Wyatt Steere

INFO 200

2/18/2022

Is Cyber Deterrence Still Viable?

On the morning of the 7th of December 1941, The Boston Globe posted a headline stating “U.S. At War! Japan Bombs Pearl Harbor, Casualties Heavy” (Galloway 2022) Over 130 million American citizens woke to the horror of Pearl Harbor. Morning habits still contain cups of coffee, grogginess, and breakfast pastries but the way in which war is waged has undergone a paradigm shift. While the trenches of World War One shifted with the lives of thousands, and oceans were crossed by B-29 Bombers in World War two, warfare now increasingly takes place within the constraints of technology. Battle lines are drawn not in the sand but online. Information gained and lost is critical to the success of cyberwarfare. With a seemingly constant increase in attacks to critical infrastructure, such as the December 2021 attack in which the FBI exposed a spearfishing campaign led by Chinese-state sponsored hackers targeting oil and natural gas pipelines, the need to deter cyberattacks and migrate deterrence theory to the cyber space is looming (Significant Cyber Incidents 2022). The impact of these crimes is massive and continues to grow, with the Canada, Mexico and the United States experiencing a “157.5 billion to cybercrimes and 0.78% loss of GDP annually” (Mcafee 2022) A commonly accepted definition by Joint Doctrine is the prevention of action by either the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. By this definition the question remains whether deterrence is possible in the cyber space? Deterrence rests on deterring crimes from three major groups, state-sponsored hackers, criminal hackers, and hacktivists (hack activists). State-sponsored hackers are motivated by political power, criminal hackers by money and hacktivists by social change and justice. All three groups must be deterred for deterrence to be deemed successful. The nature of cybercrimes and the attribution problem provides doubt on the viability of cyber deterrence. Although difficult, the argument will be made throughout this paper that cyber deterrence is possible and can revitalize the United States defense against cybercrime. The emergence of new theories discussing the viability and success of cyber deterrence such as cross-domain and a culture of strong declaratory and retaliatory protocols, paired with traditional deterrence by denial and punishment, proves that cyber deterrence remains viable and will work in conjunction to prevent attacks from all three major groups of attackers.

The field of traditional cyber deterrence is split into two distinct realms, deterrence by denial and by punishment. Martin Libicki, in his book *Cyber Deterrence and Cyber War*, describes these two realms as “Deterrence by denial is the ability to frustrate the attacks” or the enhancement of physical defenses to prevent attacks. On the other hand, “deterrence by punishment” promises “the threat of retaliation” (McKenzie, T. M. 2017). The attackers fear of retaliation by the defendant provides deterrence for an initial strike by the offense. A defendant’s ability to cultivate these two aspects of deterrence places them firmly in the dominant position to defend attacks. To solidify deterrence by denial a “robust network defenses and the ability to withstand and recover from disruptions and other attacks” must be configured by the United States (McKenzie, T. M. 2017). The stout network of defenses for America`s critical infrastructure must be expanded upon to prevent future attacks. Denial is a cornerstone to deterrence and through investment and expansion this key element can minimize the attacker`s ability to exploit systems and information. Denial helps deter all three main attacking groups (hacktivists, state-sponsored, and criminal) as increased defense deters low level attackers allowing a focus on preventing attacks from high level actors. Additionally, the defense grid requires attackers to justify more resources and personnel for their attack, decreasing the likelihood of attacks.

While, a plentiful grid of defense raises the technological skills and needs of possible attackers, minimizing threats, denial does not strike fear into these bad actors. Credible and absolute threats must be communicated to derail attacks. A standard and undeniable set of regulations must be set for any offenders. Deterrence by punishment or active deterrence promises retaliation and harm to the assailant for the actions of the cybercrime. When thinking of the three major attacker groups, state-sponsored hackers are most easily deterred. The difference between state-sponsored and others is the “ability to inflict an appropriate level of punishment on a nation-state to deter unfavorable behavior guided by that state” (McKenzie, T. M. 2017). The threat of political power allows for active deterrence to make an effect. Monetary punishments or removing the monetary incentive from the attack helps deter groups motivated by profit. Actively deterring attacking groups is most effective against state-sponsored groups but does affect criminal hackers to a degree if profit incentives are eliminated. Governments are less likely to interfere elections or government actions if the repercussions against their people or themselves are high. Unfortunately, criminal hackers and hacktivists do not have that same responsibility to others and are harder to deter. Traditional deterrence this maintains a role in any plan to fend off cyberattacks and deterrence by denial and punishment can aid in the persuasion of all three attacking groups.

The expansion of deterrence theory and development of new strategies revitalized the practicality of deterrence when it comes to the cyber space. As experience is gained with cyber defense, cyber deterrence theory expands. Two major expansions of modern cyber deterrence theory, strong declaratory and retaliatory policy paired with cross-domain deterrence, allows for increased effectiveness. The Georgetown journal, in a journal by Christopher Haley, argues that Retaliation can vary “according to the source, the magnitude, and the political environment” but the U.S. should establish “precedent by retaliating against attacks in consistent ways, thus showing the world the consequences of a given action” (Haley, C. 2013)

The emergence of a strong declaratory and retaliatory policy can set the tone for the rest of the world that the Untied States will provide a swift and retaliatory strike towards any attacker. The ability to share this message globally and then act upon it when the time comes will provide a strong idea of the ideology of the United States surrounding cyber-attacks. Less organized criminal groups and hacktivist groups will corrode under the pressure of American cyber retaliation. The policy also provides flexibility for retaliation, allowing non cyber attacks in retaliation to cyber-attacks, if the message is sent that the attack occurred due to the aggressors own cyber-attacks. Cross-Domain deterrence expands upon that flexibility. The United States does not hold its dominant world position quite so securely as the middle of the 20th century, therefore battles must be picked carefully. The emergence of cross-domain deterrence allows the United States to participate in conflicts that facilitate multiple domains (such as space, land, naval, cyberspace). The interconnection of our world through technology lends an advantage to cyber investment. Cyber has permeated warfare and the collection of confidential information through hacking is one of the greatest advantages it has provided. King Mallory, in a published paper titled New Challenges in Cross-Domain Deterrence, states the U.S. can exploit the weakness this weakness by mapping their network of instruments by which opponents create this information space” and during conflict “attack these assets through cyberattack” (Mallory, K. 2018). The combination of cyberattack with ground, naval, or air support facilitates information gathering and then the execution of gathered information for a military advantage. Cross-Domain Deterrence involves the release of this gathered information back to the aggressors. While the main object of this method is against state-sponsored hackers, it can easily apply to hacktivists and criminal hackers as well. Information is critical to any cyber attack lifecycle and without an information advantage the bad actors cannot complete their attacks without serious repercussions they could not withstanding. Applying these new theories to United States military policy lends new life to cyber deterrence.

Cyber deterrence has several vocal detractors, and the viability of deterring cyberattacks remains uncertain. In the article *Is It Time to Forget About Cyber Deterrence,* Maj Ross proposes the attribution problem with cyber-attacks. While a bombing, land invasion, or naval attack can be easily attributed to an army or country, the nature of cyber attacks lends itself to covering the tracks of the attacker. The low “barrier to entry enables many actors, and what would deter each actor is almost as varied as the actors themselves” (McKenzie, T. M. (2017). This argument lends several good points as deterring these actors from varied backgrounds makes deterrence incredibly difficult. Additionally, there are certainly tools that actors use to cover their tracks such as signed binaries, or the use of common channels and protocols.

This argument lends itself to criminal hackers and hacktivists as a state-sponsored hacker is more easily attributable. The argument has diminished in strength over time as more attribution methods have arisen and the tracking of these criminals is easier. Improvements in attribution technology based “on better data collection and the profiling of known hackers and nation states by intelligence agencies” (Goel, S. 2020). While the attribution problem may have limited deterrence in the past the argument is outdated as modern attribution methods have allowed the defense to catch up to the offense and find the criminals behind the crimes. In May of 2021, “Interpol apprehended and identified nearly 600 cybercriminals” who had targeted “several Southeast Asian governments and funneled almost 100 million” into their pockets (Mathews, L. 2021). The project was dubbed HAECHI-1. These arrests along with countless others demonstrate the progress made in improving attribution for cybercrimes.

Another topic favored among advocates against the viability of cyber deterrence is the unbridgeable gap between attackers and defense within the cyberspace. They argue that offense inherently has an advantage when it comes to cyberattacks, due to the low barrier to entry and constant innovation of new attacking techniques. An “offensive-persistent environment” within cyberspace creates a scenario where “the defense may have tactical and operational success, but the offense will persist” therefore the defense will never have definitive victory (Cameron, M. 2021). The intrinsic offensive advantage creates an environment in which the defense never has a moment to rest before the next attack comes and therefore will be worn down until exhaustion. This argument has several valid points, in that the cyber space lends advantages to the offense. The innovation of new attacking tools is nearly constant, and defenses are victims of a war of attrition.

Cyber deterrence does face the difficulty of an uphill battle, one of constant research to determine where the enemy may strike next. The opposition does not consider that while new attacks pop up, defenses are anticipating more and more of the possible attacks. The Defense Department and Cyber Security branch of Homeland Security “signed a memorandum of understanding to collaborate on a range of cybersecurity initiatives” (DOD 2021). This collaboration shows the innovation promise for innovation within the current space. Additionally, through working with private industries, the DoD shows that across last “years cyberattacks, nearly every compromise harnessed a legitimate credential and exploited the openness of Active Directory to accomplish the attacker’s objective” (CisoMag 2021). The use of legitimate credentials is an aspect of user error that cannot be compensated for. The fact that nearly all attacks were the result of user error demonstrates how little room attackers must maneuver within and must resort to exploding human error.

Cyber deterrence has numbered and vocal detractors all with valid concerns about the viability of deterrence in the modern age. They fail to consider the strives and innovation possible within this field. Currently, there are hinderances such as “highly classified documents, non-access to cyber operators, and the embryonic stage of existing military cyber organizations. Over time, we expect those hurdles to slowly melt away” (Soesanto S., Smeets M. 2021). The increased collaboration between departments, government and private industry, and a renewed concern for cybersecurity allows for defenses to outstrip state-sponsored, criminal hackers and hacktivists. Innovations in the technology and warfare industries paired with traditional deterrence aid themselves to an increasingly bright future. With further insight into the three main attacking groups, easier attribution, and massive upheaval in policy the field of cyber deterrence will play a key role in current and future wartime policy.

**Works Cited**

Cameron, M. (2021). Is it Time to Forget About Cyber deterrence? *Air and Space Power Journal - Contemporary*. https://doi.org/https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-35\_Issue-1/C-Ross.pdf

CisoMag. (2021, September 9). *3 ways the federal government is using technology to advance cybersecurity*. CISO MAG | Cyber Security Magazine. Retrieved February 19, 2022, from https://cisomag.eccouncil.org/3-ways-the-federal-government-is-using-technology-to-advance-cybersecurity/

*DOD, DHS collaborating on Innovative Cybersecurity Solutions*. U.S. Department of Defense. (2021). Retrieved February 19, 2022, from https://www.defense.gov/News/News-Stories/Article/Article/2449534/dod-dhs-collaborating-on-innovative-cybersecurity-solutions/

Galloway, T. (2022, January 4). *Attack on Pearl Harbor - topics on newspapers.com*. Topics. Retrieved February 19, 2022, from https://www.newspapers.com/topics/world-war2/pearl-harbor-attack/

Goel, S. (2020). How improved attribution in Cyber Warfare can help de-escalate cyber arms race. *Connections: The Quarterly Journal*, *19*(1), 87–95. https://doi.org/10.11610/connections.19.1.08

Haley, C. (2013, February 6). *A theory of cyber deterrence*. Georgetown Journal of International Affairs. Retrieved February 19, 2022, from https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley

Mallory, K. (2018, April 12). *New challenges in cross-domain deterrence*. RAND Corporation. Retrieved February 19, 2022, from https://www.rand.org/pubs/perspectives/PE259.html

Mathews, L. (2021, May 31). *Nearly 600 arrested in massive cybercrime bust*. Forbes. Retrieved February 19, 2022, from https://www.forbes.com/sites/leemathews/2021/05/31/nearly-600-arrested-in-massive-cybercrime-bust/?sh=55fcb04a2273

McKenzie, T. M. (2017). *Is cyber deterrence possible?* Air University Press, Air Force Research Institute.

*Significant cyber incidents*. Significant Cyber Incidents | Center for Strategic and International Studies. (2022, February). Retrieved February 19, 2022, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Soesanto S., Smeets M. (2021) Cyber Deterrence: The Past, Present, and Future. In: Osinga F., Sweijs T. (eds) NL ARMS Netherlands Annual Review of Military Studies 2020. NL ARMS (Netherlands Annual Review of Military Studies). T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-419-8\_20

*There's nowhere to hide from the economics of Cybercrime*. McAfee. (2022, February). Retrieved February 19, 2022, from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html