MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

Perspectives on Cybersecurity:
A Collaborative Study

Massachusetts Institute of Technology:
Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz

Do Not Cite or Circulate Without Permission from Authors

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

PERSPECTIVES on CYBERSECURITY

A Collaborative Study

Authors

Chrisma Jackson

Lyla Fischer

Brooke Gier

Vivian Peron

Ben Ze Yuan

Liu Yangyue

Glenn Voelz

Editors

Nazli Choucri

Chrisma Jackson

Department of Political Science

MIT

2015

Table of Contents

8. Is Deterrence Possible in Cyber Warfare?

Brooke Gier

While it may not seem like it at face value, nuclear warfare and cyber warfare have a lot in common. Both exist in domains characterized by the security dilemma, offense-defense balance, and the urge for preemptive strikes. Both are unconventional and have the capability to cause enormous damage to a state. Deterrence – the aim to prevent an adversary from attacking with the threat of retaliation - was utilized as a strategic policy answer to the nuclear tension between the Soviet Union and the United States during the Cold War. Similarly, deterrence seems like a viable option to prevent cyber attacks currently.

There are several problems with the use of deterrence, however. First, deterrence requires communication in order to work – the threat has to be communicated to the adversary, otherwise he will not know it even exists – and this communication seems to be unavailable during cyber conflict. Second, unlike nuclear warfare, cyber conflict has a range of severity – it can be harmless, or it can be catastrophic. Thus, states lose credibility - another needed component of deterrence – to punish an aggressor when the aggressor has committed a "harmless" act because it is unreasonable to do so. Third, terrorist groups and individuals have the capacity to conduct cyber warfare, unlike nuclear warfare. Thus, a rational actor – another need for deterrence – is removed. Despite these difficulties, state leaders do need to formulate an international agreement to address the cyber realm, so that in the case a cyber attack does occur, there is a plan to address it.

8.1 Cyber Definitions

There are numerous definitions floating around for cyberspace, cyber security, and cyber warfare. This paper identifies cyberspace to include both the physical and syntactic layer, as well as distinguishes cyber warfare from cyber conflict or incident. Cyber conflict is "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield."[123] Cyber warfare falls under cyber conflict, but involves attacks that are generally much more severe, malicious, and originate from a state or organization (such as a terrorist organization) against another state or organization.

8.2 The Structure of International Relations

To continue with this paper, it is important to lay down fundamental concepts of the political and cyber realm. According to traditional realist theory,[124] three fundamental aspects characterize the international system: anarchy, self-help, and sovereignty. There is no official hierarchy or governing structure over states, and each state must work for its own survival. States are sovereign over their own land, people, and resources, and externally are considered "equals" when it comes to international law.[125] States devise grand strategies- a state's theory about how it can best devote its

[123] Brandon Valeriano and Ryan C Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51(2014): 348.

[124] Realist theory is focused on because of its significance in nuclear deterrence strategy and theory.

[125] Kenneth Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Pub., 1979), 102-116.

resources to achieving its objectives– and incorporate military doctrine – a subcomponent of grand strategy that deals explicitly with military means - to ensure the security of the state.[126]

According to Barry Posen, states can adopt three different types of military doctrine.[127] An offensive doctrine aims to disarm or destroy the enemy, while a defensive doctrine aims to deny the enemy from achieving the objective he seeks. A deterrent doctrine aims to punish an aggressor - to raise his costs without reference to reducing one's own. This leaves a state vulnerable to enemy attack because it normally lacks defensive capability.[128] Normally states adopt some kind of mixture of these doctrines.

According to traditional realist theory, security dilemmas are an inherent part of the international system. By increasing one's own security, one decreases the security of others. This leads states to respond with similar measures, which leads to arms races and potential military conflicts. The offense-defense balance further affects security dilemmas. If offense has the advantage, a security dilemma is more likely to ensue more quickly and dangerously.[129] Weapon technology adopted matters. For example, building a moat and barbed wire is not going to make a neighbor state as nervous as mobilizing troops and creating weapons that can be used both defensively and offensively. When offense has the advantage, this normally leads to preemptive strikes because speed is of the essence.[130]

8.3 Nuclear Strategy: Deterrence

After the advent of the nuclear bomb and the beginning of the Cold War, deterrence became the cornerstone of U.S. strategic and military doctrine to prevent preemptive strikes. Deterrence requires capability, credibility, and communication. A state must have the ability to punish an aggressor, the credibility to actually follow through with the threat, and communicate this to its adversary.[131] The infamous Mutually Assured Destruction policy adopted in the 1960s was the fruit of the security dilemma and nuclear deterrence. It assumed that each belligerent had enough nuclear capability to destroy the other side, and the other side could also destroy its enemy if attacked.[132] It, thus, had several requirements in order to be effective: a second strike capability and a rational enemy. If states did not have a second strike capability, then they would be motivated to preemptively strike their enemy in a "use it or lose it" situation. The other side also had to be rational – in other words, he had to also desire to avoid nuclear warfare.

Nuclear strategy and deterrence have potential applications to cybersecurity. Military planners like to compare cyber weapons to nuclear weapons because each can cause massive, strategic-level damage and both require presidential authority to use.[133] Cyber warfare, like nuclear warfare, has the possibility to be avoided through deterrence. It has been widely noted that offense has the advantage

[126] Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 24.

[127] Ibid.

[128] Ibid.

[129] Charles L. Glaser and Chaim Kaufman, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22 (1998): 44-82.

[130] Ibid.

[131] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm" in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, 55-77, Washington, DC: National Academies Press.

[132] Ibid.

[133] Shane Harris, @ *War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014), 48-50.

when it comes to cyber warfare; it is easier to attack than defend against cyber attacks.[134] An attack need only succeed once, whilst defense must succeed every time. Additionally, there are numerous malware and potential cyber attacks being created on a daily basis - defense has the hard job of keeping up with these developments.[135] Therefore, theoretically preemptive strikes will be more likely, especially as cyber warfare becomes more integrated into military doctrine in the future.

8.4 The Schriever Wargame Implications for Deterrence

In fact, this has proven the case when the annual Schriever Wargame played out a cyber war scenario. Each year, a game is held premising a strategy issue currently vexing U.S. forces, with participants from more than thirty U.S government agencies including the Intelligence Community, Defense, as well as private sector actors like executives from technology companies.[136] In 2010, the game was premised on cyber warfare – an adversary in the Pacific region launched a crippling cyber attack against a U.S. ally, the ally invoked its mutual defense agreement, and the United States had to respond. Yet, before the United States could make its first move, the adversary struck preemptively to block the US forces' access to the computer networks they needed to communicate and send orders.[137]

Conventional blockades allow belligerents the ability to communicate to each other by flashing lights or hailing to each other over radio frequency – that can give warnings and signal assertive actions, but fall short of actual fire and lethal action. In the game, however, the participants did not know how to communicate – they only knew how to attempt to destroy the adversary's network.[138] Deterrence failed – assuming deterrence had even existed in the first place (it was not clear that the other side even believed in it.) The adversary's next step was to push U.S. satellites out of orbit.[139] The participants playing the U.S. side became confused and disorganized – not sure what to do short of launching a full-scale war. They realized that there were no cyber war agreements with foreign allies, and thus no "road map" for an international response.[140] Ultimately, the mock game persuaded U.S. civilian and military officials to reassess how they looked at cyber warfare and their readiness for it.

Harris argues that there is a clear set of steps that belligerents can take to avoid a nuclear war.[141] Throughout the Cold War, U.S. and Soviet officials created and demonstrated new types of missiles, as well as discussed nuclear weapons in speeches and public statements.[142] These steps did not exist or emerge during the war simulation game – there was no communication whatsoever. That is not to say these steps are not possible in the realistic future, but since integrating the cyber realm into military doctrine and grand strategy are still in its beginning stages, they have not been created yet. Either way, the necessary component of communication for cyber deterrence is lacking.

8.5 Analysis of Actual Cyber Conflict and Implications for Deterrence

Interestingly, however, the Schriever Wargame seems to have represented an anomaly from

[134] Nazli Choucri quotes James R. Gosler in *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012), 149.
[135] Ibid., 144.
[136] Harris, @ *War,* 49-50.
[137] Ibid., 50.
[138] Ibid.
[139] Ibid., 49.
[140] Ibid.
[141] Ibid., 49-50.
[142] Ibid.

current cyber international relations. Brandon Valeriano and Ryan C. Maness conducted a research study looking at how serious the cyber threat currently is between state rivals, and found very different results than the scenario presented to the participants at the Schriever Wargame. They developed a scale to assess cyber incident damages on a scale from one to five. One was a nuisance and harmless (like defacing websites) while five was "escalated dramatic effect on a country."[143] First, they found that very few states actually fight cyber battles. They expected to find one incident/dispute per year for each rivalry dyad and actually found less than that.[144] Second, there were few and far in between instances of relative severity, and none of them were so severe as to provoke military action. The highest severity was a three, and this only occurred in 13% of cases. The average severity was a 1.62.[145] The occurrence of a cyber incident was not only rare – it was unlikely to be severe at all.

Finally, they found that China was the main instigator behind many of the attacks. They noted that cyber conflicts tended to remain regional, but the most active cyber relationship was one with global implications: the outlier of the United States and China. China had initiated a cyber conflict 20 times with the United States within the eleven-year period, while the United States only initiated two. China's motivation appears to be stealing sensitive or secret information.[146] These numbers show a couple things. First, the United States' well-known cyber offense capabilities failed to deter China from cyber initiations and second, the United States has shown great restraint in deciding not to retaliate against China.

Valeriano and Maness's study shows fundamental differences between nuclear deterrence and cyber deterrence. Their inherent nature sets them apart. There is no range of severity for a nuclear attack – all nuclear attacks start on the catastrophic and disastrous level and continue to get worse from there. There is, however, a range of severity for cyber incidents. States can carry out smaller attacks that are nuisances and relatively harmless, rather than actual threats to national security.[147] This has several implications. As Harris points out, cyber conflicts lack the necessary communication component of deterrence - the "dance steps" policymakers can take to send signals. Yet even more importantly, they also seem to lack the necessary credibility requirement for deterrence.

Cyber conflicts, unlike nuclear conflicts, *can* be small and harmless and this means that one of the crucial elements of deterrence is undermined: credibility. Namely, the United States is not going to provoke a tantamount and horrendous war because China hacked into the State Department and looked at some secret files.[148] China *knows* this – and thus, the U.S. loses its credibility to threaten a disastrous punishment. Deterrence will fail until a certain point – the point at which the cyber incident becomes serious enough to call for a substantial national and possibly military response to the incident. So what does this mean for U.S. policymakers? While it is important to have an operational plan ready in case a country were to spontaneously launch a devastating cyber attack on the United States, it seems more worthwhile to invest resources into handling more realistic cyber conflicts – on a range of severity levels.

[143] Valeriano and Maness, "The Dynamics of Cyber Conflict," 353.
[144] Ibid., 355.
[145] Ibid.
[146] Ibid., 356.
[147] Valeriano and Maness, "The Dynamics of Cyber," 350-357.
[148] Ibid., 356-357.

8.6 The Trouble of Non-State Actors

Additionally, some scholars worry that terrorist groups can gain control over nuclear weapons (whether that is likely or not remains debatable);[149] however, the same can surely be said for terrorist groups and cyber warfare. Unlike nuclear weapons, cyber warfare is easily accessible to individuals and organizations.[150] The extent of the amount of damage they can cause remains unknown, yet given the constant development of cyber offensive capabilities, their ability to cause severe damage in the future is probable.

Many have already learned how to use the cyber arena to their advantage.[151] Cyber warfare in the hands of terrorist groups removes one of the main components for a deterrent policy like MAD to work – a rational actor. As U.S. policymakers move forward, this is one more important element to keep in mind.

8.7 The Importance of International Regulation

Ultimately, just because cyber incidents are not currently severe and commonplace does not prevent that from happening in the future. The Schriever Wargame showed it is imperative that major powers come together and decide an international agreement on cyber warfare for several reasons. Firstly, to ideally prevent preemptive strikes from being taken in the first place and secondly, so there are international responses in place to address such attacks in case they should ever occur. Richard Price argues that unconventional weapons are not inherently unconventional – social norms deem them so, established by state leaders.[152] They have an institutionalized stigma, and there are laws that forbade their use and policies set up to address if they are used.

Cyber weapons are arguably unconventional – they add an entire new dimension to warfare and have the ability to negatively impact entire populations at one time. Therefore, an international agreement is imperative for cyber weapons, especially as their capabilities and technologies develop. Key rival leaders need to meet and assess the different threats cyber warfare currently has upon their respective nations, and collectively decide what they believe is allowable and what they believe is not. Deterrence may not work for the low-level cases of cyber incidents, but it can surely work for the severe and devastating attacks. This needs to be established before they can be allowed to happen, and set off a chain reaction of devastating attacks. While this may not directly address the potential of terrorist groups and individuals, it is an important start that can help states respond to such a threat, should it ever occur.

[149] Scott Sagan is the most notable.

[150] Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," *Version 8-25 for internal ECIR review* (August 2011), 1-4.

[151] Choucri, *Cyberpolitics,* 152.

[152] Richard Price, *The Chemical Weapons Taboo*, (Ithaca, NY: Cornell University Press), 70-100.

References

Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge, MA: The MIT Press.

Choucri, Nazli and David D. Clark. 2011. Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. *Version 8-25 for internal ECIR review* (August 2011), 1-4.

Glaser, Charles L. and Chaim Kaufman. 1998. What Is the Offense-Defense Balance and How Can We Measure It? *International Security* 22 (Spring): 44-82.

Harris, Shane. 2014. *@ War: The Rise of the Military-Internet Complex.* New York: Houghton Mifflin Harcourt Publishing.

Morgan, Patrick M. 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. In *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, 55-77, Washington, DC: National Academies Press.

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

Price, Richard M. 1997. *The Chemical Weapons Taboo*. Ithaca, NY: Cornell University Press.
Valeriano, Brandon and Ryan C Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51 (May): 347 – 360.

Waltz, Kenneth N. 1979. *Theory of international politics*. Reading, MA: Addison-Wesley Pub. Co.