtful that other states would stop their cyber espionage activities. It is, however, important to proceed with caution as cyber espionage can have detrimental effects. A former NSA director said that states "are conducting warfare activities without thinking that it is war".[103] This can be dangerous, harmful to diplomacy, and have potentially destabilizing consequences. Without an understanding of mutually agreed upon boundaries, countries could be engaging in provocative actions that could destabilize the entire international system. However, there are other ways to address these concerns that do not require banning the activity all together.

Rather, the experience from the Cold War provides possible alternative ways to moderate behaviour in cyber espionage. During the Cold War, the CIA and KGB met secretly and agreed upon rules of behaviour, such as an agreement to not assassinate one another's agents.[104] This could be done between intelligence agencies working on cyber space. The intelligence agencies of the major powers could meet and create some quiet understandings of acceptable rules of

[102] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p. 225
[103] *Ibid*, p. 236
[104] *Ibid*, p. 236

conduct in cyber space. Indeed, the real threat to societies in not infiltration of government networks, but in critical infrastructures. The recent case of the Stuxnet virus, where a government-created virus sabotaged a nuclear plant in Iran, would be in clear violation of acceptable rules of conduct outside cyber space. If the US was caught planting an agent in Iran for the purpose of sabotaging a nuclear power plant, and risking a possible explosion, it would lead to an international outcry. The anonymity that the internet provides should not become a reason to act recklessly.

Governments claim that they do not know the identity of those who attack or infiltrate their systems. They are capable of tracing the IP address of an attacker to a country, however hackers can use computers as proxy relay points. An attack from a Chinese IP address could really be a hacker in Africa using a Chinese computer to stage the attack. If they are not able to further investigate within that country the trail goes cold. This allows hackers to carry "false flags" and disguise their nationality. Mechanisms need to be put in place to allow citizens to rely on their governments to investigate attacks and for governments to demand of each other to investigate when attacks arise from within their borders. In circumstances in which evidence of the source of an attack is deemed sufficiently reliable but not substantive enough to justify military retaliation, states can use other forms of retaliation. Tactics such as "reputational damage to an attacker's soft power may contribute to deterrence".[105]

Creating international norms takes time and requires a starting point of shared interests. In order to determine the success of an arms control treaty, it is important to first determine if all parties have an interest in limiting their own investments in the area. Chinese, US, and Russian

[105] Joseph Nye, "Power and National Security in Cyberspace", in *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011)

doctrines all insist that net-centric warfare and cyber weapons are an integral part of their military capabilities. Therefore, a full-out ban of using cyber weapons in military campaigns is against the interest of all parties involved. However, banning cyber attacks on civilians, especially if the focus is initially placed on banks, could be considered an area where all parties have an interest in limiting their development. Virtually every state has an interest in maintaining a stable financial system. Therefore, a central aspect of a state's diplomatic efforts should be the creation of a Cyber War Limitations Treaty (CWLT) that would ban attacks on the international financial sector and civilian networks.[106] This would not ban the actions of national intelligence agencies, nor would it ban their usage in conventional military operations. It would, however, begin to formulate an international understanding of what constitutes a cyber attack. Therefore, international treaties that deal with cyber weapons need to also include cyber espionage capabilities. It would be counter-productive to exert efforts trying to ban the activity without any idea of how to detect or prevent it. As well, a central aspect of this treaty should also be to place the burden of responsibility for criminal acts originating from a state on the state itself. Russia and China should no longer be considered a safe haven for cyber criminals and they should be held responsible for the criminal activities of their citizens on foreign states. While this treaty would be a substantial accomplishment, it would still be possible for cyber attacks to occur against a state's citizenry, and should therefore not replace the need to take defensive steps to protect infrastructure or lead states to ignore other aspects of a full strategy.

To date, there is no publically agreed upon consensus of the proper application of cyber weapons and cyber warfare. Rather, international norms on cyber weapons are emerging through

[106] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p p. 261

state action, without open debate or public consultation. Indeed, this emerging consensus is happening without common understanding on what constitutes a state-sponsored attack. Stable international security requires an understanding to exist between states. The recent British offers to host an international conference on norms in cyber space are a good beginning, but more needs to be done to include academics, the private-sector, and the public.[107] There exist pertinent lessons from the Cold War to be followed.

In the nascent stages of the Cold War, international norms surrounding the usage of nuclear weapons did not exist. There existed many "hawks" in the US and Russian militaries that endorsed striking quickly with nuclear weapons to forestall a greater conflict. These considerations were being calculated without proper research into the effects of a nuclear war. In fact, military leaders believed that nuclear war was too important and too close to national security to be discussed publically. This led academics on national security issues to begin investigating the repercussions of nuclear war. In response to this, Herman Kahn wrote *Thinking about the Unthinkable* (1962), which contributed to a public debate about the moral, ethical and strategic aspects of nuclear war. This was built upon thorough open research and writing by academics on the topic.[108] Furthermore, international conferences between academics from both Russian and US epistemic communities lead to a dispersion of common understandings about the fallout of nuclear weapons. Through the meeting of these epistemic communities internationally and the public debates that they generated domestically, norms were created that helped to moderate behaviour on the usage of nuclear weapons. Because of their work and the ensuing

[107] Foreign & Commonwealth Office, "Security and Freedom in the cyber age – seeking the rules of the road" (2011) [available online] http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682

[108] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p. 200

public debate, military doctrine had to move beyond its original focus of first-strike and tactical use of nuclear weapons, to second strike and deterrence capabilities.

Currently, no major policy school—such as Havard's Kennedy School, Princeton's Woodrow Wilson School, University of Toronto's Munk Centre, or University of Ottawa's Graduate School of Public and International Affairs—have any courses on cyber space policy or strategy.[109] There have also been relatively few books dedicated to the subject. This might partly be due to the fact that much of the material is secret and new. Regardless, this needs to change. According to a prominent cyber critic, Richard Clarke, the lack of a clear strategic doctrine coming from academia for the cyber age is a major problem:

> In the 1950s to 1960s, civilians—many of them outside of the government—came up with a complex strategy for the use of nuclear weapons. This strategy was then debated publicly and later incorporated into national policy. Today, planning for cyber war is at a similar stage. For example, the U.S. has a cyber command, but there hasn't been a public discussion about when and how cyber weapons should be used. There hasn't been an academic discussion either. Computer scientists and international relations experts are not talking to each other right now.[110]

There needs to be a public debate and governments need to address some serious deficiencies in its strategic cyber doctrine. Currently, other states that do not align with western beliefs on human rights, privacy, and rule of law are taking the lead in defining the boundaries of cyber warfare.

Therefore, the debate about cyber warfare needs to be brought into the international public domain. This can be accomplished by funding courses and degrees on cyber security issues at universities and schools of public policy. Academics should be encouraged to write more on this topic and to attend international conferences that bring together academics from all

---

[109] *Ibid*, p. 261

[110] Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010), p. 24

the possible belligerents in cyber space. Furthermore, states should fund training programs and career paths for federal cyber security employees. Students of national security that wish to focus on cyber security issues have few career paths or training courses available. Governments should fund and encourage more international conferences, bringing together government officials and academics, to look strategically at cyber warfare and understand the fallout of a cyber war.

Military Instruments

International efforts to create arms control treaties, define the limits of espionage, and foster the growth of stable international norms must be supported by strong military capabilities that can defend national security. This demands a strong deterrence strategy, which can be created by enacting strong, proactive defense capabilities, as well as building an offensive cyber strategy. During the Cold War, deterrence was a more nuanced doctrine than mass retaliation, and while it prevented attacks on the homeland, "it was never credible for issues at the low end of the spectrum of interests".[111] Extended deterrence dealt with attacks against allies and defense of points of interests, such as the Berlin Wall. Mass retaliation doctrine was complimented with more traditional measures, such as forward basing of forces. Ultimately, deterrence embodied a learning process that spanned the Cold War and led to many areas of agreement. Deterrence began with an acknowledgement that the adversaries would not attack each other's homeland and culminated with the declaration by Regean and Gorbachev that "a nuclear war cannot be won and must never be fought".[112]

Militaries can protect their nation from cyber attacks in other ways. One way is for the public sector to become a model for the private sector in purchasing security software. This

[111] Joseph Nye, "Power and National Security in Cyberspace", in *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011)
[112] *Ibid*

would include setting internal standards for what secure software should be and sharing these with the private sector. This will help to inform the private sector about specific security needs that should be addressed by any security measures, as well as setting a high standard for them to base their own systems upon. Furthermore, deterrence can be achieved through denial. If a firewall is strong enough or there is a prospect "for self-enforcing responses (an electric fence)" then attacks will be less attractive.[113] Active defenses could be offensive responses that activate once a firewall has been breached and would be capable of deterring even when the infiltrator's identity is hidden. As well, deterrence can be achieved through and resilience. If cyber systems are well-protected, or resilient enough to allow for quick recovery, the benefit/risk ratio of an attack diminishes.[114] Another defensive measure that can be employed is to issue statements that let the world know about acceptable boundaries for action in cyber space. Defense Secretary Robert Gates has recently argued that international tensions could be avoided "if we could establish some rules of the road as early as possible to let people know what kinds of attacks are acceptable, what kinds of acts are not and what kinds of acts may in fact be acts of war".[115] This would entail the creation of a more comprehensive deterrent strategy than has recently been articulated. In creating a deterrent strategy, a nation must choose an acceptable level of belligerent aggression and clearly signal that exceeding this threshold will result in retaliation.[116] Again, the Cold War can serve as an appropriate example of how to signal the appropriate boundaries in cyber space. For example,

---

[113] Joseph Nye, "Power and National Security in Cyberspace", in *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011)
[114] *Ibid*
[115] International Business Times, "US can use force to respond to cyber-attacks: Robert Gates", June 4, 2011 [available online] http://uk.ibtimes.com/articles/157368/20110604/u-s-cyber-space-pentagon-robert-agtes-defence-hackers-accounts.htm
[116] Callaghan, John P.; Kauffman, Rudi. Building Cyber-Security: The Prospects of Deterrence. Conference Papers -- Midwestern Political Science Association; 2008 Annual Meeting, p1-13, 13p, 1

> consider the early efforts to define appropriate thresholds for the use of nuclear weapons. Whether the targeting of metropolitan areas to end the Second World War, lifting the blockade of Berlin in 1948-1949, the wars in Korea and Vietnam, or the Cuban missile crisis, nations made decisions about the deployment of nuclear weapons that signaled where the nuclear threshold stood.[117]

Sending signals to other nations about the acceptable boundaries of cyber conflicts is vital to any deterrent strategy. The mechanisms of creating these signals and sending the right perceptions of their capabilities to adversaries are vital for the deterrence to work. While successful cyber security initiatives will start at the domestic level, the nature of cyber threats demands a coordinated and comprehensive approach. The "cyber threat spectrum that needs to be covered on the international level is significantly wider than any one nation's immediate concerns".[118]

Conclusion

Cyber space is a new and unstable domain. Its characteristics have reduced power disparities and diffused power to many smaller states and non-state actors. Diffusion, however, does not equal an erosion or elimination of power. States are still required to play a central role in maintaining security and their leadership is needed even more for cyber space. The US may be more vulnerable to attacks from smaller nations, but traditional power capabilities still exist and the US maintains substantial hard and soft power. Cyber weapons, from rogue nations or non-state criminal actors, threaten all states and pose a risk to international security.

Starting to address cyber weapons cannot begin with over-arching international treaties that ban cyber war or ambitious arms control treaties. Rather, it must begin with common areas of interest that can be easily agreed upon. These will include treaties that limit attacks on the

[117] Callaghan, John P.; Kauffman, Rudi. Building Cyber-Security: The Prospects of Deterrence. Conference Papers -- Midwestern Political Science Association; 2008 Annual Meeting, p1-13, 13p, 1
[118] *ibid*

infrastructure of the internet and the financial sector. Regardless of normative beliefs, all major states have a stake in maintaining these systems. From there, through repeated interactions and socialization of behaviour, more ambitious and comprehensive treaties will form. In the mean time, states need to create comprehensive deterrence strategies that send clear signals of boundaries and proportionality. The US' experience with the Cold War is an excellent model to provide a base for negotiations on cyber weapons. Cyber weapons and nuclear weapons share many similarities and can educate policy makers through the lessons learned during the Cold War.

The world needs leadership on cyber space in order to ensure international peace remains stable. The emergence of cyber weapons has sharpened geopolitical rivalries and threatens to de-stabilize the international system. Incidences of reckless cyber aggression have been multiplying in recent years and an international cyber arms race looms on the horizon. Almost weekly, the news is filled with fresh allegations of cyber attacks on defense systems, private networks, and critical infrastructures. Provocateur elements of national militaries are responding with hawkish declarations and accusations. Likeminded states need to take the lead and develop a grand strategy that will moderate behaviour in cyber space. To use the nuclear weapons analogy, the world exists in the period before the Limited Test Ban and Non-proliferation Treaty. However, this treaty did not occur until thirty years into the Cold War. As the two decade mark of the internet nears, the world may be approaching a similar, and equally historic, milestone.

Bibliography

Adler, Emanuel. *Communitarian International Relations: The Epistemic Foundations of International Relations* (Routledge, 2005)

Antonenko, Oksana and Giegerich, Bastian. "Rebooting NATO-Russian Relations", in *Survival*, Vol. 51, No. 2 (2009)

Callaghan, John P.; Kauffman, Rudi. Building Cyber-Security: The Prospects of Deterrence. Conference Papers -- Midwestern Political Science Association; 2008 Annual Meeting

Center For Strategic and International Security, *Cybercrime, Cyberterrorism, and Cyberwarfare*, (The CSIS Press, 1998)

Clayton, Mark. "A US Cyberwar Doctrine? Pentagon documents seen as first step, and a warning", in *The Christian Science Monitor*, May 31, 2011 [available online] http://www.csmonitor.com/USA/Military/2011/0531/A-US-cyberwar-doctrine-Pentagon-document-seen-as-first-step-and-a-warning

Department of Public Safety Canada, *Canada's Cyber Security Strategy*, 5 October 2010 [online] available from http://www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.

Editorial, "A U.S. strategy for fighting cyberattacks", in *Los Angeles Times*, June 3 2011, [available online] http://www.latimes.com/news/opinion/opinionla/la-ed-google-20110603,0,5087778.story

Eriksson, Johan and Giacomello,Giampiero. "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", in *International Political Science Review* (2006), Vol. 27, No. 3

Finnemore, Martha. "Cultivating International Cyber Norms", *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011) http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf

Friedman, Jonah. "Cyber Weapons vs. Nuclear Weapons", at *Center for Strategic & International Studies*, 26 July 2011 [available online] http://csis.org/blog/cyber-weapons-vs-nuclear-weapons

Foreign & Commonwealth Office, "Security and Freedom in the cyber age – seeking the rules of the road" (2011) [available online] http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682

Gady, Franz-Stefan and Austin, Greg. *Russia, The United States, and Cyber Diplomacy: Opening the Doors*, (EastWest Institute, 2010 [available online] www.ewi.info.com

Globe and Mail, *China's Got RedBerry*, Apr.11th 2006, [online] available at http://www.theglobeandmail.com/report-on-business/article819974.ece

Gorman, Siobhan & Barnes, Julian E. "Pentagon: Online Cyber Attacks Can Count as Acts of War", *Wall Street Journal*, May 31, 2011 [available online] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=googlenews_wsj#printMode

Gregg Heather S., "Crafting a Better US Grand Strategy in the Post-September 11 World: Lessons from the Early Years of the Cold War", in *Foreign Policy Analysis* (2010), Vol. 6.

Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers* (Library of Congress, 2007)

Hughes, Rex. "Towards a Global Regime for Cyber Warfare", *The Virtual Battlefield: Prospectives on Cyber Warfare* (IOS Press, 2009)

Ilias Chantzos, "Opinion: Joining Battle on the Cyber Warfare Front", in *Jane's Defence Weekly*, December 6, 2010 (IHS Global Limited, 2010)

Information War Monitor, *Tracing GhostNet*, March 29 2009, (SecDev Group, Munk Centre for International Studies) [online] available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

International Business Times, "US can use force to respond to cyber-attacks: Robert Gates", June 4, 2011 [available online] http://uk.ibtimes.com/articles/157368/20110604/u-s-cyber-space-pentagon-robert-agtes-defence-hackers-accounts.htm

James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", in *Survival* (2011)Vol. 53, No. 1.

Krepon, Michael. " The Stability Instability Paradox", at *Arms Control Wonk*, 2 November 2010 [available online] http://krepon.armscontrolwonk.com/archive/2911/the-stability-instability-paradox

Kissinger, Henry. *Foreign Policy and Nuclear Weapons*, (W.W. Norton, 1969)

Lewis, James A. "Securing Cyber Space for the 44th President", *A Report on the CSIS Commission on Cyber security for the 44th President*, (2008), [available online] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Lewis, James A."Sovereignty and the Role of Government in Cyberspace", in *Brown Journal of World Affairs*, Vol. 16, Issue. 2 (Spring/Summer, 2010 p. 55- 65)

Liang, Qiao and Xiangsui, Wand, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February, 1999) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7179&rep=rep1&type=pdf

McAfee Inc., Virtually Here: The Age of Cyber Warfare (Virtual Criminology Report 2009), [available online] http://www.projectcyw-d.org/resources/items/show/129

Mshvidobadze, Khatuna. "Analysis: Is Russia on the wrong side of the net?", in *Jane's Defence Weekly*, Feburary 28, 2011 (HIS Global Limited, 2011)

Muniz, Jorge Jr. "Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors", thesis presented to Faculty of U.S. Army Command and General Staff College (2009), [available online] http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA502899

Neustadt, Richard E. and May, Ernest R., *Thinking In Time: The Uses of History by Decision Makers*, (The Free Press, New York, 1986)

Newsweek, "The Evil (Cyber) Empire: Inside the World of Russian Hackers", December 20, 2009 [available online] http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html

Nye, Joseph S. "Facing up to cyber security challenges", in *Power & Politics – Harvard Kennedy School Blog*, (2011) [available online] http://belfercenter.ksg.harvard.edu/power/2011/06/13/facing-up-to-cyber-security-challenges/

Nye, Joseph S. "Power and National Security in Cyberspace", in *America's Cyber Future: Security and Prosperity in the Information Age*, Volume II (Centre for New American Security, 2011) [available online] http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf

Nye, Joesph S. "The Challenge of Soft Power", in *Time Magazine*, March 8, 1999 [available online] http://www.time.com/time/magazine/article/0,9171,21163,00.html

Posen, Barry, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars.* (Ithaca: Cornell University Press, 1984)

Qingmin Dai "Flexibly Utilization of Battlefield Information Environments, to Gain Advantageous Positions in Combat, through the use of Information Conditions": submitted for inclusion in Peng Chencang"s book, "Efforts to Explore Information Warfare Theory Applicable to our Armed Force's", (Beijing, AMS, 01 Jan 1999)

Richard A Clarke, *Cyber War: The Next Threat to National Security and What To Do About It.* (HarperCollins Publishers, 2010)

Riley, Michael & Vance,Ashlee. "Cyber Weapons: The New Arms Race", at *Bloomberg Businessweek*, 20 July 2011 [available online] http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

Saunders Richard M., "Military Force in the Foreign Policy of the Eisenhower Presidency", in *Political Science Quarterly*, Vol. 100, No.1.

Segal, Adam. "Strategies for Engaging China in Cyber Space", at *Council of Foreign Relations* [available online – June 16, 2011] http://blogs.cfr.org/asia/2011/06/16/strategies-for-engaging-china-in-cyberspace/

Segal, Adam. "The Role of Cyber security in U.S-China Relations", at *Council of Foreign Relations* [available online]http://www.cfr.org/cybersecurity/role-cybersecurity-us-china-relations/p25318?cid=rss-fullfeed-the_role_of_cybersecurity_in_u-062111&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cfr_main+%28CFR.org+-+Main+Site+Feed%29

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", in *Berkeley Journal of International Law* (2009), Vol. 27, No. 1.

Streltsov, A. A. *Gosudarstvennaya informatsionnaya politika: osnovy teorii*, State Information Policy: The Basis of the Theory, (Moscow, 2010)

Sulek, David and Moran, Ned, "What Analogies Can Tell Us About the Future of Cybersecurity", *The Virtual Battlefield: Prospectives on Cyber Warfare* (IOS Press, 2009)

Testimony by Mary Ann Davidson, Chief Security Officer at Oracle, to the United States House of Representatives Subcommittee on Emerging Threats, Cyber security, and the Science and Technology, Source: http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Davidson-Oracle-SFR_10Mar09.pdf

The Economist, *The Stuxnet Outbreak*, Sept 30th, 2010 [online] available at http://www.economist.com/world/international/displaystory.cfm?story_id=17147818

The Economist, *The Threat from the Internet: Cyberwar*, 1 July 2010 [online] available from http://www.economist.com/node/16481504

The Economist, *War in the Fifth Domain*, July 1st 2010, [online] available at http://www.economist.com/node/16478792?story_id=16478792

Tikk, Eneken. "Global Cyber security – Thinking about a Place for NATO", in *SAIS Review*, Vol. XXX, No. 2 (2010)

Todd, Major Graham H. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", in *Air Force Law Review* (2009), Vol. 64

White House, *International Strategy for Cyberspace*, May 2011 [available online] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Zakaria, Fareed. *The Post-American World* (WW Norton, 2008) [audiobook]

Zapler, Mike, "FBI Investigates Gmail Hack", in *Politico*, June 2 2011 [available online] http://www.politico.com/news/stories/0611/56103.html