REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-06-2016	FINAL	

4. TITLE AND SUBTITLE

Developing a Conceptual Framework for National Cyber Deterrence and Response

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Eric E. Aslakson (U.S. Army), Commander Lawrence W. Kempista (U.S. Navy)

Paper Advisor: Dr. William Bundy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Gravely Research Group
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Gravely Research Group. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

While much has been written on the difficulties of deterring malicious behavior in cyberspace, there has been a shortage of recommended solutions on bringing together all instruments of national power to counter this malicious behavior. The authors contend that rather than being constrained by unrealistic expectations of near-perfect attribution, the US government should explore a wider spectrum of response options to include more emphasis on soft power when sanctions may not be appropriate. The proposed National Cyber Engagement Framework provides a model of graduated deterrence (ranging from deterrence by agreement, through deterrence by sanction, to deterrence by denial of objective) and compellence measures which can be tailored to the severity of the threat and nature of the actor. Although the higher end of possible response options such as trade embargoes or kinetic attack may be perceived as too escalatory, the authors argue that if the US government continues to under-respond to cyber threats, it will fail to take the initiative in establishing and reinforcing norms of responsible behavior in cyberspace. This balance of graduated deterrence and tailored compellence response options holds the best long-term prospect of reducing malicious behavior in cyberspace. While technical advances in the area of active defense will also help in these efforts, it is expected that such improvements will be evolutionary rather than revolutionary in nature, leaving cyberspace as offense-dominant for the near-term.

15. SUBJECT TERMS

Cyberspace, Cybersecurity, Cyber Deterrence, Cyber Compellence, Attribution, Deception Operations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director, Gravely Research Group
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		33	19b. TELEPHONE NUMBER *(include area code)* 401-841-2660

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Developing a Conceptual Framework for National Cyber Deterrence and Response

by

Eric E. Aslakson, Colonel, U.S. Army

Lawrence W. Kempista, Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Gravely Research Group.

The contents of this paper reflect the personal views of the authors and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____ **Signature:** _____

01 June 2016

Contents

Abstract

While much has been written on the difficulties of deterring malicious behavior in cyberspace, there has been a shortage of recommended solutions on bringing together all instruments of national power to counter this malicious behavior. The authors contend that rather than being constrained by unrealistic expectations of near-perfect attribution, the US government should explore a wider spectrum of response options to include more emphasis on soft power when sanctions may not be appropriate. The proposed National Cyber Engagement Framework provides a model of graduated deterrence (ranging from deterrence by agreement, through deterrence by sanction, to deterrence by denial of objective) and compellence measures which can be tailored to the severity of the threat and nature of the actor. Although the higher end of possible response options such as trade embargoes or kinetic attack may be perceived as too escalatory, the authors argue that if the US government continues to under-respond to cyber threats, it will fail to take the initiative in establishing and reinforcing norms of responsible behavior in cyberspace. This balance of graduated deterrence and tailored compellence response options holds the best long-term prospect of reducing malicious behavior in cyberspace. While technical advances in the area of active defense will also help in these efforts, it is expected that such improvements will be evolutionary rather than revolutionary in nature, leaving cyberspace as offense-dominant for the near-term.

Introduction

Simply stated, it is the responsibility of the US government (USG) to protect its national interests in cyberspace. These interests are articulated in current US cybersecurity strategies and include international work to "promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[1] It follows then that the USG must develop a strategy to counter threats to these interests in cyberspace, preferably by leveraging the effective use of all instruments of national power. The purpose of this paper is to propose a new conceptual framework, the National Cyber Engagement Framework (NCEF), to help implement a national cybersecurity strategy by shaping USG policy and response to future malicious cyber activity.[2]

The authors readily acknowledge the unique challenges posed, and opportunities offered, by the proliferation of information and communications technologies. Unfortunately, much of the published literature on countering malicious cyber activity dedicates far more time and effort to detailing problems of national cybersecurity than it does to finding creative solutions to address these critical threats. For example, two of the most common concerns involve the challenges of deterring non-State actors like the Islamic State that are not bound by international agreements, and the associated difficulty of attributing the actual source of malicious activity for potential tailored response options. Regardless of these technological and policy challenges, it is not an option for the USG to cede cyberspace to adversaries who seek to undermine the

[1] See United States. White House Office, and Barack Obama. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (White House, 2011), 8; see also United States. White House Office, and Barack Obama. *National Security Strategy* (White House, 2015).

[2] This paper will use the expression "malicious cyber activity" to describe any manner of cyber or cyber-enabled activity that poses a threat to US national interests.

international banking system through cyber crime, compromise national defense systems through cyber espionage, or destroy property and potentially kill US citizens through cyber attacks on critical infrastructure.

The NCEF seeks to help address the challenges of national cybersecurity by leveraging the rich traditions of deterrence theory and practice in areas such as nuclear weapons and criminal behavior. However, this paper will not directly compare and contrast these traditions with the evolving field of cyber deterrence theory. That effort tends to distract from the necessary development of a policy framework to address contemporary cyber threats.[3] Further, the use of the term "engagement" in the NCEF is intended to evoke a broad range of interactions within and between governments, private industry, academia, and other appropriate entities to promote, and when necessary, compel responsible behavior in cyberspace.[4] Example engagements will be discussed further in the section on specific deterrence methods.

It is outside the scope of this paper to discuss in the detail the full development of an implementation plan for the NCEF to include the specific interactions of the National Security Council and other federal agencies key to national cybersecurity such as the Department of Justice and the Federal Bureau of Investigation, the Department of Homeland Security, and the Department of Defense. Nor will this paper address potentially required legislative initiatives to ensure proper resourcing and legal authorities. Instead, the paper is focused on providing a conceptual framework for US national policy makers as they further develop necessary policies, strategies, and plans to counter activity in cyberspace that is counter to US national interests.

[3] For example, with nuclear weapons development and proliferation, there is a very high technical and resource cost for entry. Whereas, for malicious cyber capabilities, the technical and resource cost of entry is relatively low. These, among many other differences should be considered, but not prevent the application of deterrence theory to cyber space.

[4] The term "engagement" can also refer to affirmative agreement of arrangement (e.g., marriage) or be used as a synonymous term for a military battle, both of which are perfectly applicable to a framework designed to promote responsible behavior in cyberspace.

Engagement Framework Overview: Deterrence and Compellence

When an actor initially considers the use of cyber-enabled means to conduct activity that the USG could reasonably consider malicious, they are faced with several internal and external factors that shape the decision on whether or not to proceed. If the actor decides not to proceed with the malicious cyber activity, or is thwarted from achieving their ultimate intended objective, that actor was deterred. If the actor decides to conduct malicious cyber activity and achieves some degree of success before discovery, that actor must be compelled to stop that current activity and to discourage similar efforts in the future. This balance of deterrence and compellence forms the heart of the NCEF.

The NCEF uses a target-focused graduated deterrence model that does not rely upon a fixed transition point between deterrence and compellence. Certain targets, such as our nation's critical infrastructure,[5] may warrant protection through the use of sophisticated cyber deception techniques. In this case, a malicious actor may be enticed to continue expending resources on what they mistakenly believe to be successful activity that is actually being manipulated by the cyber defenders to deny the actor their desired objective. Conversely, the Framework utilizes an intent-focused compellence model where the likely intent of the malicious activity will largely determine the nature of the response. It may be difficult to precisely determine the intent of any particular malicious cyber activity, though the type of target selected, and the tools and techniques utilized, may provide essential clues. For example, malicious activity that has the apparent intent of stealing personally identifiable information of national security personnel for

[5] According to the Department of Homeland Security website (http://www.dhs.gov/critical-infrastructure-sectors), there are a total of sixteen critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Also see Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience" (https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil) for further details on US critical infrastructure.

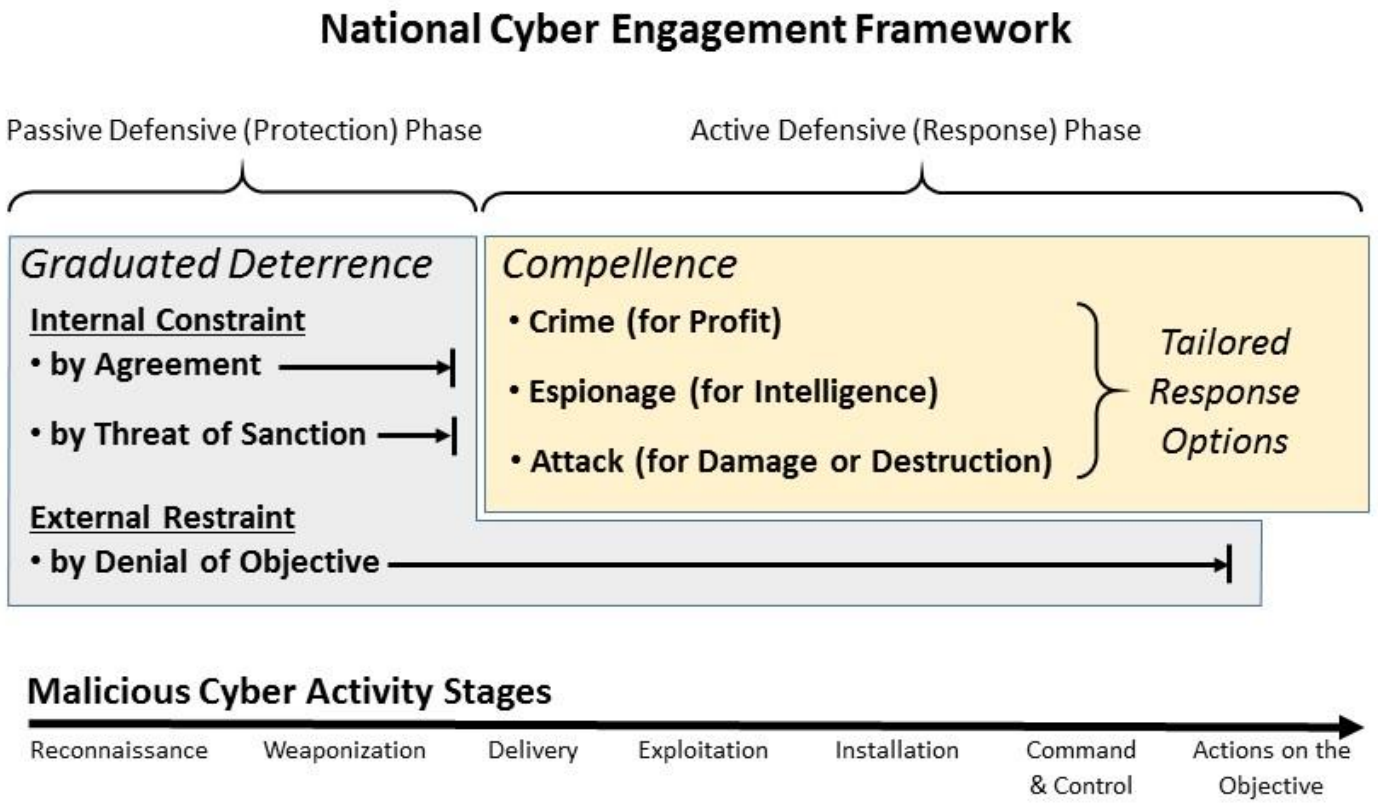
espionage purposes, regardless of specific targeted entity or organization, will warrant a response that is distinct from malicious activity that is targeting the destruction of an urban electric power generation facility.

Figure 1 provides a graphical representation of the NCEF, showing the relationship between deterrence and compellence measures as they relate to the progressive stages of typical malicious cyber activity from initial preparation through successful completion.[6] The Framework uses the concept of graduated deterrence to impose costs over time, and does not rely upon a fixed transition point between deterrence and compellence, particularly as it relates to deterrence by denial of objective.[7] The following sections of the paper will provide a brief overview of deterrence and compellence theory, with descriptions of specific methods of employment for each of these aspects of cyber engagement.

Methods of Deterrence

Academic literature on deterrence theory offers a vast array of different methods to dissuade undesirable behavior, or using national security language, to change the decision calculus of an adversary actor. For the purposes of the NCEF, we will limit our discussion to three basic methods of deterrence most applicable to the cyberspace domain: 1) Deterrence by Agreement, 2) Deterrence by Threat of Sanction, and 3) Deterrence by Denial of Objective. The first two methods of deterrence rely on a measure of internal restraint, where an actor makes a rational determination that the value of the object, or the benefit to be gained, does not outweigh

[6] The framework leverages Lockheed Martin's Cyber Kill Chain methodology to describe the seven stages of typical malicious cyber activity (http://cyber.lockheedmartin.com/solutions/cyber-kill-chain).
[7] Thomas Schelling described graduated deterrence as the progressive process of imposing cost on an adversary over time. This concept has particular applicability to cyberspace deterrence and compellence. See Thomas Schelling, *Arms and Influence* (Greenwood Publishing Group, 1966).



Note: This framework leverages Lockheed Martin's Cyber Kill Chain methodology to describe the stages of typical malicious cyber activity, and at which stage which aspects of deterrence (listed by method) and compellence (listed by intent of the malicious activity) are most appropriate.

Figure 1. National Cyber Engagement Framework

the potential cost of pursuing a given course of action.[8] While the last method, deterrence by denial of objective, relies upon external constraint. In this case, an actor has made the determination to conduct malicious activity in cyberspace but that activity is thwarted prior to successful completion. Each of the three methods of deterring malicious activity in cyberspace will be discussed below within the context of US national security and the NCEF.

Deterrence by Agreement

Deterrence by agreement is a form of deterrence where a State makes a rational determination that it is not in their best interest to directly pursue or otherwise sponsor activity in cyberspace that has the reasonable expectation of being considered malicious or contrary to the national security interests of the USG.[9] In this context, States agree to operate in cyberspace consistent with consensus international norms, rules, and principles, or other binding obligations like treaties. Many factors figure into this demonstration of restraint, such as formal and informal trade arrangements, military exchanges, other entangling or interdependent types of relationships. This method of deterrence, though affirmative by nature, must be underpinned by a credible sanctions regime (see discussion on deterrence by threat of sanction) that can impose sufficient cost upon violations of these norms and agreements.

These agreements are formulated through international bodies such as the Groups of Government Experts (GGE) supported by the United Nations Office for Disarmament Affairs (UNODA). The UNODA is the principle UN office responsible for the promotion of global norms for the disarmament of weapons of mass destruction and select conventional arms such as

[8] The expression "rational determination" refers to some deliberative thought process on the part of the actor. It does not infer any sense of reasonableness or correctness.
[9] This form of deterrence has limited applicability to non-State actors who do not enter into formal State-level agreements or may not be influenced by international norms and practices.

landmines and cluster munitions. Though the UNODA itself does not specifically address illicit behavior in cyberspace, it does provide substantive support to the UN GGE, which was established in 2004 to examine current and future threats in cyberspace and recommend potential cooperative measures to address these threats. The most recent GGE, comprised of twenty Member States to include China, Germany, Russia, and the United States, released a substantive consensus report in July 2015 which detailed principles and norms of responsible behavior of States in cyberspace and examined how international law applies to the State use of communications technologies. Examples of these norms, rules, and principles of responsible State behavior detailed in the July 2015 report include not knowingly allowing sovereign territory to be used for malicious cyber activity that intentionally damages or impairs the use of critical infrastructure that provides services to the public, and not knowingly supporting activity that hinders the activities of another State's cybersecurity incident response teams.[10]

With international cybersecurity agreements, partner States seek to build international cooperation, predictability, and stability through two primary methods: capacity building measures and confidence building measures. Though the terms capacity and confidence building measures sound similar in name, they are distinct in method and purpose. With capacity building measures in cyberspace, the USG wants to improve the capacity of other governments to improve their own cybersecurity and respond to internal threats through various means to include the use of internal law enforcement and military agencies. This improvement can happen in many different ways to include the exchange of cyber security best practices and

[10] See United Nation's 2015 Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174). Also see May 2015 Senate testimony of Christopher Painter, US Department of State Coordinator for Cyber Issues, entitled "Cybersecurity: Setting the Rules for Responsible Global Behavior," (http://www.state.gov/s/cyberissues/releasesandremarks/243801.htm) for further details on USG efforts in this area.

cooperative training exchanges. Whereas, with confidence building measures, the USG wants to assure international partners in the strength and viability of the partnership and reduce misperceptions through such activities as the transparent exchange of cyber threat intelligence and the strengthening of relationships between State-level cybersecurity agencies.[11] Further, international agreements, similar to the nuclear weapons non-proliferation agreements, may be leveraged to reduce the proliferation of technologies that support the most egregious forms of malicious activity in cyberspace or induce widespread vulnerabilities in common cyberspace systems.

Deterrence by Threat of Sanction

Deterrence by threat of sanction, similar to deterrence by agreement, is a form of deterrence in which an actor demonstrates internal restraint by making a rational decision to not pursue malicious activity in cyberspace. However, unlike deterrence by agreement, this form of deterrence does not rely on the positive benefits gained through interstate relationships and agreements. Rather, it relies upon the negative costs imposed through sanction or punishment.[12] Consequently, this form of deterrence is more applicable to non-State actors, many of which flout the concepts of international responsible behavior in cyberspace.

Of the three forms of deterrence in the Framework, deterrence by threat of sanction is most reliant upon the credible and perhaps demonstrated will of the USG to impose sanctions upon malicious actors in cyberspace, particularly if those imposed costs may have reciprocal negative effects upon US interests. The subsequent section of the paper on methods of compellence will discuss sanction actions in more detail, for the tailored response actions

[11] Ibid.
[12] For the purposes of this framework, use of the term "sanction" includes all relevant forms of punishment and retaliation, to include the concept of massive destruction that is prevalent in discussions of nuclear deterrence.

required to compel malicious actors in cyberspace are essentially identical to the threatened sanctions in this method of deterrence. The compellence section will also describe different types of sanctions categorized by instrument of national power, how those sanctions may be selected based on the nature of the malicious activity and certainty of attribution, and how the selected sanctions should be employed to be effective compellence measures.

Deterrence by Denial of Objective

Deterrence by denial of objective is a form of deterrence by external constraint, where a State or non-State actor is determined to pursue malicious cyber activity, but these activities blocked from achieving their ultimate objective. As referenced, the NCEF uses a model of graduated deterrence which combines the more traditional form of deterrence by denial which largely just blocks activity, with a new form of deterrence by denial of objective which harnesses the potential of cyber technology to trick an adversary into believing their malicious activity is successful.

Traditional deterrence by denial is often described as passive, latent, or even static defensive measures. An example of this form of passive deterrence is the use of common access cards by the Department of Defense. In this case, the application of additional identity management measures (a physical card combined with a personal identification number - known as two-factor authentication) has increased the difficulty for cyber aggressors to exploit Department of Defense networks. This imposition by relatively simple methods led to the decrease of intrusions on these networks by more than half.[13]

However, such a categorization of deterrence is incomplete and is becoming obsolete in the modern cyberspace environment. Cyber defenders are increasingly taking more aggressive

[13] Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," *Center for Strategic and International Studies* (December 2008).

postures, generally described as active defensive measures, in order to counter more persistent and capable attackers. Such defensive profiles can take forensic intelligence and apply automated countermeasures that can "interdict, isolate, or remove threat vectors, denying benefit and engaging, deceiving, or stopping adversaries while imposing costs regardless of the source."[14]

Considering the technical nature of cyberspace, and the methods employed to both protect and defend national interests in that domain as briefly described above, it is beneficial to provide a more detailed technical analysis of cyber defense and deception techniques employed in deterrence by denial of objective operations. That discussion will be provided in the Appendix of this paper.

Methods of Compellence

Thomas Schelling, in his influential work *Arms and Influence*, written during the height of 1960's Cold War conflict, described compellence as the offensive complement to deterrence. He said compellence is about "inducing [an enemy] withdrawal, or his acquiescence, or his collaboration by an action that threatens to hurt."[15] Schelling also described specific aspects of compellence strategy (proportionality and duration) that are important to consider for active defensive measures in cyberspace which will be discussed in more detail below. For example, compellence measures are not simply designed to punish successful malicious activity. They must be calibrated in proportionality (i.e., severity) and duration to properly induce an adversary to stop successful activity. Response actions that are disproportionate to the original activity, or cannot be terminated when the adversary ceases the offending malicious activity, may be

[14] Scott Jasper, "Deterring Malicious Behavior in Cyberspace," *Strategic Studies Quarterly* (Spring 2015).
[15] Schelling, 79-80.

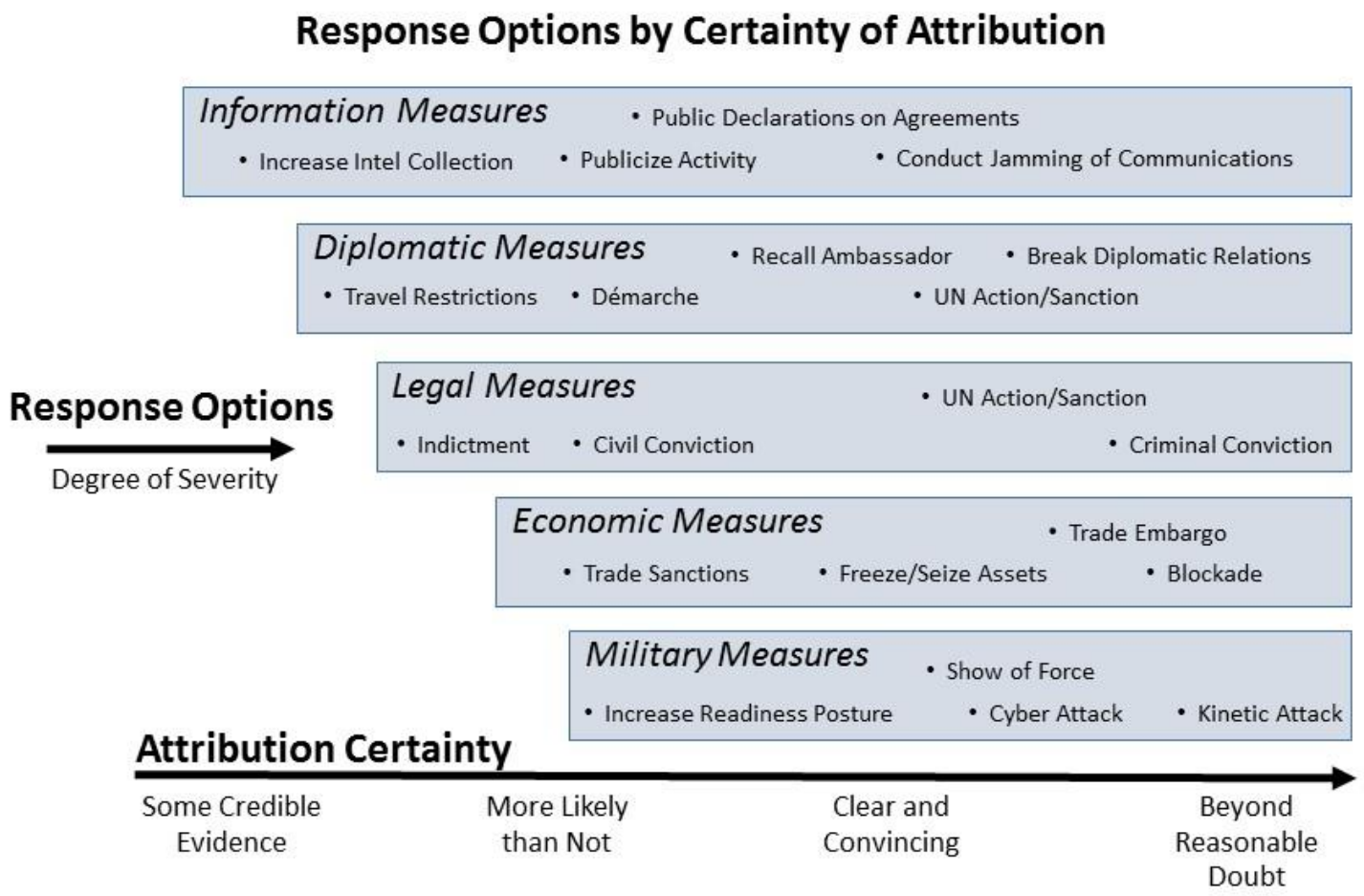
considered capricious and undermine the validity of the response action in the eyes of the international community.[16]

For the NCEF, specific compellence methods or response actions are selected based on the nature of the malicious activity and certainty of attribution, and categorized by instrument of national power. Figure 2 (Response Options by Certainty of Attribution) provides a graphical representation of that process. These actions will be discussed in more detail in the section of the paper on the challenges of attribution. At this point, it is important to describe different types of malicious activity and how those distinctions inform the selection of appropriate response actions.[17]

Malicious cyber activity falls into three broad categories for the purposes of this discussion: cyber crime, cyber espionage, and cyber attack. A given activity is binned into one of these categories based on the intent of the actor, and it is this intent, as far as it can be determined, that will shape tailored response actions. For example, using cyber-enabled network intrusion to steal personally identifiable information (identity theft) in order to file fraudulent tax returns for tax refund theft is cyber crime. Using cyber-enabled network intrusion to steal plans for new weapons systems (intellectual property theft) to enable a State adversary to develop weapon counter-measures is cyber espionage. Using cyber-enabled network intrusion to implant

[16] See Forrest Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," *4th International Conference on Cyber Conflict* (2012) (https://ccdcoe.org/cycon/2012/proceedings/d2r1s2_hare.pdf) for further discussion on compellence in cyber conflict.

[17] For example, many lower-level denial-of-service and phishing attacks can be successfully prevented through current anti-spoofing technologies and appropriate training for computer users. See Dorothy Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 2 (April 2015) (http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf) for further examples of tailored response actions in cyberspace



Note: Not intended to provide an exhaustive list of response options, but to be illustrative of a framework that associates severity of response options with degree of attribution certainty, leveraging common terminology from legal standards for burden of proof.

Figure 2. Response Options by Certainty of Attribution

malware that will physically destroy electrical components to disable a national power grid preceding a military ground invasion is cyber attack.[18]

Figure 2 depicts a wide range of responses available to a State to counter a cyber aggressor who has committed malicious activity in cyberspace. The first key point is that as cyber attacks will not be deterred solely through defensive measures in cyberspace, a State must make available all instruments of national power to create flexible and tailored responses for a given threat. Within each of these instruments lies numerous actions that can be escalated or drawn down based on the adversary's behavior. Secondly, by recognizing that the current standards of nearly incontrovertible attribution are incredibly limiting, a State can open up areas of interaction along "softer" lines of operation. While high burdens of proof are certainly appropriate for military responses, particularly during peacetime, the same hurdle is not necessary to conduct informational campaigns or apply diplomatic pressure. The challenge therefore lies in the ability of the interagency to coordinate these actions to maintain consistency and deliver appropriate signaling to begin to reverse the alarming trend of cyber attacks.

An example scenario would be a State that detects a cyber attack in progress against non-critical but important infrastructure, and is able to apply technical countermeasures to deny the attacker's objectives. Although the attack was unsuccessful, the State deems that the activity is worthy of response to deter further action against more valuable targets. Initially, the state has some positive indications of the country of origin, but the lacks sufficient proof to make a certain case. Understanding that punitive measures may be viewed as unacceptable, the State turns to the information domain and increases intelligence collection against the adversary to improve

[18] The Tallin Manual defines a cyber attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." See Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (London: Cambridge University Press, 2013), 106.

attribution, while also opening diplomatic lines to express that such activity will not be tolerated. As attribution improves, these actions move can move from private to public, with statements supporting cyber security agreements and denouncing aggressive actions and the States that conduct or support them. If the activity continues to escalate and the actor shows no sign of ceasing the unwanted behavior, legal actions either against the individual or the State can come into play, with the goal of setting an example for the establishment of cyber norms of behavior. Beyond this point, tensions will likely spill over into other domains, and the defending State may take economic measures such as freezing assets or applying sanctions, or begin to make overtures that a military response may be required.

While these actions provide escalatory responses that signal the State's willingness to defend its critical cyber infrastructure, it is important not to devolve into a posture of pure brinksmanship. A State must remain fully ready to de-escalate once the attacker's actions cease to be threatening. The resumption of normal behavior is critical to establishing deterrence by clarifying the boundaries of acceptable behavior. Such a strategy may not generate immediate results in the reduction of cyber attacks, but over time we believe that only through consistent and patient enforcement of appropriate behavior can we establish and reinforce cyberspace norms between States. It took three decades for States to begin to make serious negotiations for the control of nuclear weapons; it's time we begin to look at cyberspace in the similar manner.

Challenges of Attribution

The concept of attribution is an albatross hanging around the neck of the broader dialogue on the practicality of deterring malicious activity in cyberspace.[19] This challenge is reflected in two primary ways. First, the frequent use of attribution adjectives like "conclusive," "definitive," and "incontrovertible" in cyber deterrence literature creates an unnecessarily high expectation of proof for positive attribution. Second, attribution is often considered an essential component of cyber deterrence, which it is not. As discussed earlier, deterrence is frequently conflated with compellence. Some degree attribution is necessary for tailored response options at the heart of any cyber compellence strategy. Whereas, with deterrence, attribution is obviously irrelevant for malicious cyber activity that was deterred by agreement or the threat of sanction. It only becomes necessary in the more sophisticated and tailored deterrence by denial of objective deception operations.

Instead, a more productive approach to attribution in cyberspace is to consider the determination of attribution not as a binary choice but as a decision along a sliding scale of certainty. We can borrow terminology and concepts from the legal standards for the burden of proof, such as clear and convincing evidence, to help provide a common frame of reference.[20] Figure 2 provides an example attribution certainty scale along the bottom arrow, from "some credible evidence" on the left side of the arrow to "beyond a reasonable doubt" on the right.

[19] Attribution, or the positive identification of those responsible for any particular cyber activity, is complicated by many factors to include the pervasive use of technologies to anonymize identities and locations on the Internet. However, some authors such as Eric Sterner are optimistic that the challenge of positively attributing activity in cyberspace is trending positive. Technical tools for identifying the sources of cyber attacks continue to improve, as does the quality and availability of computer forensic evidence. This has enabled better development, profiling, and tracking of persistent cyber threats. See Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly* 5, no. 1 (2011).

[20] See Cornell University Law School's Legal Information Institute legal dictionary (https://www.law.cornell.edu/wex) for detailed definitions of the terms used.

Figure 2 also addresses the second challenge listed above, by linking compellence response options (associated with their appropriate instrument of nation power) to attribution certainty. Further, the sample response options are listed by progressive severity. The more certain the attribution, the more severe the potential response option. For example, a cyber attack against a US nuclear facility (critical infrastructure) that is attributed beyond a reasonable doubt to a particular State-level actor may warrant a proportional kinetic military strike in response. Whereas, if there was only some credible evidence for positive attribution in that cyber attack, the USG must limit the severity of the response, but they still could respond.

Implications of Attribution, Credibility, and Proportionality

There are notable precautions to consider when determining response actions under this compellence model for a particular cyber incident. The line in which a defender crosses into what may be viewed as an unacceptable action is often not clear, and can vary significantly based on how aggressive the malicious actor is judged. Iasiello warns us that the trend towards active cyber defense that employs offensive actions to punish the adversary are not practical in the current environment. In addition to the challenges of attribution to an actor or State, the technical difficulties of achieving a truly proportional result to halt current and deter future activity presents numerous complications. The attacker's ability to use multiple computers, the risk of collateral damage, and the potential for friendly fire present too many uncontrollable variables that inhibit a State's capability to provide deterrence by sanction. Instead, he prefers a middle ground denoted as "aggressive defense" which based on mitigating intrusions through

denial and deception as the most practical courses of action until cyber power "can be leveraged as a means of détente."[21]

In their argument for moving away from deterrence and towards a war-fighting posture in cyberspace, Harknett, Callaghan, and Kauffman attest that as the confidence of an attacker in remaining anonymous is raised, deterrence becomes weaker. Even once the technical challenge of attribution is achieved, the attacker still must be convinced that a retribution can be inflicted. If tailored responses are required to achieve deterrence, and most contend that they are, the ability to prepare against all possible scenarios is severely undermined as long cyber aggressors can "cover their attacks with ease and concealment."[22] Therefore, while robust defense is certainly desirable, due to the current offense-dominant nature of cyberspace it will be eventually undermined by a determined attacker, leading to the need for counteraction supported by effective attribution technologies.

Some authors such as Lindsay instead make the counter-argument that events like Stuxnet actually more clearly demonstrate the weaknesses of cyber aggression instead of heralding a new age of vulnerabilities. In acknowledging that the general trend in thought is that cyberspace gives asymmetric advantages to militarily weaker actors that can undermine deterrence, the empirical facts indicate an opposite interpretation. As long as cyber weaponization remains sufficiently complex and social uncertainties hinder bold State actions in cyberspace, defense will be the more feasible option to pursue. Lindsay runs counter to most current views on the scale of threats in cyberspace by observing that despite growing complexity, cyber warfare will generally "fill out the lower end of adversarial interaction" and "prove to be a

[21] Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters* (2014) http://works.bepress.com/emilio_iasiello/5/.
[22] Richard Harknett et al., "Leaving Deterrence Behind: War-Fighting and National Cybersecurity." *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010).

temperamental and unreliable strategic instrument on its own."[23] Interestingly enough, although these views depart from the general consensus, his argument still ends up supporting the concept that deterrence by denial of objective is still the best course to pursue for the immediate future.

While also lamenting the difficulties in attribution, Trujillo contends that another major barrier to the achievement of cyber deterrence lies in the credibility of the defender. While the US has preeminent offensive capabilities in cyberspace, it is unable to effectively deter attacks without worthy demonstration. Deterrence therefore is reliant on at least a minimal level of action in order to remain credible. The challenge thus lies in the fact that unlike kinetic weapons, once cyber weapons such as Stuxnet are used they become available for analysis and modification for others. Furthermore, predictions on the resulting consequences of a cyber attack remain difficult, complicating the determination of a proportional response to aggression.[24]

Jensen discusses at length the legal challenges of ensuring proportionality in cyber attacks. Using the Geneva Convention as a basis, he explores the "constant-care" duty of military commanders to spare the civilian population from the effects of military operations. Extending this concept to cyberspace would seem to put perhaps unrealistic burdens on a commander using a cyber weapon to include constantly maintaining situational awareness, oversight of the cyber tool, and the ability to adjust course at any sign of illegal impact.

Furthermore, while assessment of the indirect effects of a kinetic weapon have improved significantly in the era of precision strike, predicting second and third-order effects from a cyber attack have proven exceptionally difficult if not impossible to predict. He goes on to assess that one of the main difficulties is that the segregation of military and civilian targets has previously

[23] Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, No. 3 (August 2013), 365–404.
[24] Clorinda Trujillo, "The Limits of Cyberspace Deterrence" *Joint Force Quarterly* 75 (4Q 2014).

been thought of in a geographic sense, and there are obvious challenges when applying similar language to the virtual and often dual-use nature of cyberspace. His analysis demonstrates the ongoing technical challenges in not only developing potent cyber weapons, but the responsibilities of the commander in understanding as well as possible their potential impacts prior to their implementation.[25]

Conclusion

As has been demonstrated, the road to successful deterrence in cyberspace will be long and difficult, but advancements in policy will be critical towards achieving that goal. A spectrum of responses across all instruments of power must be coordinated and implemented in a proportional manner to the certainty of attribution. Active defense, which blends the principles of denial of objective with tailored elements of retribution, will be the necessary posture in order to establish and reinforce norms in cyberspace. As the boundaries of appropriate behavior are signaled, clarified, and upheld over time, cyber agreements will increase in strength, locking in the gains achieved through technical and policy advancements.

For the short term, however, offense has the advantage over defense, and this trend is not expected to shift in the near future. The increasing opportunities for vulnerabilities in our ever-increasingly connected society combined with the low cost of entry and relative anonymity of a potential cyber aggressor will ensure that at a minimum at least low-level attacks will continue with regularity. Given that the original concept and structure of the internet promoted freedom and openness, it has taken decades for States to slowly build a primitive version of "cyber

[25] Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack" *International Legal Studies* 198 (2013). http://dx.doi.org/10.2139/ssrn.2154938.

Westphalia" that has some respect for limited borders and security. Further efforts will continue the arms race between attacker and defender, but a game-changing revolutionary leap is unlikely.

Finally, the technical difficulties of attribution and proportionality will keep deterrence by denial of objective the foremost option for investment for the expected future. As attribution becomes more certain, and cyber weapons are tailored and predictable enough for targeted action, the options of limited retribution in a framework of graduated deterrence become practical. We should not expect, however, that attribution and proportionality will ever reach the clarity achieved in our more successful applications of nuclear deterrence. For now, such examples may provide us with the grammar for framing the discussion, but we must write the rest of the story.

Appendix

Of all the specific aspects of the NCEF discussed in this paper, including concepts of graduated deterrence and compellence inspired from nuclear deterrence strategy, perhaps the concept most worthy of further detailed technical discussion is that of deterrence by denial of objective. This appendix will provide technical background information to better explain how sophisticated cyber defensive operations can prevent successful malicious cyber activity through various measures to include cyber deception.

Cyber Deception

Cybersecurity authors, such as Sickles and Grahn, see the rising volume and sophistication of deceptive techniques employed in malicious cyber activity and propose to "fight fire with fire." They cite the Allied invasion on D-Day in 1945 to provide an analogy of success through the use of deception. They offer seven ways to security defenders employ deception efforts including concealment to misdirect attacker's efforts, camouflage to obscure infrastructure, disinformation to present false successes or errors, displays to delay attacker's efforts on false targets, ruses to declare honeypots that are actually fake to deter efforts nearby, and insights to better understand threat trends in order to maximize a deception strategy. The key vulnerability to applying successful deception efforts is that a single mistake can destroy the illusion, thereby quickly invalidating the investment in design and construction efforts. Therefore, execution of deception strategy must be carefully considered beforehand and consistently monitored and updated to present credible targets to increasingly sophisticated attackers.[26]

[26] Matthew Sickels and Anne Grahn, "7 Ways to Deceive Cyber Attackers," *Forsythe Focus* (August 19, 2014), accessed May 24, 2016. http://focus.forsythe.com/articles/337/7-Ways-to-Deceive-Cyber-Attackers.

Crandall describes how modern deception technologies are less reliant on knowledge of threat patterns, and instead use advanced luring techniques to keep attackers off-guard. She argues that a "prevention only strategy" is no longer sufficient, but that security teams "must go on the offensive" by creating environments with continuous, real-time detection. Dynamic deception conducted through Deception Engagement Servers is the next step up from honeypots/honeynets, providing a potentially efficient solution to capitalize on continuous detection by implementing high interaction traps and luring techniques that are not reliant on additional manpower, a major concern for the Department of Defense as it struggles to fully staff its cyber workforce.[27]

Higgins also expands on the necessary shift from passive-only defense to active defense. This active defense still employs the concepts of deterrence by denial by identifying and frustrating attacks, but goes further in interfering with reconnaissance and pinpointing the attacker's location to contribute to attribution. A network of virtualized decoys, similar to a honeynet, can provide an infinite set of dynamically generated pages, delaying attackers and forcing them to take more and more steps to breach security.[28]

[27] Carolyn Crandall, "The Ins and Outs of Deception for Cyber Security." *Network World* (January 06, 2016), accessed May 24, 2016. http://www.networkworld.com/article/3019760/network-security/the-ins-and-outs-of-deception-for-cyber-security.html.
[28] Kelly Jackson Higgins, "Free 'Active Defense' Tools Emerge." *Dark Reading* (July 11, 2013), accessed May 24, 2016. http://www.darkreading.com/attacks-breaches/free-active-defense-tools-emerge/d/d-id/1140109.

Technical Aspects of Cyber Defense

Hutchins et al., present perhaps the best case in describing the evolution of cyber defense against increasingly potent threats.[29] As well-resourced and trained adversaries, known as advanced persistent threats, implement multi-year malicious intrusion campaigns, it is becoming more important to view the battlefield not only in technical terms, but as a contest for information superiority. By closely mapping and studying the cyber kill chain, a defender can

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Table 1. Technical Cyber Defensive Measures by Information Operations Capability and Phase of Cyber Activity

employ an intelligence-based approach in order to plan successive courses of action.

Table 1 (Technical Cyber Defensive Measures by Information Operations Capability and Phase of Cyber Activity) combines the phases of the proposed cyber kill chain model with

[29] Eric Hutchins et al., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," (http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf)

various military information operations capabilities available to a military commander.[30] The intersection of these axes describes a specific cyber technique that can cause the intended effect. A further description of each capability follows.

Intrusion Detection Systems (IDS)

Host Intrusion Detection System (HIDS) includes anti-threat applications such as firewalls, anti-virus software, and spyware-detection programs. These agents are broadly installed across an entire network on each terminal that is allowed two-way access to the outside. They provide strictly passive monitoring and alerting on local OS and application activity, using a "combination of signatures, rules, and heuristics to identify anomalous activity."[31] Network Intrusion Detection System (NIDS) is similar in concept to HIDS in its use of anti-threat software to detect patterns of malicious activity. These systems differ in location, however, as they are instead installed at specific nodes to monitor network traffic. Network traffic can then be monitored through system functions within hardware such as switchports, or by the use of a separate network tap.[32]

Intrusion Prevention Systems (IPS)

Whereas IDS provide a passive means to inform security personnel upon the identification of a potential attack, Intrusion Prevention System (IPS) makes attempts to stop the activity. These efforts may range from simply denying the offending packets, up to rewriting the packet to ensure the hacking attempt fails while marking the event for evidence against the attacker. Similarly to IDS, IPS can be employed on a host or network basis (HIPS/NIPS), with

[30] See Joint Publication 3-10, Information Operations (2014) (http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf) for detailed information on information operations capabilities.
[31] "IDFAQ: What Is Intrusion Detection?" SANS. Accessed May 25, 2016. https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1.
[32] Margaret Rouse and Rebecca Jaeger. "What Is HIDS/NIDS (Host Intrusion Detection Systems and Network Intrusion Detection Systems)?" Accessed May 25, 2016. http://searchsecurity.techtarget.com/definition/HIDS-NIDS.

greater security potential available to the dispersed nature of host-based deployment, but at significantly increased installation and maintenance costs. While IPS is the newer technology and more capable technology, it is likely that IDS and IPS will continue to provide passive and active monitoring options to cyber defenders.[33]

Access Control Lists (ACL)

Access Control Lists and firewalls are tools that permit or restrict data flows into and out of a network. ACLs provide a basic level of security that are best suited to high speed interfaces where heavy restriction is not tolerable. Firewalls provide additional services such as stateful packet inspection, which "improve on the functions of packet filters by tracking the State of connections and blocking packets that deviate from the expected State."[34] These two technologies can be combined to provide a DMZ, or demilitarized buffer zone; in this example, the external router could be secured with more permissive ACLs that allow greater access to the outside. The internal router could then be equipped with a more restrictive firewall to provide greater security to the internal network from threats.[35]

Audit Logs

Audit logs are used by network administrators to determine "where visitors are coming from, how often they return, and how they navigate through" a site or network. They will generally consist of user logins, source addresses, destination addresses, resources accessed, and timestamps. Regular review of inbound information can help detect a variety of unwanted

[33] Vangie Beal, "Intrusion Detection (IDS) and Prevention (IPS) Systems." Webopedia.com. Accessed May 25, 2016. http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp.

[34] Karen Kent and Paul Hoffman. *Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology* (Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology) 2008.

[35] Wilson, Tracey. "Securing Networks: Access Control List (ACL) Concepts." Securing Networks: Access Control List (ACL) Concepts. May 16, 2012. Accessed May 25, 2016. https://www.pluralsight.com/blog/it-ops/access-control-list-concepts.

activity including account access attempts, port scans, and malformed requests. Outbound monitoring can be a key indicator of a compromised terminal on the network.[36] Although audit logs are reactive in nature, detecting malicious activity after it has already bypassed other measures, they are certainly not without important use in a defense-in-depth approach. While one of the challenging aspects of countering cyber weapons is their ability to be deployed nearly instantaneously, they often generate the greatest effect on extended timelines after employment, either in continued exfiltration of data or in lying dormant waiting for activation to achieve a catastrophic effect. Audit logs are therefore a key element of system hardening by continually assessing the health of the network. The challenge lies in properly managing the resources devoted to this effort, as "device logs can be one of the most helpful tools infosec pros have, or they can be a huge waste of space."[37]

Change Root (chroot)

The change root function is a way to run processes off of a different root directory. A chroot jail utilizes this function to create an artificial root directory that prevents access to files outside of it. This can be done for both internal control measures (limiting access to the root for only processes that require it) and as a defensive measure against intruders attempting to conduct malicious behavior. For a chroot jail to be successful, it must have a copy of all the binaries and libraries necessary for a user's needs, so that authorized processes can be run while "limiting the exposure of untrusted processes within a system"[38]

[36] "UC Davis Cyber-Safety Program: Audit Logs | Security." UC Davis Cyber-Safety Program: Audit Logs | Security. Accessed May 25, 2016. https://security.ucdavis.edu/auditlogs.html.
[37] Cobb, Michael. "Best Practices for Audit, Log Review for IT Security Investigations." *Computer Weekly*. Accessed May 25, 2016. http://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations.
[38] "3.13 Configuring and Using Chroot Jails." Oracle LinuxSecurity Guide for Release 6. Accessed May 25, 2016. https://docs.oracle.com/cd/E37670_01/E36387/html/ol_cj_sec.html.

Proxy Firewalls

A proxy firewall acts as an intermediary between in-house clients and servers on the Internet, filtering messages at the application level. It determines what traffic is allowed or denied, while also employing stateful inspection and deep packet inspection on incoming traffic to provide indications of a potential attack. Unlike previously mentioned firewalls, a proxy firewall has its own IP address, which ensures that an outside network connection will never receive packets from the sending network directly. While this additional connection for all inbound and outbound traffic provides a significant level of security, it also runs the risk of becoming a bottleneck that slows performance as well as a potential single point of failure.[39]

Security Patches

Patches are simply security updates within the cyber world. When a product is determined to have bugs that effect performance or weaknesses that can be exploited, a developer can release patches that correct the vulnerability. The patches must then in turn be installed across the effected products by local administrators. Knowledge of such vulnerabilities are critical currency in a malicious actor's capability to conduct operations, making the creation and installation of patches to close holes a key aspect of cyber defense for developers and network administrators alike.[40]

Anti-Virus (AV) Software

Most anti-virus software scans files after they either enter a mail server or infect a terminal. Inline anti-virus software can scan messages as they arrive and stop malicious software

[39] Margaret Rouse and Sharon Shea. "Proxy Firewall." SearchSecurity. Accessed May 25, 2016. http://searchsecurity.techtarget.com/definition/proxy-firewall.

[40] "What Are Security Patches and Why Are They Important? | Cybersecurity | Articles | ID Theft Blog." Identity Theft Resource Center. June 24, 2013. Accessed May 25, 2016. http://www.idtheftcenter.org/Cybersecurity/what-are-security-patches-and-why-are-they-important.html.

by refusing to accept the offending email and its attachments. Like most other cyber defense options, there are tradeoffs in speed and performance, but these are potentially offset by the mitigation of threats that would create greater impact. One hybrid solution offered by some products is to scan incoming files through a buffer in parallel, which would allow a nearly-complete stream to continue to the user, but the small remainder required for execution would not be released until the file has passed the scan.[41]

Data Execution Prevention (DEP)

Data Execution Prevention includes hardware and software that performs "additional checks on memory to help prevent malicious code from running on a system." This is primarily through the prevention of code execution from non-typical locations such as data pages including the default heap, stack, and memory pools. When it encounters code running from these locations, it will raise an exception to stop the process. This is a counter to a class of attacks that attempts to "insert and run code from non-executable memory locations"[42]

Tarpits

A Tarpit is a measure to slow down and delay incoming connections. A server that has identified unwanted connection will stop it from processing while still maintaining connection; approved new users and requests are allowed access in its place. This can be used to inhibit spamming by prohibiting the propagation of mass messages through a mail server, stop unwanted port scans, or interdict command and control functions from malicious actors. The use of tarpits, along with other deception efforts, can provide deterrence by exhibiting strength that

[41] Joel Snyder, "Achieving Network Security with Tomorrow's Antivirus Tools." SearchSecurity. Accessed May 25, 2016. http://searchsecurity.techtarget.com/feature/Achieving-network-security-with-tomorrows-antivirus-tools.
[42] "A Detailed Description of the Data Execution Prevention (DEP) Feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003." Microsoft. Accessed May 25, 2016. https://support.microsoft.com/en-us/kb/875352.

convinces attackers to seek easier targets. (Heckman, 197) For application to our model, such implementation would be most useful in protecting information deemed of higher sensitivity such as critical infrastructure, as such measure would deter efforts against that particular target through exhaustion or frustration, but not necessarily deter the attackers' will to persist against other targets.[43]

Honeypots

Unlike tarpits that seek to delay and halt unwanted actions, honeypots attempt to seduce cyber aggressors into expending effort against either certain low-risk real servers, or sophisticated decoy servers. A designated real server used in this fashion would be classified as high interaction honeypot, which allows the attacker significant control in order to track what they attempt. A low interaction honeypot such as a replicated fake server relies on its ability to appear as a legitimate target, traps the attacker willingly while passively monitoring. Not only will this cause the attacker to waste time and resources on useless targets, thereby denying their objective, but it also provides two additional advantages to cyber security efforts. First, through logging and tracing the intruders attempts to probe and gain access are documented; these results provide insight on the attacker's tradecraft to help strengthen defenses on real systems. Secondly, the forensics can also be used to aid attribution for follow-on compellence actions.[44]

[43] Kristin Heckman et al., "Cyber Denial, Deception and Counter Deception." *Advances in Information Security* (2015). doi:10.1007/978-3-319-25133-2.
[44] Loras Even, "IDFAQ: What Is a Honeypot?" SANS. Accessed May 25, 2016. https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9.