Journal of Strategic Security

Volume 7
Number 1 *Volume 7, No. 1: Spring 2014*

Article 6

Is Cyber Deterrence an Illusory Course of Action?

Emilio Iasiello
Private Sector, iasiello@aol.com

Is Cyber Deterrence an Illusory Course of Action?

Author Biography

Emilio Iasiello is the chief threat analyst for a global cyber intelligence firm, supporting federal and commercial entities to manage cyber risks, understand their threat environment, and help prioritize their investments against those threats impacting their business or mission. He has worked in cyber threat analysis since 2002 both as a government contractor and a government civilian with the Department of State and the Department of Defense, respectively. Emilio has written papers on the development of a new cyber threat analytic methodology, the cyber threat to aviation, a proposal to fix U.S. national cyber security efforts, and the IT Supply Chain.

Abstract

With the U.S. government acknowledgement of the seriousness of cyber threats, particularly against its critical infrastructures, as well as the Department of Defense officially labeling cyberspace as a war fighting domain, the Cold War strategy of deterrence is being applied to the cyber domain. However, unlike the nuclear realm, cyber deterrence must incorporate a wide spectrum of potential adversaries of various skill, determination, and capability, ranging from individual actors to state run enterprises. What's more, the very principles that achieved success in deterring the launch of nuclear weapons during the Cold War, namely the threat of severe retaliation, cannot be achieved in cyberspace, thus neutralizing the potential effectiveness of leveraging a similar strategy. Attribution challenges, the ability to respond quickly and effectively, and the ability to sustain a model of repeatability prove to be insurmountable in a domain where actors operate in obfuscation.

Introduction

With the U.S. government (USG) acknowledgement of the seriousness of cyber threats, particularly against its critical infrastructures, as well as the Department of Defense (DoD) officially labeling cyberspace as a war fighting domain, security experts, policymakers, and think tank researchers have resurrected a potential Cold War strategy to implement against the new threats fermenting in cyberspace.[1] It is argued that the same principles that successfully contributed to nuclear deterrence with the Soviet Union can be applied to cyberspace and the hostile actors that operate within. However compelling, similar strategies are not transferrable and the key factors that made nuclear deterrence a viable solution does not carry the same value in cyberspace. While only a handful of states have demonstrated the capability to develop nuclear weapons, more than 140 nations have or are developing cyber weapons, and more than thirty countries are creating military cyber units, according to some estimates. Moreover, this threat actor landscape does not consist of nation states alone. Included are cyber criminals, hackers, and hacktivists of varying levels of sophistication and resources willing to use their capabilities to support nefarious objectives.[2]

There are advocates favoring the implementation of a cyber deterrence strategy to mitigate the volume of hostile cyber activity against public and private sector interests. However, too many factors—including attribution challenges and sustainability against this vast threat actor landscape—inhibit cyber deterrence options from achieving their desired outcome in the near term. What's more, other deterrent strategies such as those employed against nuclear weapon use, terrorism, and rogue state behavior is not suitable models for the cyber realm. Despite some commonalities, the cyber domain lacks the transparency and actor visibility required to develop deterrence measures. Despite these hindrances, nation states should seek to develop, refine, and implement national level cyber security strategies that focus on cyber defense improvements and enforce accountability to measure their successes. While there will always be sophisticated actors able to thwart the most robust cyber security defenses, the success of hostile activity against networks are the result of poor cyber security practices such as unpatched systems and users not well trained in information assurance principles. Cyber security is an ongoing effort that needs to be relentlessly monitored and adapted to a constantly changing threat environment.

What is Cyber Deterrence?

Before one embraces the design and development of a nation state cyber deterrent strategy, it is important to understand the basic concepts of deterrence and what it entails for a strategy of cyber deterrence. At its base, a deterrence strategy seeks to influence an adversary from not

[1] "International Strategy for Cyberspace," *The White House*, May 2011, available at: *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*; "Department of Defense's Strategy for Operating in Cyberspace," *U.S. Department of Defense*, July 2011, available at: *http://www.defense.gov/news/d20110714cyber.pdf.*

[2] "Nuclear Weapons: Who Has Them At a Glance," *Arms Control Association,* April 2013, available at: *http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat*; Susan W. Brenner and Leo L. Clarke, "Civilians in Cyberwarfare: Casualties," *SMU Science & Technology Law Review* 13 (2010): 249; Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *Air Force Law Review* 64 rev 96 (2009); William J. Lynn, III, "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack," *Foreign Affairs* (September 28, 2011), available at: *www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.*

attacking a target by making him believe the costs and consequences will outweigh any potential benefits. Therefore, a working definition by the author and perhaps more importantly what it involves and its intended effects may sound something like this:

> "Cyber deterrence is a strategy by which a defending state seeks to maintain the status quo by signaling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor."

With this baseline understanding, it is equally essential to identify the types of deterrence that are available and have been used throughout the course of history. Although there are a myriad iterations and subsets, there are largely two types of deterrence strategies employed by the United States—deterrence by punishment and deterrence by denial.

- **Deterrence by punishment** intimates to an attacker that there will be significant punishment in retaliation for an attack.[3] In this scenario, retaliation need not be limited to specific actions, but can incorporate other means as well, such as kinetic strikes or more diplomatic means such as economic sanctions.[4] An example of deterrence by punishment is the Cold War's mutually assured destruction doctrine wherein the threat of using a nuclear weapon prevented an adversary from using a similar weapon.

  Applying the same principle to cyberspace, deterrence by punishment can take the form of digital actions such as a retaliatory cyber strike against perpetrators of a cyber attack, or a pre-emptive strike against adversary's mounting an attack against networks. However, deterrence by punishment against a cyber attack could also entail kinetic attacks against targets, diplomatic bargaining, or economic sanctions. If one believes that the United States was behind the STUXNET attack that targeted Iranian nuclear centrifuges, this could be perceived as a pre-emptive deterrence by punishment against Iran for continuing to refine its uranium enrichment procedures.

- **Deterrence by denial** is less conflict driven, seeking to convince potential attackers that their effort will not succeed and they will be denied the benefits they seek.[5] The benefit of this strategy is that it may be based on defensive measures and thus not only be a means of preventing the enemy from acting but also providing a solution in case the challenger decides to act.[6] An example of this type of deterrence is the U.S. naval blockade around Cuba in 1962. In this instance, the United States opted to deny entry to Russian ships from entering Cuban waters rather than deploying air strikes against Cuban missile sites.

[3] Jeffrey W. Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats," *World Politics Review* (June 11, 2013), available at: *http://www.worldpoliticsreview.com/articles/13006/use-with-caution-the-value-and-limits-of-deterrence-against-asymmetric-threats.*
[4] Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3:3 (December 2011): 54.
[5] Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats."
[6] Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," 54.

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

> In cyberspace, deterrence by denial assumes a more traditional defensive role by discouraging or frustrating attacks via robust, proactive, and costly defenses. It requires a large, focused commitment by the government to secure the systems and networks under its control, in tandem with the full cooperation of the private owners of the infrastructure.[7] The cost increases significantly given the breadth of this endeavor including the use of advanced security practices and the adoption of trusted hardware and software components.[8]

Necessary Factors for Effective Cyber Deterrence

Cyber deterrence is difficult to execute, as there are several factors that must occur in order to achieve the results of either subset of deterrence strategy. A cyber deterrence strategy must have established parameters from which to operate successfully. Without them, an adversary will not be able to receive and process the defender's intent, which runs the risks of misunderstanding or misinterpreting them, thereby increasing the risk of escalation and quite possibly, that of state on state confrontation.

Communication

Part of any deterrence strategy is to be able to effectively communicate to the international community, and particularly adversaries, on what is acceptable and what are redlines that will be addressed if crossed. In *Arms and Influence*, author Thomas Schelling notes that successful deterrence using either punishment or denial methods depends upon effective communication between a state and the entity it wishes to deter.[9] Working in tandem with communication is the notion of credibility. A nation state must not just pronounce activity it considers crossing redlines, but must be prepared to act as a result of that activity. A nation state risks losing its international credibility when it fails to do this. An example of this occurred in 2012 when President Barack Obama proclaimed that any use of chemical weapons by the Syrian government against its citizenry would result in a crossed redline.[10] However, once intelligence confirmed that chemical weapons had been used six months later, Obama still had not acted to back up his public assertion.[11] By refusing to back up his bold statement, the United States lost some of its credibility. Even after it agreed to supply the Syrian rebels with arms in July 2013, many in the international community viewed this as "too little too late."[12]

In cyberspace, communication assumes an important function given that the domain is one steeped in ambiguity. Effective communication would require a consensus for operating norms of behavior in cyberspace, a difficult endeavor to achieve as evidenced when the United States and China failed to identify common language in the July 2013 Strategic and Economic

---

[7] David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy* 9:5 (September/October 2011): 36-40.
[8] W.K. Clark and P.L. Levin, "Securing the Information Highway," *Foreign Affairs,* Nov./Dec. 2009: 2-10.
[9] Jonathan Solomon, "Cybercdeterrence between Nation States: Plausible Strategy or Pipe Dream?" Strategic Studies Quarterly (Spring 2011): 2.
[10] "Obama Warns Al-Asad Against Chemical Weapons, Declares 'World is Watching,'" *CNN Online*, December 3, 2012, available at: *http://www.cnn.com/2012/12/03/world/meast/syria-civil-war.*
[11] Terrence Burlij and Christina Bellantoni, "Syria Crossed Obama's Redline. What Happens Next?" *PBS Online*, June 14, 2013, available at: *http://www.pbs.org/newshour/rundown/2013/06/administration-sharpens-focus-on-syria-with-chemical-weapons-report.html.*
[12] "Few Satisfied, But U.S. Presses Syrian Arms Effort," *Las Vegas Sun Online*, July 26, 2013, available at: *http://www.lasvegassun.com/news/2013/jul/26/us-obama-aid-to-syria/.*

Dialogue.[13] The United States prefers to use the term "cyber security" to focus on the technologies and networks of automated machines, whereas countries like China and Russia prefer to use the broader term "information security" to include the information resident on or passing through networks as well as the technologies themselves.[14] The key to this discrepancy rests in the activities that occur in cyberspace; China is pursuing a broader interpretation to be able to dictate and control the content and information to which its citizenry has access, whereas the U.S. supports the policy of Internet freedom. As of the second December 2013 meeting of the China - U.S. Cybersecurity Working Group, the two countries remain at an impasse in finding common ground on definition language. Without a common lexicon in place, communication between the two sides is fated to remain in disagreement, failing to achieve consensus on how the Internet should be used appropriately. Similarly, when addressing hostile activities in cyberspace where the actors are foreign to each other, the inability to communicate further impedes the ability to send clear messages and deescalate tensions. The 2001 Council of Europe-led Convention on Cybercrime provides a good framework from which agreed upon terminology can be achieved. The agreement successfully identifies key terminology agreed upon by all signatories. To date, there have been forty-one ratifications/accessions to the Convention. Notably, while listed as a non-member state, Russia has yet to sign or ratify the agreement, and China has not joined indicating their reluctance to accept terminology agreed to by Western States.[15]

Signaling

Signaling game logic has been applied to many areas of international politics in the past decade, including decisions to go to war, crisis bargaining, international economic negotiations, regional integration, and foreign policies of democratic states.[16] Whether in peacetime or war, a key element of any cyber deterrence strategy includes the ability to properly signal intentions to the receiver. Without the ability to signal, cyber deterrence by punishment is rendered ineffective and runs the risk of being misunderstood or misinterpreted, increasing the risk of escalation and conflict. For example, prior to the execution of deterrence by punishment, the defending state must clearly signal its discontent to the aggressor (whether a nation state or non-state actor) in such a way that the aggressor interprets it correctly, understands it, and concludes that the potential costs of undertaking such action far outweigh any potential benefits. However, it should be noted that the signaling nation state must have an established body of work and credibility conducting successful and destructive cyber retaliation for signaling to be effective. If the adversary does not believe the credibility of a signaling nation state or if it flat out does not care, it is immaterial how much signaling is completed. In this case, the aggressor will not be deterred by threat of punishment.

Like communication, signaling in cyberspace can be easily misinterpreted, ignored, or not even noticed by the aggressor. Signaling can be done overtly, covertly, or through diplomatic,

[13] Bill Gertz, "U.S., China Strategic and Economic Dialogue Criticized," *Washington Free Beacon*, July 16, 2013, available at: *http://freebeacon.com/u-s-china-conclude-strategic-and-economic-dialogue-talks/.*
[14] Tim Farnsworth, "China and Russia Submit Cyber Proposal," *Arms Control Association*, November 2011, available at: *http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.*
[15] "Convention on Cybercrime," *Council of Europe*, CETS No. 185, November 25, 2013, available at: *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.*
[16] James Igoe Walsh, "Do States Play Signaling Games?" *Cooperation and Conflict: Journal of the Nordic International Studies Association* 42:4 (2007): 441.

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

economic, or military channels. Take for example the STUXNET incident. If the United States government were responsible for the deployment of STUXNET on Iranian centrifuges, the USG may have signaled to the Iranian government through diplomatic channels that such an action—without revealing the intended target—would transpire if Iran did not cease its enrichment process. Thus, when the centrifuges broke down and were replaced, it would have been clear that United States was behind the event. Another example of potential signaling in cyberspace would be the use of distributed denial-of-service (DDoS) attacks. Continuing with the STUXNET scenario, U.S. banks were targeted by DDoS attacks shortly after the discovery of STUXNET. Many U.S. lawmakers immediately suspected the Iranian government to having conducted or orchestrated the attacks via proxies.[17] If Iran was responsible, prior signaling through diplomatic or third party channels without revealing specific targets would have clearly conveyed to the USG that Iran was not only responding to the STUXNET attack, but also that it had a cyber capability to do so as well.

Attribution

It is extremely difficult to determine attribution in cyberspace where savvy operators have a multitude of obfuscation techniques to thwart defenders from correctly identifying their true point of origin. Whether it's compromising a series of computers in different countries prior to executing attacks, or using anonymizers and proxies, cyberspace is an environment favoring those seeking to conduct surreptitious malicious acts. Attribution is a necessary component of any deterrence strategy as it is incumbent on the defending state to positively attribute an aggressor prior to the commencement of any retaliatory action. However, complete attribution may not be needed to engage in deterrence by denial where other forms of non-destructive actions can be directed against an aggressor. Jason Healey of the Atlantic Council presents a strong case for determining the "spectrum of state responsibility," a tool designed to help analysts with imperfect knowledge assign responsibility for a particular attack, or campaign of attacks, with more precision and transparency.[18] The spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack.[19] The level of attributed nation state culpability would serve as the guide for the type and appropriate level of response ranging from ignoring the initial attack or striking back at the perceived aggressor.

Successful attribution practices in cyberspace will ideally meld technical, cognitive, and behavioral analysis to better identify the aggressors, as well as those influences that may be helping to guide their operations. Technical analysis is not sufficient for attribution purposes, considering many hostile actors implement the same tactics, techniques, and procedures, as well as tools, or engage in "false flag" operations in conducting malicious activity.[20] No standard

[17] Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *The Washington Post*, September 21, 2012, available at: *http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sites-quds-force-cyberattacks.*

[18] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, January 2012, available at: *http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.*

[19] Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks."

[20] Kelly Jackson Higgins, "The Intersection Between Cyberespionage and Cybercrime," *Dark Reading*, June 21, 2012, available at: *http://www.darkreading.com/attacks-breaches/the-intersection-between-cyberespionage/240002514;* Kelly Jackson Higgins, "Attackers Engage in False Flag Attack Manipulation," *Dark*

methodology exists today for establishing a degree of confidence in determining cyber-attribution.[21] When it comes to possibly deploying a cyber deterrence by punishment, the defender must be able to identify the perpetrator for an appropriate response action. Several problems inhibit quick and accurate attribution processes including: misattribution; the time it takes to collect and analyze the attack method employed; and identifying actor motive, behavior, and outside influences. Nevertheless, in order to avoid public embarrassment and reduce the volume and likelihood of collateral damage, an acceptable level of attribution must be performed prior to the commencement of any retaliatory action.

Proportionality

Based on the 1949 Geneva Conventions on the Law of Armed Conflict and the principles of proportionality, as well as those expressed in NATO's recent drafting of the Tallinn Manual advocating cyber war's assimilation into conventional warfare, a retaliatory cyber action needs to be proportional, particularly if leveled against a suspected state or state-sponsored actor. That is, "it must be comparable to the initial wrong and not equate to an escalation."[22] Here, a nation state's credibility is interlinked with proportionality in that the nation state must not only strike back against the aggressor but it must do so in a way as to make its point—that is, it must be a forceful strike—but not so forceful as to solicit negative reaction in the global community. A nation state's credibility on the world stage rests in its ability to back what it says, and be judicious enough to not be perceived as heavy-handed. What is more, it needs to consider unintended consequences as a result of cyber retaliation. Take for example the STUXNET worm used against Iranian nuclear centrifuges. The malware was written to target specific configuration requirements, in this case, the Siemens software resident on the centrifuges. However, despite being surreptitiously inserted and deployed on a non-Internet connected network, the virus did escape, infecting computers in Azerbaijan, Indonesia, India, Pakistan, and the United States.[23] Such outcomes can not only prove detrimental to a nation state's public image, but also risk bringing in third party nation states or politically or ideologically motivated actors into the conflict (e.g., the hacker attacks against U.S. government websites after the accidental bombing of the Chinese Embassy in the then Yugoslavia in 1999 and the initiation of 2001 China - U.S. hacker conflict after the collision of the U.S. spy plane and a Chinese jet).[24]

Proportionality in cyberspace is difficult to achieve for a variety of reasons. It should reflect the commensurate amount of damage done to a target that was suffered by the victim as to mitigate the risk of escalation. Perhaps more importantly, a nation state acting independently of a respected international organization such as the United Nations mandate, it runs the risk of

---

Reading, October 1, 2012, available at: *http://www.darkreading.com/attacks-breaches/attackers-engage-in-false-flag-attack-ma/240008256.*

[21] Emilio Iasiello, "Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills," *National Defense*, December 2012, available at: *http://www.nationaldefensemagazine.org/archive/2012/December/Pages/IdentifyingCyber-AttackerstoRequireHigh-TechSleuthingSkills.aspx.*

[22] Eric Talbon Jensen, "Cyber Deterrence," *Emory International Law Review* 26:2 (2012): 799.

[23] "W32.Stuxnet," *Symantec*, February 26, 2013, available at: *http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.*

[24] Ellen Mesmer, "Kosovo Cyber War Intensifies; Chinese Hackers Targeting U.S. Sites, Government Says," *CNN Online*, May 12, 1999, available at: *http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg/*; Craig S. Smith, "May 6-12: The First World Hacker War," *The New York Times*, May 13, 2001, available at: *http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html.*

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

diplomatic and even economic blowback for its action. Therefore, prior to retaliation, the type of kinetic or non-kinetic response, the promptness of the retaliation, the projected consequences and battle damage assessment, and the potential political fallout should all be factored in the decision making process.

Other Deterrence Strategies

There are other deterrent strategies that have achieved mixed levels of success that can be used to as potential benchmarks for cyber deterrence. In these cases, while there are some shared commonalities such as diverse threat actor landscapes, asymmetric capabilities of defenders and aggressors, and military operations, each have their own unique challenges that can't be assimilated to the cyber environment. A brief examination of nuclear, terrorism, and rogue state deterrence models will serve as comparative paradigms to see if some of the principles that make them successful can be applied to the cyber domain.

Nuclear Deterrence

There is no greater example of a successful deterrent strategy than that demonstrated by the United States and the Soviet Union during the Cold War. At its core, nuclear deterrence was directed at states already armed with nuclear weapons and was aimed at deterring their use.[25] By the early 1970s, the "mutually assured destruction" theory prevailed; neither the United States nor the Soviet Union was motivated, foolish, ignorant, or incoherent to accept the risk of nuclear war.[26] The results of nuclear deterrence have been a resounding achievement, as no nation state since that time has ever deployed a nuclear weapon against a target, as the costs in lives, recovery, international prestige, and natural resources have far outweighed any prospective benefit to using nuclear weapons in any conflict.

But can the principles involved in nuclear deterrence be applied to cyberspace? Widely viewed as an asymmetric power/threat like its nuclear counterpart, the cyber domain is easily translatable into a similar paradigm in certain areas. The below Table highlights key similarities shared between cyber and nuclear deterrence strategies:

Table 1: Key Similarities Between Cyber and Nuclear Conflict[27]

1.	Both operate at all three level of military operations: strategic, operational, and tactical, with the potential to have effects ranging from small- to population-scale.
2.	Both have the capacity to create large-scale, even existentially, destructive effects.
3.	Both can be conducted between nation-states, between a nation-state and non-state actors, or between hybrids involving nation-states and non-state actor proxies.
4.	Both nuclear and cyber conflict "could present the adversary with decisive defeat, negating the need to fight conventional wars."
5.	Both can intentionally or unintentionally cause *cascade effects* beyond the scope of the

[25] Jeffrey Record, "Nuclear Deterrence, Preventative War, and Counterproliferation," *The Cato Institute* 519 (July 8,2004), available at: *http://www.cato.org/sites/cato.org/files/pubs/pdf/pa519.pdf.*
[26] Keith B. Payne and C. Dale Walton, "Deterrence in the Post-Cold War World," *Strategy in the Contemporary World, An Introduction to Strategic Studies*, ed. John Baylis, James Wirtz, Eliot Cohen, and Colins. Gray (New York: Oxford University Press, 2002):169.
[27] Dr. James C. Mulvenon and Dr. Gregory J. Rattray, "Addressing Cyber Instability: Executive Summary," *The Atlantic Council*, July 8,2004, available at: *http://www.acus.org/files/CCSA_Addressing_Cyber_Instability.pdf.*

	original attack target.

However, despite some crossover, there are too many inconsistencies that prevent an even partial adoption of the nuclear deterrence model. These range from the volume of actors operating in cyberspace to the comparison of weapon strength to the dual use nature of the tools themselves.

Key differences include:

- Nation states typically do not assume responsibility for hostile actions taken in cyber space.
- There has been no awe inspiring, game changing show of what a cyber attack can do; while incidents like STUXNET and the wiper malware that destroyed 30,000 hard drives for the Saudi oil company Saudi Aramco were significant disruptions, they were not enough to severely impact operations at either the nuclear facility or the oil company.
- Attribution in cyberspace is extremely difficult and cannot be as precise as identifying a nation state that has launched a nuclear weapon and,
- Unlike nuclear weapons development, which can be monitored, there is no similar transparency for nation state production of cyber weapons, nor an international watchdog agency to track such developments.[28]

Factor in the involvement of proxy groups and third party cutouts, the expanding and borderless nature of the operating environment, and the uncertainty that actors can actually be deterred, and it is evident that the same fundamental transparencies that have made nuclear deterrence a success do not have the same applicability in cyberspace.

Terrorism Deterrence

Several authors believe that terrorism deterrence can succeed on some level, particularly if a terrorist organization assumes the attributes of a nation state, when real assets can be damaged influencing terrorist leadership to constrain its policies in order to preserve them.[29] One author argues that the assassination of top-level leaders and operational commanders have had a temporary deterrent effect, if only to provide a lull time in which these groups have had to reorganize themselves.[30] Another author advocates for deterrence to achieve success against the terrorist target, the threatened party must understand the (implicit or explicit) threat, and decision-making by the adversary must be sufficiently influenced by calculations of costs and benefits.[31] Another author states that even if terrorists are generally not deterrable some specific terrorist actions may be deterrable even today.[32]

Nevertheless, there are far more obstacles to, rather than benefits from, deterring terrorism, many of which are shared by the cyber domain, particularly when it comes to trying to deter a

[28] Iasiello, Emilio, *Cyber Attack: A Dull Tool to Shape Foreign Policy* (Tallinn: NATO CCD COE Publications, May 2013), 398.
[29] Shmuel Bar, "Deterring Terrorists," *Hoover Institution*, June 2, 2008, available at: *http://www.hoover.org/publications/policy-review/article/5674.*
[30] Bar, "Deterring Terrorists."
[31] Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism," *International Security* 30:3 (Winter 2005/2006): 87.
[32] Davis, Paul K. and Brian Michael Jenkins, *Deterrence &Influence in Counterterrorism: A Component in the War on Al Qaeda* (Santa Monica, CA: RAND Corp., 2002), 59.

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

perseverant adversary that does not necessarily reside in one or the same location. How does one deter the activities of an individual or group without knowing who they are or where they reside?

Another factor complicating deterrence efforts is motivation. While the terrorist leadership may value their own lives, groups are full of individuals willing to die for a cause. United Kingdom national security scholar John Gearson suggests that traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so called soldiers seek martyrdom and death and whose most potent protection is statelessness.[33] Upon closer inspection, the first half of Gearson's statement is very applicable toward hostile cyber actors as well. Actors motivated by a cause, whether political, ideological, or financial, are hard pressed to be deterred unless some formative action can cause them significant physical, emotional, or financial impact to curb engagement in further hostile activity in cyberspace.

Another facet challenging a successful deterrence strategy is consistently influencing terrorist behavior. In order to be successful, a direct response deterrent threat must be made conditional on an adversary's behavior; if individuals and political groups believe that they will be targeted as part of the U.S. war on terror regardless of their actions, they have less incentive to show restraint.[34] To date, there have been no publicly observed incidents or evidence where cyber deterrence by denial or punishment has been successfully used to mitigate hostile cyber activity, or influence the actors directing or conducting the activity.

Rogue States

The United States also engages in deterrent strategies against those rogue states that pose a threat to its national security interests. There are cases to be made on both sides of the equation regarding if U.S. policies successfully deter states such as Syria and North Korea. On one hand, there has not been a military conflict between the United States and these adversaries suggesting current deterrence efforts have been a success. On the other hand, these states continue to pursue programs viewed by the U.S. government as hostile regardless of U.S. diplomatic/economic efforts to halt their progress. In its second term, the Bush administration announced a new approach that it called "tailored deterrence" to be leveraged against these rogue states.[35] The basis for this line of reasoning was that different strategies could be crafted for different states and situations, and that the United States would have to learn what regimes valued most in order to develop a deterrent strategy that would most effectively target the psychological profiles of their leaders.[36] However, there are recent anecdotal examples that illustrate why rogue state deterrence is difficult to achieve.

- **North Korea:** In 2013, North Korea conducted its third nuclear test. In response, the United States sent B-52 bombers followed by B-2 stealth bombers on practice flights over South Korea. North Korea responded by increased hostile rhetoric and appeared prepared to launch a test flight of a new missile. Worried about escalating the situation,

[33] John Gearson, "Deterring Conventional Terrorism: From Punishment to Denial and Resilience," *Contemporary Security Policy*, 33:1 (2012): 171.
[34] Matt Kroenig and Barry Pavel, "How to Deter Terrorism," *The Washington Quarterly* 5:2 (Spring 2012): 21.
[35] Knopf, "Use With Caution: The Value and Limits of Deterrence Against Asymmetric Threats."
[36] Ibid.

the U.S. dialed back its comments and military maneuvers.[37] In this instance, deterrent military actions did not reduce tensions between the U.S. and North Korea, and even risked escalating matters to a military conflict.

- **Syria:** In August 2012, in response to Syrian rebels attempting to overthrow the Syrian regime of Bashar al-Assad, President Barack Obama stated that any use of chemical weapons would cross a "red line." The President bolstered these comments in December adding that use of chemical weapons would have "consequences"—bureaucratic-speak for potential kinetic or military responses.[38] However, when the United States failed to act once chemical weapons had been used, the U.S. government lost considerable credibility—a necessary component of a deterrent by punishment strategy.

Potential removal from office is not always a deterrent factor when dealing with rogue nation states run by authoritarian regimes. What is more, the removal of leaders still has not dissuaded other totalitarian leaders from their courses of action. For example, Muammar Gaddafi's besiegement by civil war in 2011 coupled with his ultimate demise with the support of U.S. and NATO material and logistical support has done nothing to convince Syria's al-Assad to step down.

Similarly, nation state operators, mercenary groups for hire, hacktivists, or criminals will likely be undeterred by law enforcement, intelligence, or military engagement. Cyber criminals continue their activities despite several high profile international arrests.[39] Suspected nation state actors continue to engage in cyber espionage despite being called out in public forums.[40] Operation Ababil hacktivists continue to conduct DDoS against U.S. financial institutions for the better part of a year and a half without consequence.[41] Ultimately, trying to apply a rogue state deterrent strategy against the cyber environment may not be a suitable fit, due to the complexity and diversity of the threat actor landscape. Many of these actors do not operate like a rogue state whose ultimate purpose is regime stability and preservation of leadership; as such, these actors do not cherish the same values. Even suspected nation state actors answer to their chain of command and would only stop given the proper instruction from above.

Can Cyber Deterrence Work?

Martin Libicki states, "The goal of cyber deterrence is to reduce the risk of cyber attacks to an acceptable level at an acceptable cost," where the defending nation state mitigates potential offensive action by threatening a potent retaliation.[42] But can such a policy actually be successful? While it is entirely possible that cyber deterrence will not be executed in a vacuum,

[37] Ibid.
[38] Ibid.
[39] "FBI: More Arrests in International Cyber Crime Takedown," *Infosec Island*, July 13, 2012, available at: *http://www.infosecisland.com/blogview/21907-FBI-More-Arrests-in-International-Cyber-Crime-Takedown.html*; James O'Toole, "Global Financial Cybercrime Sting Yields 24 Arrests," *Money CNN Online*, June 26, 2012, available at: *http://money.cnn.com/2012/06/26/technology/cybercrime-arrests/index.htm.*
[40] Steve Ragan, "China's APT 1 Still Operating With the Same Modus Operandi," *Security Week*, May 1, 2013, available at: *http://www.securityweek.com/chinas-apt1-still-operating-same-modus-operandi.*
[41] Tracy Kitten, "DDoS: Attackers Announce Phase 4," *Bank Info Security*, July 23, 2013, available at: *http://www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1.*
[42] Libicki, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corp., 2009), available at: *http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.*

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

in its 2011 *Strategy for Operating in Cyberspace*, the DoD justified the use of active cyber defense measures to prevent intrusions and affect adversary activities on DoD networks and systems.[43] This responsibility, coupled with the disclosure of the once classified Presidential Policy Directive-20 (if this is a legitimate document), indicate that the U.S. can engage in offensive cyber activity to curb an imminent threat, or ongoing attack that do not require prior Presidential approval, suggesting that deterrent cyber actions may be conducted as an isolated effort.[44] Therefore, taken in this context, prior to engaging in a retaliatory strike back option, it is necessary to make some points clear with regards to cyber deterrence. In no way does advocating offensive actions for defensive purposes nullify the need to have an established cyber defense posture. As such, some truths remain:

1. **Traditional Cyber Defenses Still Need to Be in Place**. An argument can be made that a successful "deterrence by punishment" policy would greatly reduce expenditures associated with traditional cyber security to include devices, programs, and the costs associated with upkeep, maintenance, and replacement. However, this is misleading. A deterrence strategy cannot address all of cyberspace's hostile actors. If deterrence is meant to dissuade serious actors such as nation states or the more sophisticated cyber criminals and hacktivists groups, what will stop the majority of other "noise" that targets networks? Jim Lewis, a cyber expert from the Center of Strategic & International Studies, states that "survey data consistently shows that 80-90 percent of successful breaches of corporate networks required only the most basic techniques, and that 96 percent of those could have been avoided if proper security controls were in place."[45] Indeed, the same sentiment was expressed when Australia's Defense Signals Directorate in partnership with the U.S. National Security Agency came up with a list of measures that would mitigate most of the "successful" attacks they had surveyed in 2009 and 2010.[46] Thus, even the most basic computer security practices would still be required in order to achieve maximum cyber defense coverage.

2. **Deterrence by Punishment Relies on the Rationality of Actors**. Deterrence is an option that will work only if the people/groups/government being deterred are rational; and as such, can be deterred because they are unwilling to risk losing something of greater value. Currently, adversaries operate in cyberspace because they do not fear retaliation due to known attribution challenges, and the connected, nebulous, unsecure environment favors their maneuvers. Therefore, a nation state may be more conducive to deterrence than a terrorist or hacktivist organization. If the adversary does not hold a rational view of the world and his place in it, or he does not have anything to lose or be threatened, he may be very difficult to deter from a specific course of action.

3. **The Adversary Must Have Something of Value**. Building on the previous statement, the adversary must have something of value for a pre-emptive/retaliatory strike to be effective. If he doesn't, then the threat of cyber deterrence becomes inconsequential. For

[43] "Strategy for Operating in Cyberspace," *Department of* Defense, June 2011, available at: *http://www.defense.gov/news/d20110714cyber.pdf.*
[44] "Presidential Policy Directive-20," *The White House*, available at: *http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.*
[45] James A. Lewis, "Raising the Bar on Cyber Security," *Center for Strategic & International Studies*, February 12, 2013, available at: *http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf.*
[46] Lewis, "Raising the Bar on Cyber Security."

example, a nation state likely has many assets linked to the Internet or are at least networked. But what if it is a closed state? For example, North Korea has very few online assets connected to the Internet that can be targeted remotely (suggesting that any effective cyber operation against a high value target would have to be conducted via close operations, as was suspected in the STUXNET incident). And if the adversary is a cellular-structured terrorist or hacktivist group dispersed globally, what value point can be leveraged that will have sway over the actions of the entire group?

With these truths in mind, and upon review of current deterrence strategies against other targets, it is evident that cyber deterrence by punishment success rests in three fundamental axioms:

- **Attribution.** It may seem like common sense, but it is essential for a government to know who attacked it before launching any counterattack. But how does one gain reasonable confidence in a domain that thrives on ambiguity? There are so many factors to consider prior to launching a retaliatory strike including but not limited to: the attacker's identity (If linked to a nation state, did the attacker receive orders from above or is he acting alone? If a third party, is it working on behalf of a nation state government or just acting to support it? Is it a false flag operation, why or why not?); motivations for the attack (What prompted the attack? Was it in itself retaliation for something that the targeted nation state did?); and the intention of the attack (Was the intent of the attack to destroy, degrade, deny, or disrupt, or something else? Did the attack have an intended purpose other than what is being seen on the surface?). Also, some things to consider: if the originating attack were viewed as cause-motivated, several states, hackers, or hacktivists would have reasons to having conducted the attack. Even if these third parties were acting on behalf of the state, do you hold the state or the actors responsible? Who exactly is the target – the nation state pulling the strings or the actors conducting the attacks?

  But is attribution enough? When one looks at the amount of governments that have singled out China as the main hacking threat to their nations, little has been done to either stop or deter Chinese cyber espionage. President Obama has had several talks with Chinese counterpart Xi Jinping that has yet to yield any substantive results.[47] While there has been no known U.S. attempt at conducting a retaliatory strike (as of yet) against the Chinese, this goes to prove that attribution is not a panacea, even when directly confronting the alleged perpetrator directly, and that the challenge remains to convince the attacker that he has in fact been caught doing something specific.[48]

- **Repeatability**. Repeatability across many different threat actors is an important facet of cyber deterrence, and one of its biggest questions. Can individual actors, cyber criminal groups, foreign intelligence services, military units all be deterred using the same

[47] Scott Neumann, "Chinese Cyber Hacking Discussed at Obama-Xi Summit," *NPR Online*, June 9, 2013, available at: *http://www.npr.org/blogs/thetwo-way/2013/06/09/190058558/chinese-cyber-hacking-discussed-at-obama-xi-summit;* Lucian Constantin, "The Chinese Hacker Group that Hit the New York Times is Back with Updated Tools," *Computerworld*, August 12, 2013, available at: *http://www.computerworld.com/s/article/9241577/The_Chinese_hacker_group_that_hit_the_N.Y._Times_is_back_with_updated_tools.*

[48] Libicki, "Cyberdeterrence and Cyberwar."

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

strategy? A quick answer is no. Different strategies and applications would have to be applied to different actor targets. For example, how a government might deter a criminal group targeting its defense industrial base may be different than how it might deter an adversarial nation state, or even an allied one, from conducting espionage activity. For many large, well-networked nation states, the cyber threat actors targeting its assets are diverse. Suffice to say, individual actors and smaller, less capable groups (unless working on behalf of an adversarial nation state) are unlikely to be on the end of a retaliatory cyber attack for their activities. However, larger, more sophisticated cyber crime groups, hacktivists, and nation state actors are more primed for retaliation as they generally generate more publicity and cause the most damage. For deterrence by punishment to work effectively, the target needs to understand that the retaliatory action is a direct result of the offending action. If a target fails to understand the retaliation, it may be necessary to repeat the act using stronger, more obvious tactics. However, this runs the risk of misinterpretation by the target, and if the target has failed to understand the retaliatory nature of the cyber attack, it may see such an attack as an originating act. This could quickly escalate the situation into greater cyber conflict.

- **Success**. In the case of cyber deterrence by punishment, there is the tactical objective of either stopping a cyber attack while it's happening, punishing the offenders after it happened, or punishing the offenders prior to them launching an initial attack. In the case of punishing an offender during a cyber attack, the objective would be to get him to stop attacking; in the case of punishing an offender after attack, the objective would be to hurt him so he will not engage in similar activity in the future; and finally, in the case of a pre-emptive strike, the objective would be to again hurt him enough so that he will be deterred from ever engaging in an attack. Tactically, these objectives all have merit, but how will they strategically be viable? In other words, would the battle be won at the expense of losing the war? For example, engaging in a pre-emptive or retaliatory cyber strike presupposes that you have successfully attributed, identified, and reconnoitered the target, presumably, in this case, the computer from which the adversary is operating. While the pre-emptive/retaliatory strike may destroy that computer, the adversary may have ten or fifty more computers from which to keep operating. In this example, can the defending nation believe that they really won the engagement? In another example, if the pre-emptive/retaliatory strike is directed at a different target (e.g., a power grid, a critical infrastructure, etc.), how does the victim state take proportionality into account, especially if the adversary has not even conducted an attack? Furthermore, how does the defending state know that the adversary will understand that the pre-emptive/retaliatory strike is in response to potential, ongoing, or future action, and that the message of deterrence will be received, and accepted? What is more, if the adversary is a nation state, how does one account for potential escalatory actions as a result of a perceived disproportionate retaliatory strike? Martin Libicki points out that:

> "attackers are likely to escalate if they (1) do not believe cyber retaliation is merited; (2) face internal pressures to respond in an obviously painful way; or (3) believe they will lose in a cyber tit-for-tat but can counter in domains where they enjoy superiority."[49]

[49] Ibid.

Conclusion

In cyberspace, the effort to counter hostile acts through use of preemptive or retaliatory strikes may seem like a step in the right direction, especially when considering the failures suffered by network defenders to mitigate the threat of malicious activity. However, thousands of cyber attacks occur per day, suggesting great difficulty in distinguishing serious threats from minor ones.[50] Stepping on an ant in your kitchen doesn't prevent an infestation; similarly, cyber deterrence is not a panacea for threat actors seeking to exploit public and private sector networks. At present, there are too many unexplored variables and an undeveloped plan for its use to make this an effective course of action.

Attribution challenges, the ability to respond quickly, effectively, and accurately, and the ability to create and sustain a model by which repeatability can be leveraged against different threat actors will continue to prove too insurmountable in the near term for victimized countries to launch pre-emptive or retaliatory cyber strikes. Cyber deterrence by denial has a better chance of succeeding; however, only in a limited capacity as network defenders have consistently been beaten by smarter, more agile adversaries obfuscating themselves in cyberspace. Instead of striking back against adversaries, organizations need to evaluate their current security postures to determine its effectiveness in the current cyber climate.

Cyber security is not a static solution; as attackers gain more knowledge and experience, their tactics, techniques, and procedures will morph over time. Defense strategies that worked a year ago will likely not have the same success given the rate at which this landscape changes. According to the Department of Homeland Security's U.S. Computer Emergency Response Team,

> "a comprehensive cyber security program leverages industry standards and best practices to protect systems and detect potential problems along with processes to be informed of current threats and enable timely response and recovery."[51]

Organizations need to implement adaptable security plans that take into account the dynamic aspects of cyberspace, and include milestones and performance measures to ensure that goals are met in a timely manner. Stricter security standards such as vulnerability patching and user awareness must be enacted in order to hold stakeholders accountable for compliance failure. The well respected SANS Institute, a leader in computer security training and certification, advocates the implementation of twenty security controls for cyber defense, and maintains that organizations successfully incorporating these controls have reduced their security risk.[52] Ultimately, due diligence with respect to cyber security is the deciding factor in combating hostile cyber activity.

---

[50] Franklin D. Kramer, "Policy Recommendations for a Strategic Framework," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Dulles, VA: Potomac Books, Inc. and National Defense University Press, 2009), 15.
[51] Eric Byers, "Essential Cyber Security Concepts for CEOs," *Belden*, February 28, 2013, available at: *http://www.belden.com/blog/industrialsecurity/Essential-Cyber-Security-Concepts-for-CEOs.cfm.*
[52] "The Critical Security Controls," *SANS*, available at: *http://www.sans.org/critical-security-controls/.*

https://scholarcommons.usf.edu/jss/vol7/iss1/6
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5