COMP116: INTRODUCTION TO COMPUTER SECURITY

THE APPROACHES AND LIMITATIONS OF CYBER DETERRENCE

December 15, 2015

Hayley Cohen

Mentor: Ming Chow

Tufts University Department of Computer Science

Fall 2015

Contents

ABSTRACT

The theory of deterrence is not a new one. It is a theory that claims if a country's defense is strong and there is some sense of vengeance established, it is more likely that an attacker might retract. Deterrence can be applied to all of the long-standing war domains: land, air, space and water. However, now there is a call to develop a method of deterrence for the newest domain, the cyber realm. This domain of war is still very new, although it is starting to gain as much attention, if not more, as the pre-existing domains. Both governments and private sectors are working to figure out the best way to approach and handle cyber terrorism. It has been proposed that cyber deterrence is imperative and that there are several different approaches to achieving cyber deterrence. This paper will analyze what these approaches are and how they come together to create cyber deterrence in real world situation. As the theory develops, a question of its practicality arises. This paper will assess both the political and technical limitations to cyber deterrence and how they affect the feasibility of the approach to be successful.

TO THE COMMUNITY

The most dangerous weapon is the one that no one knows about. In the cyber realm, most weapons aren't known of until an actual attack occurs. The new war domain is a dangerous one because of the possible consequences. Attacks in the cyber domain differ from attacks in other domains as they target a broader range of victims. Cyber attacks not only target and affect states but also can target private companies or individuals. Any institution from a hospital or bank to a school or police station has the possibility of falling victim to a cyber attack. Where as during the Cold War, when deterrence originally found its way into the national security strategy, it was only nations that possessed nuclear weapons and it was a limited number of nations, over 140 nations are recorded to be developing cyber weapons and thus over 30 countries have included cyber units in their militaries. The same way that governments incorporated plans of deterrence into their security strategies, it is important for plans to deter and defense against cyber attacks be made. If a broader spectrum of people understands the approaches to deterring cyber attacks, a nation has a higher probability of having a strong a security strategy.

INTRODUCTION

Deterrence, by definition, is the strategy intended to dissuade an opponent from taking an action not yet started. The theory became most popular during the cold war as nuclear weapons developed. The idea was for the weapons to "be always at the ready, yet never used." The theory justified the possession of nuclear weapons and often was compared to two people standing with guns to each others heads. It created an uneasy and tense relationship but a peaceful one nonetheless.

The newest domain of warfare lies in the cyber realm and while deterrence is still necessary and very relevant, the classic theory of deterrence is no longer sufficient. The emerging theories of cyber deterrence are much more flexible and involve several different approaches. Cyber threats and attacks are very different from classic attacks. They are intangible and exits purely in a virtual world. Also, classic deterrence only had to focus on weapons of mass destruction; there are an infinite amount of possible cyber weapons. Therefore, the theories emerging for cyber deterrence are much more flexible. Since the cyber realm is still developing, there are many different approaches, each one with benefits and drawbacks.

APPROACHES TO CYBER DETERENCE

Cyber deterrence is becoming a part of many national security strategies. As the domain of the cyber realm grows, it becomes more and more important for nations to be prepared with a deterrence plan. The approach to cyber deterrence is much more flexible than the traditionally theory. It is shaped by the motives and methods of the cyber attack. Some approaches to cyber deterrence are general, at the basic level this could be installing a firewall to stop unwanted traffic from coming in. Others can be much more specific such as blocking all traffic from a particular server.

Consistent with the traditional method of deterrence, retaliation is one of the conceivable

approaches to deter in the cyber realm. When an attacker is identified, law enforcement has the opportunity to step in and strike back. The difference in this scenario is that the retaliation can be kinetic, or cyber. Even though a kinetic response is an option, it is more practical to keep the retaliation within the same domain and strike back with a cyber attack. Regardless of the method of retaliation, there is much debate if striking back is necessary at all. Retaliation could cause the conflict to escalate or ultimately hurt the victim more. The general question with any sort of deterrence is whether or not the risks out way the benefits. In the case of retaliation, there is too much risk to strike back. Another flaw is that to successfully deter an attacker with retaliation, the attacker has to be confident that the nation has the ability to retaliate and the nation has to be confident that there is something to strike back. This was easier to do with the traditional method because if a nation had nuclear weapons, they had something physical to show off. In the cyber realm, weapons are generally invisible until put to use. Therefore, the attacker doesn't know if a nation actually has the capacity to strike back. Conversely, if the attacker doesn't have a cyber infrastructure, there is nothing to strike at in the cyber realm.

Resiliency is another approach to cyber deterrence. Resiliency is the idea that a system is so durable that any attack would not do significant damage. Resiliency as a form of deterrence can be approached two different ways. The first is through redundancy. If a nation relies solely on one system, and that system is breached, then there can be significant consequences. If the system is the main cyber infrastructure for a nation, the outcome of an attack has the possibility of not only affecting the government but also civilians. Therefore, a nation can create alternative systems that run the required capabilities. The alternative systems can be in the possession of the nation itself, allied nations or third-party companies. If a cyber attack were to occur, the fallback systems could be used until any issues are resolved. The nation wouldn't lose any of the critical capabilities and thus the attack would not be as detrimental. The redundant systems do not necessarily need to exist all the time but it's important to plan

where they would exist. If an attack were to occur, the party hosting the system can quickly open and host the necessary ports and capabilities. The second approach to resiliency is reconstitution. If a nation can revive quickly from an attack, the effects are minimal and the system can restart without much damage. Reconstitution can be achieved by having a stockpile of servers or a reserve of bandwidth that can be used in the event of a debilitating attack.

As strong as resiliency and retaliation have the potential to be, the ultimate deterrence is invisibility. The only way to completely protect oneself is to become invisible to everyone. A system can be made invisible by disguising it as something else. Even if an attacker knows that the system exists, they still have to be able to locate it. Although, invisibility is the strongest deterrence, there are legal issues that need to be considered. One particularly common method of hiding a military or government system is to pose it as a civilian computer. This is controversial due to the practice of open carry. In any other domain, this would be carrying firearms openly so that the casual observer is aware. In the cyber domain, if a system were being posed on a civilian computer, the casual observer would not be aware.

As strategies of cyber deterrence develop, it has become clear that there are some major limitations that make it impossible to have a completely effective approach. One of the most limitation factors is the idea of attribution. When there is a kinetic attack, it is easier to identify who the attacker is. If an attack comes from a Chinese military, it's pretty safe to say that the attack comes from China. Even if an attack comes from a boat or a plane, it's relatively easy to identify or track down who is responsible. When there is a cyber attack, attributing the attack to a particular group becomes extremely difficult. It often requires further investigation, and depending on the scale of the attack it may not be worth the resources. Even if the exact computer that the attack came from can be identified, that is not enough evidence to conclude who is responsible. When this is the case, deterrence becomes even more difficult. Without a known attacker, retaliation becomes impossible. With no target, there is nothing to

strike at. Attribution also limits a nation from strategizing. Without knowing where threats are coming for, it is difficult to plan a defense against a group or anticipate future attacks. As a result, many argue that due to the issue the lack of attribution causes, cyber deterrence is completely obsolete. Although it does create many set backs, in cases where it is imperative to identify the attacker, attribution tends to not be an issue. It has been found that cyber threats that the United States has seen are conducted with an explicit political goal. If the attacker remained anonymous, then they would not be able to get credit for whatever their intentions were. Therefore, they claim responsibility to some extent.

Another limitation is that cyber attacks are generally single use weapons. A cyber attack is developed to achieve a very specific task. The task could be to shut down a specific system or computer or target a particular network. Since the attacks are not repetitive, it is difficult to develop a theory that would apply across the boards. In kinetic realm, when weapons were developed, nations learn the affects and those affects are for the most part consistent for that particular weapon. This makes strategizing simpler, identify the weapon, learn the outcome and prepare accordingly. In the cyber realm this is not the case. The weapon is often not discovered until it is put to use, and the outcomes can vary depending on the motive, so there isn't much to prepare for.

APPLICATIONS

As cyber threats become more prevalent, nations are developing stronger security strategies. The idea of cyber threats and cyber deterrence are starting to make their way into the previously published U.S. strategy documents. The focus of these documents is still primarily on attacks from weapons of mass destruction but there is a clear acknowledgment of cyber attacks. Nonetheless, the National Military Strategy to Secure Cyberspace was published in 2007 and outlines the nations security plan in regards to cyber attacks. The department of defense classifies the details but the document demonstrates that the dangers of cyber

threats are acknowledged and the nation is aware that it needs to plan accordingly.

One of the first cases of cyber deterrence was in Estonia in 2007. The attacks on the government lasted 22 days and were primarily distributed denial of service (DDOS) attacks. These attacks flooded the system with data so that no legitimate traffic could be created. Estonia relies heavily on its cyber infrastructure so these attacks had the potential of being devastating. The Estonian response demonstrated the resilience approach to deterrence. The attacks were on critical systems but they did not cause serious damage. Estonia has a computer emergency response team and due to their strong response, the ports that were shut down to prevent further attacks could be reopened in a timely fashion. Although Estonia was successful with their deterrence response, it also demonstrated one of the flaws. Estonia was not easily able to identify the attacker. A thorough investigation could have legitimized any suspects but that would take more time and effort. Since Estonia was able to recover without knowing the attacker, it wasn't deemed necessary to pursue a full investigation. Although no official claim could be made, Estonia was able to ultimately conclude that Russia was most probable to be responsible due to various circumstances. Once the attacker was identified, the idea of striking back just wasn't plausible because Russia did not have a strong cyber infrastructure to strike.

Another noteworthy example of cyber deterrence occurred in Georgia in 2008. The attacks were on network infrastructures and could disable Georgia's communication with the outside world. Georgia was not nearly as prepared as Estonia but they were still able to deter the attacks. With the help of other nations and companies, Georgia used the redundancy approach. Those providing aid hosted the necessary sites on their better-defended systems. Therefore, although the main networks were compromised, Georgia was able to perform the critical capabilities.

The attacks in both Georgia and Estonia were credited to Russia, which demonstrates another limitation of deterrence. The most dangerous weapon is the one that no one knows

about. In other domains, this is more difficult to come by. Even weapons of mass destruction have a level of predictability. In the cyber realm, a single weapon has a broad spectrum of capabilities that are not necessarily known. As a result, deterrence methods cannot address a particular attack but rather need to address the outcomes.

SUMMARY

It is important for nations to develop strong security strategies because the possible cyber attacks do not only affect governments, but also have the capabilities of affecting civilian institutions and services. Although cyber deterrence can be costly, the costs are insignificant compared to the consequences that could arise from a cyber attack.

The current approaches are still flawed and there are some major limitations but as the cyber realm grows and cyber threats become more frequent, the approaches to cyber deterrence will become stronger and more effective.

REFERENCES

Cyber Deterrence Is a Strategic Imperative. (2015, April 28). *Wall Street Journal.* Retrieved from http://blogs.wsj.com/cio/2015/04/28/cyber-deterrence-is-a-strategic-imperative/

Freedberg, S. (2014, November 7). NATO Hews To Strategic Ambiguity On Cyber Deterrence. Retrieved from http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/

Glaser, C. (2011). Deterrence of Cyber Attacks and U.S. National Security. *Thoughtful Analysis of Cyber Security* Issues, 1-8.

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than Practice. 1-26.

Haley, C. (2013). A Theory of Cyber Deterrence. *Georgetown Journal of International Affairs.* Retrieved December 6, 2015, from http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/

Kugler, R. (n.d.). Deterrence of Cyber Attacks.

Talbot Jensen, E. (n.d.). Cyber Deterrence. *Emory International Law Review*, 26(2), 1-53.