In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare

Hanna Samir Kassab

The characteristic vice of the utopian is naivety; of the realist, sterility.

EH Carr

Abstract Deterrence theory states that world stability can be maintained if the costs of war far out-weigh its benefits. Weapons and strategies that make defense cheaper and offense more costly decrease the likelihood of conflict. Nuclear weapons may have thereby helped create the stability of the Cold War via the costs associated with launching first; according to this argument, war between the US and USSR never occurred because the price of war (i.e. mutual destruction) was too high. This theoretical paper will extend this argument to cyber-attacks and suggest that in order to maintain the security of a nation's information technology, cyber-defense systems that correspond with Deterrence theory must be introduced. Cyber-attacks can be deterred if the proper system, a virus wall, is in place to counter any infiltration of a nation's defense systems. This proposed virus wall would be a way to achieve stability from nation state cyber-attacks. Theoretical advancements of International Relations will also be proposed, specifically considering the area of Security Studies.

H. S. Kassab (✉)
Department of International Studies, University of Miami, Miami, FL, USA
e-mail: h.kassab@umiami.edu

J.-F. Kremer and B. Müller (eds.), *Cyberspace and International Relations*,
DOI: 10.1007/978-3-642-37481-4_4, © Springer-Verlag Berlin Heidelberg 2014

1 Introduction

Deterrence theory states that world stability can be maintained if the costs of war far out-weigh its benefits. Weapons and strategies that make defense cheaper and offense more expensive decrease the likelihood of conflict. Nuclear weapons may have thereby helped create Cold War stability via the costs associated with launching first; according to this argument, war between the United States and Soviet Union never occurred because the price of war (i.e. mutual destruction) was too high.

This theoretical paper will extend this argument to cyber-attacks and suggest that in order to maintain the security of a state's information technology, cyber-defense systems that correspond with Deterrence theory must be introduced. Cyber-attacks are on the rise because it is cheap, easy and hard to detect. Attackers do not need to spend much time or money learning how to break into computer (Cheswick et al. 2003, p. 259). As such, the difficulty entails discouraging such behavior.

This chapter will specifically discuss cyber-attacks as infiltrations. One way to counter infiltration and deter cyber-attack is to introduce proper defense systems such as the virus wall. A virus wall would operate like a defense shield; if an attacker attempts to penetrate a system, then, it would bring about the complete destruction of the attacker's own system through a sudden onslaught of highly sophisticated computer viruses. Since the exact nature of the viruses that compose any given retaliatory attack would be unknowable in advance, attackers would be unprepared to develop their defenses and therefore, rational actors would be discouraged from such engagements. This proposed virus wall would be a way to achieve stability from state cyber-attacks via infiltration, eliminating the benefits of cyber-attack by making it harder, more expensive and easier to detect. Current strategies are inadequate and self-perpetuating, centreing around offensive behavior. This proposed strategy seeks to stabilize cyberspace now vital to national security.

This chapter will be broken up into five main sections. It is first necessary to apply cyber-warfare to the theory of Structural Realism. Cyberspace is the new anarchy, a new battle ground with no overarching authority to place limits on an actor's behavior. Within this new anarchy, new forms of capabilities can be found, but not as we expect. Cyber-warriors, state sponsored hackers, can now break into state institutions and compromise the national security of that state. Structural Realism, with all its elegance, will be applied to these new features of the international system. The second part of this essay will dwell on a reformulation of power. Power can no longer be the inflexible definition formulated by Waltz so many years ago. Rather, I recommend a more elastic concept of power borrowed from the Classical Realist, Hans Morgenthau. Power cannot be considered as a laundry list of state led formulations. Instead, power can be everything and anything: the control of man over man (Morgenthau 1985, p. 11). The third part of this essay aims to focus on more theoretical issues: how best to conceptualize (or re–re-conceptualize) security considering the introduction of cyber-warfare in the international system. I will consider broadened notions of security such as the Copenhagen school of Security Studies. Fourthly, I will discuss the unsus-

tainability and the danger of continuing cyber-attacks in the long-term. Fifthly, I will delve into the task at hand: formulating a system to protect states and more importantly humanity, from the volatility of the international system. I will conceptualize the virus-wall as a way to confront cyber-infiltration. This will be done by borrowing from the lessons of Mutually Assured Destruction and Offense-Defense theory. I will then conclude by discussing the theoretical tradition within International Relations, defining its tradition since its inception: to theorize stability and peace within a system of anarchy.

2 The Trojan War and the Growing Importance of Cyber-Security

Globalization has been hailed as the way to world peace. According to Giddens in his book "Runaway World," the forces of globalization grates against the sovereignty of states and its ability to regulate and govern domestic international affairs, while trying to create one sovereign: the market (Giddens 2003, p. 31). Globalization was brought about by increased modes of communication that destroys time and space (Ibid, 10). This makes state borders more porous and changing. Rapid technological innovation facilitated this transformation, reducing costs of transport and communication and supposedly making the world a better place (Ibid, 28). The globe is interconnected and this has made all nations more prone to shock.

The problem with cyberspace, like any international problem today (the financial and monetary systems for example, another paper perhaps), is the lack of governance to manage this new fast paced world (Mathiason 2009, p. xiv). Governance is needed to ensure the smooth running of the system by solving market failures and cyber-warfare. There has been attempts to raise the issue, but disagreements as to who is to govern and how has delayed progress. There are five competitors in the race to control the internet; states are not the only contenders. International organizations, the private sector, non-governmental organizations and lastly, academics are those seen as stakeholders in the race to regulate the internet (Ibid, 23). There are no established rules or norms to monitor behavior in cyberspace, not to mention a lack of institutions to define expectations and make states accountable for their actions.

A good way to understand cyber-attacks is to use a metaphor: the Trojan horse. Mentioned in Homer's Odyssey, the Trojan horse, a hallowed out wooden statue, was used by the Greeks during the Trojan War to infiltrate the impenetrable walls of the city of Troy. The horse is considered divine by the Trojans who took it as a sign of victory against the Greeks and as a gift from the gods. Many said to burn it, but they eventually welcomed it into the city and celebrated their perceived triumph. However, as the story goes, the Greeks filled the empty replica with soldiers who took the city as the Trojans slept. This metaphor is integral to appreciate the necessity for cyber-security; a cyber-attack may very well

Table 1 Watershed moments in history

Year	Type of attack[a]	Summary of Cyber-attack[b]
2007	Denial of service	Estonian ministries, banks and media attacked by Russia
2008	Hacking/infiltration/denial of service	Russia, South Ossetian, Georgian and Azeri websites attacked during Russia/Georgia war
2010	Hacking/infiltration/denial of service	Between Pakistan and India: an extension of their state of war
2010	Viral attack	Iranian nuclear facilities attacked by two intricate worm, Stuxnet and Flame which targeted and destroyed 58 % of all hardware
2000s	Infiltration/spear-phishing/ theft/espionage	People's Republic of China attack on US government, Chinese activists, business and citizens
2011	Hijacking	Iran brings down US drone
2000s	Hacking and hactivism	Breaking into systems for pleasure, criminal and political purposes

[a]From: Cheswik et al. 2003, p. 105
[b]From BBC News 2012a, b, c

destroy a state's ability to survive within the anarchical international system. States have already broken into sensitive databases. The armies of cyber-warfare are its hackers. Their weapons: ingenuity, dexterity and intelligence. They use these skills to infiltrate, steal and destroy, using programs such as viruses and techniques like phishing to accomplish their goals. These attacks can be for espionage, sabotage and destructive purposes. They can shut off power grids, siphon money, disrupt communication, cut off shipping, transport, fuel and water, disrupt the stock market and even hijack drones. This ultimately destroys the domestic stability of a state and creates chaos. Even more pertinent is cutting off state communication resulting in decapitation to gain strategic and tactical advantage prior to full scale invasion (Table 1).

Furthermore, cyber-warfare is a continuation of past strategies that destroy the state from within. In the past, kingdoms during war, sent spies to infiltrate the walls of other kingdoms to destroy or infect the water supply. Attackers threw dead bodies over citadel walls and made life difficult for those protected inside. These offensive measures are similar to cyber-attacks: they desire to weaken the state from inside. Again, the Trojan horse is a related strategy inherent to the strategy of cyber warfare and so, cyber-warfare is not anything new, but an extension, a new episode, an innovative technique that seeks to weaken the state from its interior, rather than through symmetrical means.

Considering this, cyber warfare is something to be expected considering the anarchical structure of the world; it is not entirely a new phenomenon. Rather, it is simply another arena of world politics that has been militarized to ensure security while limiting the security of others. It presents an opportunity to destroy a state's national security and autonomy and create a vulnerability that is so precarious, that its very survival, and that of its people, is at stake.

3 Revisiting Theory, Reconsidering Power

In order to relate to cyber-warfare theoretically and in terms of the Cold War, Structural Realism will be used. In the field of International Relations, Structural Realism was developed primarily as a reaction to Social Science's challenge for a more rigorous and scientific method. Structural Realists, like Kenneth Waltz, take on this challenge. This theory looks at the structure of the world system and the way it shapes the behavior of states. States rationally pursue their interests through a self-help system, without an overarching orderer. Therefore, the primary aim of all states, regardless of size and strength, is survival.

This world system of anarchy is permanent unless the structure changes. No state, or unit of that structure, can alter this framework. This, according to the theory, is the cause of war (Waltz 1979, p. 118). Structural Realism posits that states and state interaction is governed within this structure. To Waltz, a system is defined as a set of interacting units. A system consists of a structure, and "… the structure is the systems-level component that makes it possible to think of the units as forming a set as distinct from a mere collection" (Ibid, 40). The structure is defined by three factors. First, by anarchy, that is the absence of an overarching authority. Second, by the functions and then the capabilities of interacting units, more specifically, states (Ibid, 88). In this environment states seek to survive by any means, either through war or isolation. Nothing can alter the state's behavior unless the system itself transforms. Thus, Waltz sees the world as afflicted by the overwhelming structure of anarchy that cannot be mitigated. Structural Realists like Waltz see power as "…defined in terms of the distribution of capabilities" (Ibid, 192). For Waltz, the distribution of capabilities makes up the third pillar that forms the structure of the international system. The structure deviates with fluctuations in the distribution of capabilities among nations (Ibid, 97). Power "…is estimated by comparing the capabilities of a number of units" (Ibid, 98). Structural Realism claims that these capabilities can be economic, military and other factors like: size of population and territory, political stability and competence. States must use this capability in order to ensure their survival (Ibid, 131).

Considering the theory of Structural Realism, are cyber-attacks worth studying? Yes, they affect the distribution of capabilities, the relative power, and thus survival of states in the international system. As said in the previous section, cyber-warfare is not novel but just another arena in which states, and state interests, will collide. It only seems new because Waltz's definition of power, does not take into consideration new forms of power. For the purpose of this paper, I will reconceptualize power to take into consideration cyber warfare as a new plateau states upon which states will fight. I will adopt Morgenthau's conception of power defined in his magnum opus "Politics Among Nations." For Morgenthau, power "…may comprise anything that establishes and maintains the control of man…power covers all social relationships which serve that end, from physical violence to the most subtle psychological ties by which one mind controls another" (Morgenthau 1985, p. 11). The techniques of cyber-war desire to limit one's autonomy and control. Consider the weapons of cyber-war (Table 2).

Table 2 Some weapons of Cyber-warfare that redefines power (Cheswick et al. 2003, pp. 95–118)

Theft	Passwords, sensitive data through guessing, theft or compromised computer system
Bugs/back doors	Incorrect coding, difficult to find in prog ram resulting in system failure.
Authentication failure	Sign-in mechanism failure due to interference, server compromised
Protocol failures	Denial of use of application due to faulty protocol
Information leakage	Computer espionage
Exponential attacks	Use of Viruses and Worms that rapidly spread and cause harm to computer systems
Denial of service attacks	Overuse and straining of hardware to shut down or degrade service
Botnets	Espionage, Trojan horses and worms
Active attacks	Intruder who modifies, deletes and sends own data

These weapons not only decrease the power of the state, but render it under the control of another actor. Considering this, the problem is that we do not know where control begins, and where it ends. In this arena, power is no more state centric or real, it can be technological and can manifest itself through binary code. Power, especially considering cyber-warfare, must always be conceptualized holistically, and, as a result, an integral part of national and human security. The United States Department of Defense sees this new realm as integral to their national security. The Navy and Airforce now have cyber bureaus. The army, for example, has developed US Army Cyber Command (USCYBERCOM) which: "…plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (US Army Cyber Command). The aim of this bureau is to ensure that the United States and its allies are guaranteed free access to internet facilities and not to be controlled as such. Also, they desire to control the internet for their adversaries as identified. Thus, for the purpose of this chapter, cyber-warfare, and other arenas of warfare that defy the state, the concept of power must be redefined as Morgenthau distinguished so many years ago. The concept of power must be kept fluid and flexible, so that students of international relations can readily recognize new arenas of warfare and identify new generations of threats to ensure stability and security in the international system.

4 Re–re-Conceptualizing Security?

While this paper uses Structural Realism to analyze cyber-warfare, I must first address the diverse theoretical perceptions of what constitutes security. With all that is happening, scholars must finally decide to agree on this concept.

Cyber-security fits well with broadened notions of security and the Copenhagen Sectorial Approach of Security Studies. We must briefly integrate cyber-warfare into these perspectives. Traditional notions of state centered security still dominate today's discourse, and much of this chapter. I would like to discuss these matters to fully understand and acknowledge threats to the well-being of the state and humanity.

Traditional notions of security have centered mostly on the state. Realists argue that since the beginning of organized units of people, their primary concern has been survival and autonomy from outsiders. To Waltz, security is main function of the unit of analysis, the state. Anarchy is the main causal mechanism for this push for security. Arms races, alliances and concerts have existed to try to guarantee survival from threats to a state's security.

By the early eighties, the concept of security began to be contested. Richard Ullman, in his piece on "Redefining Security" 83' does not agree with such a "narrow" definition of security. He argues that security cannot simply be with the state and achieved through military. He defines national security as anything that interferes with the autonomy of states and the degradation of human life (Ullman 1983, p. 133). There are two main tradeoffs to any formulation of security: the first is liberty and security and the second, costs verses prevention (Ibid, 131). On many occasions, security curtails individual liberties and destroys the security and autonomy of the individual. This stems from the Hobbesian notion of security as one that sacrifices liberties for security. For Ullman, security cannot be defined by the state, but rather by what the state is supposed to protect: the human inside and the prevention of violent death. Violent death can be brought on by a bullet from a foreign soldier or from a violent person ostracized from society. The second is the costs verses prevention (Ibid). Looking at economic security, Ullman argues that it may be more efficient to invest in Green technology and energy alternatives than to build up military strength in the Persian Gulf. Military buildup may lead to the security dilemma which is essentially a negative sum game: in an attempt to become secure through military buildup, others perceive you as a threat and will balance against you. Thus, everyone is made more insecure (Ibid, 140).

To Ullman, security should be redefined by looking at the object of security rather than the means to security: a bullet in the head results in death; where it came from, whether from a looter or a neighboring state, is irrelevant. Integrally, security according to Ullman can no longer be considered state centric, but human centric. Thus, insecurity can be defined as anything that degrades human life and reduces state autonomy. Cyber-security fits in well with this analysis. As discussed prior, cyber-attacks have the potential to degrade human life and reduce state autonomy. National security can no longer be considered as military threats to the state, but rather, must focus on these aspects, even if we have to sacrifice an analytical concept. Furthermore, I would imagine he would agree with this chapter's proposition. Cyber-deterrence considers the long-term costs of cyber-warfare and chooses to prevent conflict for the sake of human enjoyment.

The next innovation of Security Studies is the Copenhagen school developed soon after the fall of the Soviet Union. This approach absorbs both traditional

and broadened notions of security using referent objects and levels of analysis. Barry Buzan, along with Ole Waever and Jaap de Wilde developed the theory of Securitization in "Security: A new framework of analysis" 98'. Securitization literature uses discourse analysis, speech acts, to understand how referent objects are securitized, moved from normal politics, or standard procedures within set laws and institutions, to an area of exceptional urgency. This is done through a speech act by someone with significant agency to shape structures and an accepting audience: a statesman, someone from an epistemic community, etc. (Buzan et al. 1998, p. 23).

The authors' use levels of analysis to see how each sector (military, economic, environmental, political and societal) can impact, influence and affect one another. These levels are systemic, subsystemic, regional and local (Ibid, 6). From this, the Copenhagen school presents a very convincing and practical answer to the traditional challenge for an elegant definition of security. It takes seriously the traditionalist challenge for coherence, but rejects their focus on solely military matters (Ibid, 4). Rather the Copenhagen school prefers to explore the logic of security itself to discover what distinguishes security and the process of securitization from other less pertinent matters (Ibid, 5).

Considering levels and sectors, levels are the ontological objects where events occur (Ibid). Buzan et al. cite four: local, regional, non-regional/subsystemic and global. Sectors serve as referent objects to disaggregate the clutter of the world's insecurity for the purposes of analysis by removing the irrelevant factors or variables (Ibid, 8). Security is divided into five distinct sectors: military, economic, environment, political and societal. These five sectors are referent objects that overlap and influence another (Ibid, 7). However, they are divided in order to explain just now they can create insecurity. The levels of analysis are used to see how sectors compare with one another and affect different referent objects. Thus, in a very scientific way, Buzan et al. disaggregate the different sectors of society to simplify and then, put them all back together again (Ibid, 167). This creates a formidable innovation to security studies.

To update this theory, cyberspace is simultaneously a level of analysis, and a sector. Cyber-space should be considered a level of analysis because it is a place where things happen (Ibid, 5). It is an ontological object that this chapter (and entire book) seeks to analyze.

5 New Copenhagen School

Six sector approach	Levels of analysis
(1) Military	(1) Global
(2) Political	(2) Non-regional—sub-systemic
(3) Societal	(3)Regional
(4) Economic	(4) Local
(5) Environment	(5) Cyberspace
(6) Cyberspace	

Table 3 Securitization at different levels of analysis (Ibid, 165)

Dynamics/ sectors	Military	Environment	Economic	Societal	Political	Cyber
Global	**	****	****	**	***	****
Non-regional/subsystemic	**	**	**	**	*	****
Regional	****	***	***	****	****	****
Local	***	****	**	***	**	****
Cyber	****	***	****	***	**	****

****- dominant securitization, ***- subdominant securitization, **- minor securitization, *- no securitization

Cyberspace is also a sector as it is currently being securitized by state and non-state actors; it is a site of contention. The act of securitization can move issues/referent objects from normal politics and bracket it to take extra-ordinary measures, above politics, to a more extreme form of politicization (Ibid, 24). There are two stages of securitization: the first is the portrayal of event/issue/person as a threat to the referent object. The second is the need for the public to consent, to successfully convince the audience. We see this happening. First, states perceive that their security as under attack and are doing what they can to exert control. The kill-switch is a firm example of this (to be discussed in the following section). Non-state actors see the internet as being attacked. They are doing their part to securitizing cyber-space as well. For example, hacktivists like Anonymous and Lolzsec see their freedom of speech and expression on the internet under threat. Their activities are a response to what they perceive as an attempt by states and corporations to annex the internet for their purposes.

The purpose of the Copenhagen school is to see what sector matters most at what level, and how easily a referent objects are securitized. For this reason, I have updated Buzan et al's chart that analyzes securitization at different levels of analysis.

As one can see, I have ranked the cyber sector as a high priority. As Buzan et al. says "the relative weight of sectors should depend primarily upon the degree of securitization but should also consider the relative importance of types of issues when sectoral concerns clash" (Ibid, 165) (Table 3). This is because information, especially military, economic and political sectors all are highly dependent on the integrity of electronic information systems. Worms and viruses have the ability to spread across borders, regions to even cover the globe, affecting all levels of analysis. With sectors, a successful large-scale cyber-attack could collapse the entire world economy. There could be military reprisals as well; political and societal cohesion would be torn asunder, resulting in anarchy and environmental destruction. All aspects of life would be disturbed; the acquisition of food clothing and shelter would be the only things that matter. Here, we see that Morgenthau's conception of power fits in better than Waltz's, as cyber-attacks are an extension of an actor's power that desires to control and supplant.

6 Dangerous Reactions to Cyber-Warfare and the Unsustainability of the Obama Doctrine

Thus far, there are no adequate plans for dealing with cyber-attacks. Although the Pentagon and the Executive branch of the United States as well as academics of International Relations and Foreign Policy have contemplated a handful of ideas, none have proved robust and viable. This is because the threat has not been adequately identified. This of course stems from the improper use of power as an analytical concept as well as the neglect of Structural Realism and the lessons of the Cold War.

The first, and most erroneous, is the military option. In the future, a US president could consider economic sanctions, cyber-retaliation or a military strike if key computer systems were attacked. According to Pentagon spokesman Colonel Dave Lapan, "A response to a cyber-incident or attack on the US would not necessarily be a cyber-response. All appropriate options would be on the table" (BBC News 2011a, b). As such, the United States will respond in ways that would bring further reprisals and military responses.

This of has not been an effective deterrent to stop cyber-attacks. Rather, there have been more: the United States and its allies continue to be victims of these attacks, not only from states, but by hackers and hactivists alike. More importantly, the credibility of the United States can potentially be called into question for failing to respond to cyber-attacks in military fashion. This goes against the doctrine of Mutually Assured Doctrine (discussed later), in that states should remain not only capable, but credible, when it comes to promises of reprisal. In this regard, the United States has been irresponsible in its behavior, not only to the American people, but to global stability and peace.

Another idea that has been toyed with is the Kill Switch. The Kill Switch is effectively a "a device…or…a typed code…that can bring the World Wide Web to a sudden halt against an impenetrable wall of 404 Error codes" (Radford 2012, DiscoveryNews.com). There many issues with this. Electric grids, water, security systems, the bar code readers at supermarkets, international commerce and trade, would be immobilized. Production would come to a sudden halt, businesses will close. Our entire contemporary way of life will be held hostage. How will persons live? How will the government keep power and prevent theft and anarchy? This option will do more harm than good: it should not be on the table. The ability of governments to do this is also in question, especially because the internet is a decentralized apparatus of communication. As of today, there are no borders on the internet; states have sought to control the internet, but face competition with private enterprise and other non-state actors for ownership (Mathiason 2009, p. xiv).

Academics have also suggested policy to engage cyber-warfare. Most are adequate, but not enough. Clark and Levin "Securing the Information Highway" in 2009 suggests ways to enhance electronic defenses against cyber-attacks by state and non-state actors. They argue that while cyber-attacks are hard to trace, cheap, effective and on the rise, there are procedures to defend against them. He employs

risk management and develops strategies that address everything from communication networks to chips inside computers, through diversity. His most effective suggestion is the use of multiple systems. If one system is lost in a cyber-attack due to viral or worm infection, then there would be two or three other identical systems waiting to replace it. This minimizes the cost of attack for a while. There is of course the possibility for a second or third strike to take out these replacement systems. Another useful suggestion by Clark and Levin is to become self-sufficient in the manufacture and consumption of significant national security computer hardware. Outside hardware systems from the People's Republic of China and the use of other imported technologies could have monitoring bugs in place for espionage purposes. There is much to be done on the defense side of cyber-security. The offense-side of these matters has been developed over the years, especially during the Obama Administration. This, even though it presents important strategic advantages, can lead to dangerous and deadly reprisals.

The Obama Doctrine has been defined by many scholars, but has been discussed most succinctly by Charles A. Kupchan in his article "Enemies into Friends" in 2010. The Obama Doctrine formulates a foreign policy of engagement with those previously considered enemies: Iran and North Korea. As said, Obama is willing to "extend a hand" to those "who cling to power through corruption and deceit" if they "are willing to unclench" their fists (Obama, Inaugural Address). Obama is known for using soft power over hard. He takes credit for rebuilding alliances and won the Nobel Peace Prize for his example. He is also known for other activities. The Obama Doctrine uses other forms of power other forms that extend the influence of the United States. The Obama Doctrine combines diplomacy with a new form of high-tech, low-budget and politically astute intervention, one that maximizes America's influence while minimizing costs for a cash-strapped government. James M. Linsday also discusses this in his article "George W. Bush and Barack Obama: the future of US leadership." He argues that the change of leadership brought about a more multilateral rather than unilateral approach to defending similar goals. Both leaders want to maintain US security and global leadership, but go about it in fundamentally different ways. Rather than the "shock and awe" of the Bush Doctrine, the Obama Doctrine uses diplomacy and inexpensive, yet effective technological weaponry, like drones, viruses and covert operations (Osama bin Ladin assassination). It is suspected that the United States, in conjunction with Israel, developed the Stuxnet and Flame worms that destroyed much of the Iranian nuclear facilities in Natanz, Iran (BBCNews 2012). These worms are said to be the most complex and advanced pieces of malware ever to be created. Many doubt that this was created by a non-state actor. Instead, many point to the mentioned states as the perpetrators. This act significantly increases the profile and popularity of cyber-warfare as method of advancing state interests.

Attacks such as this are an integral extension of the Obama Doctrine and possess many advantages, especially in the respect to the growing debt. The United States cannot afford another war and must seriously consider retrenchment in a conventional sense (Parent and Macdonald 2012). It is a cost effective way of neutralizing the enemy, more specifically, delaying Iranian nuclear capability and

preventing all-out war in the Middle East. This, in conjunction with assassination of nuclear scientists, presents a seductive argument in favor of cyber-warfare. However, in many respects, I think this policy is not only unsustainable, but counter-productive and a product of short term thinking. That which we have done can also be done to us. The Iranians, with their own allies and invent, can also develop capabilities to respond to these attacks. Costs have nothing to do with these endeavors; any nation or non-state actor can create or duplicate a worm just as sophisticated as Stuxnet and Flame. The United States with its allies must prepare for this eventuality; Pandora's Box has been opened, and once open, it will be difficult, almost impossible to close. Like the atomic bomb of 1945, the United States must consider that belligerent nations may also be developing their own Stuxnet and Flame worms; duplication is far easier than innovation. Considering this, the right policies must be developed to dissuade. The Cold War and Deterrence theory presents an opportunity to devise ways to do so. In this respect, Cyber-deterrence must be considered as an automatic response to cyber-attacks for the preservation of national autonomy and human enjoyment.

7 Revisiting the Cold War

After World War II, scholars and statesmen came up with the traditional, state-centric definition of security which still dominates today. This conception advocates that one's autonomy and the ability to deter an enemy, enables a nation's security. This gave rise to deterrence theory. Thomas C. Schelling in "The strategy of Conflict" outlines Deterrence theory as the ability to absorb a sudden nuclear attack from the Soviet Union and counter attack. This was referred to as Mutually Assured Destruction (Schelling 1960, p. 207). Deterrence theory argues that international political stability can be upheld if the costs of attack are greater than its rewards. Tactics and armaments that make defense easier and offense more difficult are integral to achieve such balance. Conversely, if offense is easier and cheaper, then war is more likely. For example, World War I began because offense was easier than defense; it was easier to attack first than to try to absorb an attack. It is argued that during the Cold War, nuclear weapons achieved such equilibrium. Through second strike capability, ensuring Mutually Assured Destruction, the US would be able to successfully deter the Soviet Union by absorbing their first strike, reorganizing, and launching a devastating second strike to neutralize the Soviets. This of course may cause a nuclear winter, destroying much of the world, but the very thought of being annihilated would successfully deter both parties (Waltz 1989, p. 626). For this to work, actors must be always credible and capable to maintain a balance.

Mutually Assured Destruction also forms the foundations of Offense-Defense Theory, an integral part of Defensive Realist theory (van Evera 1998, p. 6). Defensive Realism argues that states pursue power optimization rather than power maximization. States look at the costs and benefits of war before embarking on military adventures: the costs of attack must be more than the cost of defense.

In sum, Deterrence theory suggests that in order to guarantee stability, one must make the costs of war much greater than the benefits for the other party (Ibid, 7). Once an aggressor understands that the costs of war would be far greater than the benefits of war, his actions would be curtailed. In essence, the purpose of this work is to extend this argument to cyber-security: to maintain the security of a nation's information technology, cyber-defense systems and policies must be formulated with Deterrence theory in mind.

8 MAD, the Viruswall and Cyber-Stability

As said, contemporary efforts to create cyber-security are not sustainable and will do more harm than good in the near future. As argued, scholars must look to Cold War and learn innovative ways to counter cyber-attacks. This is my attempt.[1]

The idea of the virus-wall comes from the combination of a firewall and a virus. As will be discussed firewalls fail as a way to protect a sensitive databases. Instead of a simple firewall, I would like to imagine a firewall that has the ability to infect infiltrators with a virus that is so powerful, contagious and unstoppable, it would be designed to destroy the attacker's computer system and those in its proximity. This is to make the costs of cyber-attack more costly and create some stability in cyber-space.

First, firewalls are defined as "…any device, software or arrangement or equipment that limits network access" (Cheswick et al. 2003, p. 175). It acts as a barrier to deny access to the unwanted and unauthorized. The firewall must remain full-bodied and impenetrable to deflect attacks. Firewalls can be found inside hardware such as routers, modems and so on (Ibid). There are four main categories of firewall: packet filtering, circuit gateways, application gateways and dynamic packet filters. Without going into much detail, each type attempts to block unwanted users. These function in similar ways, using their source and destination address to identify users (Ibid, 176). In this way, it is a passive way to deny access to the unauthorized.

Secondly, viruses are exponential attacks that use programs to spread themselves quickly. Worms follow the same logic, except are programs that travel by themselves. They operate the same way as biological weapons, their effects being felt in a matter of hours (Ibid, 106). They work best within weak and unprotected systems, those prone to bugs and users that practice irresponsible behavior. Viruses and worms can cause economies to slowdown and stop, and sometimes result in loss of life (Ibid, 17). They usually infect "targets of opportunity" or weak security systems, but can also be sophisticated enough to destroy political targets.

Firewalls do help keep access out and can defend against viral and worm attacks, but the fact remains, break-ins do occur. Failures can be a result of poor

[1] I am in no way a computer expert, but I am attempting to create a new way to protect data. In this sense, this part presented some difficulty, but the idea behind, deterrence, is solid. Hopefully, this idea will be picked up by an agency or computer security company.

design as well as conscious efforts to undermine security, i.e., cyber-attacks. There are many ways to get past a firewall. One of the most malevolent ways to tunnel in, which is "an architectural concept in which one or more protocol layers are repeated so that a virtual topology is created on top of a physical topology" (Ibid, 223). In other words, unauthorized users can encapsulate data from one area of a database to another using the faculties of the firewall. Once inside, the message is inserted into the network and tucks itself inside the database rendering it undetectable. This way, unauthorized actors can infiltrate, steal or control the database that is supposedly protected by this firewall.

What can be done to avoid this type of infiltration? It is here that I will discuss the proposed virus-wall system. If an attacker infiltrates a database's virus-wall by tunneling through it, a virus should attach itself onto the attacker, that is, use the tunnel that was created to seek out and destroy the source of the attack. To recall, a virus attaches itself through contact with an uninfected user. If there is no communication, then there is no transmission. There will be no infection if there are no attackers making contact with the infected database (Ibid, 106). The problem with firewalls is that it is a passive means of defense; after all, the walls of Troy were penetrated by enemy forces. The scheme is to infect the database with the virus without harming the database.

Furthermore, the virus should be so aggressive to knock out all the computers within its vicinity. This way, the cost of attack would be so outrageous, no further attacks would be launched. Staying true to Defensive Realism and the assumptions of Mutually Assured Destruction, such a system would minimize the occurrence of cyber-warfare as the benefits of carrying out such activities would be cancelled out by its enormous and unreasonable costs (van Evera 1998, p. 8).

To understand this further, consider this analogy. Let us imagine a much sought after database as a sick person. If one willfully touches the infected person with a very infectious virus, for example, to steal their wallet, one will become ill. This would be enough to insure that that person's wallet will remain safe. The key to this is communication: the potential crook must know that the wallet is infected. In this sense, like Mutually Assured Destruction, actors must always remain credible and capable: they must maintain such a system and follow through, and communicate this strategy to any potential attackers. Once attackers know and understand the repercussions of attack, then there would be no attack.

There are, of course, moral and ethical issues that must be discussed. Like Mutually Assured Destruction of the Cold War, cyber-deterrence disturbs the lives of many innocent people. I am arguing for a system that seeks to destroy the computers in proximity to the attacker's. An entire state's economic growth and development can be hindered by this proposed system. Is it fair? Of course not, but like the logic of sanctions (the way they are supposed to work) the citizens must confront the initial attacker to prevent any further cyber-attacks. However, there must be an antidote available to the attackers after some time. The antidote would effectively remove the virus from infected computer systems. Before the antidote is given, a second virus-wall will replace the first to continue cyber-deterrence. In this sense, cyber-warfare can be effectively stopped bringing balance to cyberspace.

Fortunately, there is a similar system to this already in existence. Overwatch Textron Systems, a cyber-security company, is proud to demonstrate the abilities of their capabilities which,

> Through our breakthrough CogDat® technology, users can track and visualize every action performed on all of the files in their control. This unprecedented situational awareness at the file level-of-detail allows users to understand how their data is handled. Multi-source data access and correlation extends this situational awareness to other environments such as access controls (who is in your facility and when), network account log monitoring, traffic monitoring, and other inputs (overwatchsys.com 2012).

This means total transparency; one would be able to identify and monitor those accessing the program, identifying the perpetrator before the infiltration is committed. This would dramatically cut down espionage and crime as this system presents the perfect deterrent. States and non-state actors would thus be discouraged from conducting illegal activities.

However, this may not stop cyber-attack. Rather, this system is a soft version and differs to what I recommend. Currently, there are no laws to punish states who conduct cyber-attacks; there is a definite lack of governance over cyber-space and the internet. As said, states operate within an international system as described by Structural Realism: it is one of the self-help comprising of an anarchical structure. Even with the perpetrators properly identified, it would be very difficult to bring offenders to justice. They would be protected by their state's borders. Thus, actors may continue their attacks with no fear; only of reprisal. There would be no stability as described by the idea of Mutually Assured Destruction. There should be a mechanism in place to disrupt these activities by making punishment for such indiscretion a reality.

Fundamentally, any system is better than the non-system in place. It places a check on states who seek to ruin the quality of life of others in order to raise their own relative power. The cat is already out of the bag, and once states begin attacking one another's electrical grids and defense secrets, there is a very good chance war could break out. To recall, a military response is an option as a response to cyber-attack, according to the United States government. While the benefits of cyber-attack are great, so are the costs to those attacked; a response to attack should be expected and this makes for a very dangerous world. In the long-run, cyber-warfare can only become more costly with reprisals. Once this happens, all-out war becomes more and more attractive. This paper tries to solve this by imagining a system where the tactic of cyber-attack becomes more and more expensive and less and less likely.

9 Defining and Continuing the International Relations Tradition

I began with E.H. Carr's quote "The characteristic vice of the utopian is naivety; of the realist, sterility" (Carr 1978, p. 12) to stir up the issue of this work's scholarly contribution. In doing so, I define academia's raison d'être in terms of

his theoretical tradition. Carr is known as the founder of modern International Relations. He begins his classic "The Twenty Years' Crisis by identifying the duty of academics: "Our [political scientists] first business…is to collect, classify and analyze our facts and draw our inferences…" (Carr 1978, p. 2). He continues: "The passionate desire to prevent war determined the whole course and direction of this study" (Ibid, 8). Further, that "Political Science is the science not only of what is, but of what ought to be" (Ibid, 5), that a good mix of the two antithetical forces of utopianism and realism will result in coherent and productive foreign policy (Ibid, 222).

Following Carr, the Realisms of International Relations have a normative aspect which inherently defines them as well as the field. For example, Classical Realism through Morgenthau argues that "…it shares with all social theory the need, for the sake of theoretical understanding, to stress the rational elements of political reality; for it is these rational elements that make reality intelligible for theory" (Morgenthau 1948, p 10). Neoliberal Institutionalism also has its own normative roots, i.e. world peace through cooperation. Keohane expounds: "although it would be naïve to believe that increased cooperation…will necessarily foster humane values in world politics, it seems clear that more effective coordination policy among governments would often help" (Keohane 1984, p 11). Even Structural Realism, with its purposive theory serves a normative function: to explain and predict. More so, the need take international politics and forcibly divorce variables from one another needs normative faith. Thus, our honored tradition includes the search for something good: world peace and stability.

Furthermore, the Realisms dictates that states must be made to behave well through power, whether through Carr's appeasement (1978), Morgenthau's Diplomacy (1948), Waltz's Balance of Power (1948, 1979), Schelling Deterrence theory, (1977), Keohane's Regimes (1984), and of course, Offense-Defense theory (van Evera 1998). This world is undeniably anarchical. Stability must be brought to it with the strategic use of power. Power is common to all forms of the political and the Realisms deem power as a dualist force that simultaneously prevents and enhances peace.

This chapter continues the tradition of Realism, in that it desires to see a stable world through the use of power. As said, cyber-warfare is nothing novel, only a part of the structure of the international system and its distribution of capabilities, or power. Like other capabilities such as conventional and nuclear weapons, the use of weapons of cyber-warfare, viruses and worms, can be checked through strategies borrowing from Offense-Defense theory: if the costs of war outweigh the benefits, then states would not go to war. States must make cyber-attacks more expensive than advantageous, and thus, impossible. Currently, states are attacking one another through the cyber realm because it is cheap, easy and hard to detect. My argument, the use of cyber-deterrence, hopes to end cyber-warfare by making it too expensive and difficult, not to mention easier to detect as a nation's cyber infrastructure would be knocked out. In such a way, I, as an inheritor of this discipline, engage with those who went on before, as we continue to comprehend the complexities of war and peace.

10 Conclusion

The search for cyber-security in a realm of anarchy is not an elusive one. Using the tools of International Relations, Structural Realism and Offense-Defense theory, we are more able to suggest ways to counter cyber-attacks. States now rely on cyber-space for defense and internal cohesion. Coherent cyber-security policy must be in place to defend the nation and its people against attack. Contemporary responses are not enough; computer engineers must think up new ways to counter new threats, and defend the security of the nation and the citizen.

This chapter searches for such a solution. It suggests that cyber-attacks can be deterred if there was a system in place to make any infiltration costly. Borrowing from Mutually Assured Destruction, if a nation's security is at risk due to infiltration, then the response should be an overwhelming, resulting in the destruction of the attack's computer systems. In this way any act of aggression, and any perceived advantage of carrying out such an attack, would result in instant defeat.

Ultimately, my conclusion remains: cyber-warfare presents a new chapter in international politics while continuing business as usual. While there are many benefits to conducting cyber-warfare, the costs to the citizen is simply too great. States can achieve their goals through diplomacy, not espionage. The international system is anarchic volatile enough. A stabilizer must be introduced to force states to be good. This can be done with the introduction of a system borrowed from the Cold War: the cyber-deterrent.

This chapter also discussed the field of International Relations. Cyber-warfare tests the theories of Structural Realism and its concept of power. Structural Realism passes in its explanation of cyber-warfare as an extension of the world's structure. As a theory, it possesses great explanatory powers that elucidate, and, in this case, predict international events and outcomes. However, its rigid concept of power fails in its flexibility to take into account change: new fronts and methods of conflict. It must be substituted for that of the Classical Realist. The purpose of cyber-warfare is to control and avoid control: in essence, it is a way that states can blackmail and alter one another's behavior. In order to adapt to changing environments, a flexible theory of power must be considered to predict new methods and techniques of control. States cannot afford to be caught by surprise. This is the purpose of theory, to make sense of a confusing and cluttered world. In writing this chapter, I proudly continue the tradition International Relations was founded on: to discover ways to secure some stability in a world forever ignorant of it.

References

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Colorado: Lyne Rienner.

Carr, E. H. (1978). The twenty years crisis, 1919–1939: An introduction to the study of international relations. London: Macmillan.

Cheswik, W., Bellowin, S., & Rubin, A. (2003). *Firewalls and internet security: Repelling the wily hacker*. Boston: Pearson Education, Inc.

Clark, W. K., & Levin, P. L. (2009, November 1). Securing the information highway. *Foreign affairs*. Retrieved September 12, 2012, from http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.

US Army Cyber Command (2012). Retrieved September 12, 2012 from http://www.arcyber.army.mil/.

Giddens, J. (2003). *Runaway world: How globalization is reshaping our lives*. New York: Routledge.

Keohane, R. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton, NJ: Princeton University Press.

Krasner, S. (1983). *International regimes*. Cambridge: Cornell University Press.

Kupchan, C. A. (2010, March 1). Enemies into friends. *Foreign affairs*. Retrieved September 12, 2012, from http://www.foreignaffairs.com/articles/65986/charles-a-kupchan/enemies-into-friends.

Linday, J. (2012). George W. Bush and Barack Obama: The future of US leadership. *International Affairs, 87*(4), 765–779.

Mathiason, J. (2009). *Internet governance: The new frontiers of global institutions*. New York: Routledge.

Morgenthau, H. (1985). *Politics among nations: The struggle for power and peace*. New York: Alfred A. Knopf.

BBC News, (2012a).US Pentagon to treat cyber-attacks as 'acts of war'. Last modified June 1, 2011. Retrieved September, 2012 from http://www.bbc.co.uk/news/world-us-canada-13614125.

BBC News, (2012b). Internet based attacks on critical systems rise. Last modified April 18, 2011. Retrieved September 12, 2012 from http://www.bbc.com/news/technology-13122339.

BBC News (2012c). Flame: Massive Cyber-attack discovered, researchers say. Retrieved September 12, 2012 from http://www.bbc.com/news/technology-18238326.

Obama, B. (2009). Inaugural Address. Retrieved September 2012 from http://www.presidency.ucsb.edu/ws/index.php?pid=44&st=&st1=#axzz1cX85656y.

Parent, J. M., & MacDonald, P. K. (2011, October 14). The wisdom of retrenchment. *Foreign affairs*. Retrieved September 12, 2012, from http://www.foreignaffairs.com/articles/136510/joseph-m-parent-and-paul-k-macdonald/the-wisdom-of-retrenchment.

Radford, B. (2012) Does the internet have a 'kill-switch'? in Discovery News. Retrieved September 12, 2012 from http://news.discovery.com/tech/does-the-internet-have-a-kill-switch-120907.html.

Schelling, T. (1960). *The strategy of conflict*. London: Oxford University Press.

Ullman, R. (1983). Redefining security. *International Security, 8*(1), 129–153.

van Evera, S. (1998). Offense, defense and the causes of war. *International Security, 22*(4), 5–43.

Waltz, K. (1979). *Theory of international relations*. New York: Columbia University Press.

Waltz, K. (1989). Origins of War in Neorealist theory. *Journal of Interdisciplinary History, 18*(4), 615–628.

Overwatch Textron Systems. (2012). September 14, 2012 from http://www.overwatchsys.com/.