PERSPECTIVES ON CYBER POWER

CPP-4

Is Cyber Deterrence Possible?

Timothy M. McKenzie
Colonel, USAF

AIR FORCE RESEARCH INSTITUTE PAPERS

Air University

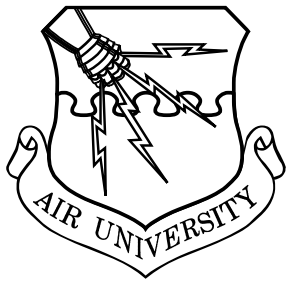
Steven L. Kwast, Lieutenant General, Commander and President

Air Force Research Institute

Dale L. Hayden, PhD, Director

AIR UNIVERSITY

Air Force Research Institute
Perspectives on Cyber Power



Is Cyber Deterrence Possible?

Timothy M. McKenzie
Colonel, USAF

CPP–4

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

Project Editor
Jeanne K. Shamburger

Copy Editor
Carolyn Burns

Cover Art, Book Design, and Illustrations
Daniel Armstrong

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark

AIR FORCE RESEARCH INSTITUTE

AIR UNIVERSITY PRESS

Director and Publisher
Dale L. Hayden, PhD

Editor in Chief
Oreste M. Johnson

Managing Editor
Dr. Ernest Allan Rockwell

Design and Production Manager
Cheryl King

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
afri.aupress@us.af.mil

http://aupress.au.af.mil/
http://afri.au.af.mil/
https://www.facebook.com/AirUnivPress/
https://twitter.com/aupress

AIR UNIVERSITY PRESS
A DIVISION OF THE AIR FORCE RESEARCH INSTITUTE

Library of Congress Cataloging-in-Publication Data

Names: McKenzie, Timothy M., 1969– author. | Air University (U.S.). Air Force Research Institute, issuing body.
Title: Is cyber deterrence possible? / Timothy M. McKenzie
Other titles: Air Force Research Institute perspectives on cyber power ; CPP-4. 2329-5821
Description: First edition. | Maxwell Air Force Base, Alabama : Air University Press, Air Force Research Institute, [2017] | Series: Perspectives on cyber power, ISSN 2329-5821 ; CPP-4 | Includes bibliographical references.
Identifiers: LCCN 2016052326| ISBN 9781585662739 | ISBN 1585662739
Subjects: LCSH: Cyberterrorism—United States—Prevention. | Deterrence (Strategy) | Cyber intelligence (Computer security)—International cooperation. | Cyberspace—Military aspects—United States. | Security, International. | Information warfare—United States—Prevention.
Classification: LCC U167.5.C92 M35 2017 | DDC 355.3/43—dc23 | SUDOC D 301.26/31:4

LC record available at https://lccn.loc.gov/2016052326

Published by Air University in January 2017

Disclaimer

Air Force Research Institute Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Air Force Research Institute studies are available via the AU Press website at http://aupress.au.af.mil/papers.asp. Please submit comments to afri.aupress@us.af.mil.

Contents

Illustrations

About the Author

Col Timothy M. McKenzie is assigned to the Space and Missile Systems Center, Los Angeles AFB, California. He began his career in 1993 after receiving a commission through the Reserve Officer Training Corps and graduating from Northern Arizona University with a bachelor of science degree in electrical engineering. He has served in a number of assignments in the Air Force's and Department of Defense's space acquisition sectors, including the Space and Missile System Systems Center, National Reconnaissance Office, and Secretary of the Air Force staff. In addition to space acquisition, Colonel McKenzie has conducted command and control of the Global Positioning System satellite constellation and worldwide computer security red-team assessments.

Abstract

In recent years, the importance of operating in and protecting the cyber domain has gained much attention. As long as our nation relies on computer networks as a foundation for military and economic power, our national and economic security are at risk through the cyber domain. Cyber attacks on US industry and government systems severely impact our economy and ability to execute modern network-centric warfare.

Our reliance on networked systems and the high costs associated with cyber attacks have led many leaders in the US government and Department of Defense to focus resources toward developing a strategy for deterring adversaries from attacking our networks in the first place. This effort has led to much debate about the question, is cyber deterrence possible? Deterrence in the cyber domain is drastically different and far more complicated than in other military domains (air, land, sea, and space). Cyber weapons and offensive cyber techniques are relatively inexpensive and easily obtained or developed. The number of adversary groups capable of attacking US networks is large, and our ability to deter each group will vary based on its motives and levels of risk tolerance. An effective cyber deterrence strategy must be multilayered and use all instruments of US national power. This paper discusses the difficulties of deterring unwanted cyber activities, provides some realistic expectations for a deterrence strategy, and offers proposals to help mitigate the problems.

Introduction

The United States' reliance on networked systems and the high costs associated with cyber attacks have led many leaders in the US government and the Department of Defense (DOD) to prioritize protecting our critical networked infrastructure. Part of that focus is trying to develop a strategy for deterring adversaries from attacking our networks in the first place. This effort has led to much debate around the question of whether cyber deterrence is possible.

Answering this question is difficult since the number of adversary groups capable of attacking US networks is large and our ability to deter each group will vary based on its motives and levels of risk tolerance. The United States should not expect a cyber deterrence strategy to achieve the kind of results seen with our nuclear deterrence strategy during the Cold War. However, a *limited* US cyber deterrence strategy is possible. To be effective, this strategy must be multilayered and use all instruments of US national power. The strategy employed against one adversary group (e.g., criminal actors) will be different than that against another group (e.g., state or state-sponsored actors). This paper explores (1) the difficulties of deterring unwanted cyber activities by each group of cyber threats, (2) realistic expectations for a deterrence strategy, and (3) proposals to help mitigate the problems.

Background

In recent years, the importance of operating in and protecting the cyber domain has gained much attention. The US president, members of Congress, and senior DOD/military officials are keenly aware of the criticality of cyber to US national security. The 2010 *National Security Strategy* says the following regarding cybersecurity:

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. . . . Our digital infrastructure . . . is a strategic national asset, and protecting it . . . is a national security priority.[1]

As long as our nation relies on computer networks as a foundation for military and economic power, our national and economic security can be placed at risk through the cyber domain. Cyber attacks on US industry and government

---

The author wrote this paper in 2014 while a student at the Air War College Cyber Horizons program, Maxwell AFB, Alabama.

systems have significant impacts to our economy. As many as 500,000 US jobs are lost each year from costs associated with cyber espionage, and hacking costs the overall US economy as much as $100 billion each year.[2] A comprehensive cyber deterrence strategy is one option available to the United States for preventing or minimizing further impacts to critical US national security digital infrastructure.

General Deterrence Theory

To answer the question of whether cyber deterrence is possible, one must understand the theories or concepts behind successful deterrent strategies and how they apply to cyber. There is no single definition of deterrence or shortage of theories for its practical application. Joint doctrine defines *deterrence* as the "prevention of action by either the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[3] Deterrent options can be either passive or active in nature. In his book *Cyber Deterrence and Cyber War*, Martin Libicki describes these options as (1) "deterrence by denial (the ability to frustrate the attacks)" or passive deterrence and (2) "deterrence by punishment (the threat of retaliation)" or active deterrence.[4] From a cyber perspective, passive deterrence includes those actions taken to secure our networks from attacks or to build resilient networks that minimize the effects of an attack. These actions are an important part of good system security engineering and doctrine but do not play a substantial role in actively deterring cyber attacks. They can, however, have a deterrent effect by denying the adversary any meaningful effects to our systems, networks, or operations. As an alternative, active deterrence threatens retaliation or some type of undesirable response to a cyber attack or incident.

What are the attributes that lead to a successful deterrence strategy? For the purposes of this study, seven commonly cited deterrence attributes are highlighted for evaluation: interest, deterrent declaration, credibility, fear, denial measures, penalty measures, and cost-benefit calculation (see table).

In the case of cyber, our interest is in preventing cyber attacks against critical US government and civilian infrastructure. The deterrent declaration (or warning) must be loud and clear so the target cannot misread it, clearly documented in national policy, and consistently echoed in the words and actions of civilian and military leaders. To deter a target actively, one must have the means to threaten the target into inaction.[5] Most articles on cyber deterrence assert that retaliation will be in the form of a counter cyber attack. A cyber-attack response is just one of the many instruments of national power available to actively deter or respond to a cyber attack or incident. Finding the proper

mix of passive and active actions is the key to building a successful strategy. Passive cyber deterrence (deterrence by denial) alone will not inflict the necessary *fear* in an adversary to prevent attacks. There must be a *credible* threat to impose an undesirable set of *penalty measures* (active deterrence) to have a successful and effective strategy

Table. Deterrence attributes

Deterrence attribute	*Definition*
Interest	A state employs a deterrence strategy to protect an interest.
Deterrent declaration	To keep adversaries from attacking the interest, a state makes a deterrent declaration: Do not do *this*, or else *that* will happen. *This* is any adversary action that threatens the interest, and *that* includes either denial measures, penalty measures, or both.
Credibility	Credibility is the attacker's calculation of the defender's capability and intent to carry out the deterrent declaration. For other states to take a deterrent declaration seriously, the declaration must be credible and believable.
Fear	If a potential adversary fears the denial or penalty measures, that actor is less likely to take an undesirable action.
Denial measures (passive measures)	Denial is the defensive aspect of deterrence and consists of prevention and futility. Deterrence by prevention means that if an attack is launched, the defensive measures will disrupt the attack to keep it from succeeding. Deterrence by futility means that even if an attack breaches defenses, it will not have its desired effect on the target.
Penalty measures (active measures)	Penalty is the offensive aspect of deterrence and consists of retaliation. Classical deterrence theory demands that penalty measures be certain, severe, and immediate.
Cost-benefit calculation	What are the benefits and costs of action versus the benefits and costs of restraint?

Adapted from Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice," *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–35, http://www.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf.

What Is a Cyber Attack?

The next step in determining if cyber deterrence is possible is understanding and defining what actions the United States is trying to prevent. Senior civilian and military leaders often use the term *cyber attack* incorrectly when discussing malicious actions against our critical infrastructure. In 2013 Air Force general William M. Fraser III told the Senate Armed Services Committee that

US Transportation Command was "hit by almost 45,000 cyber attacks during 2011, and quadruple that number [in 2012]."[6] In this case, General Fraser used an extremely broad definition of cyber attack.

Because malicious cyber actions can be grouped in many ways, not all malicious actions should be classified as an attack. *Merriam-Webster* defines an *attack* as "to act violently against (someone or something)." In the cyber domain, the "someone" is US citizens or allies while the "something" is the critical US digital infrastructure that is the backbone of our economic and military power. In his commentary for the *National Interest*, Panayotis A. Yannakogeorgos uses the definition of cyber attack from the *Tallinn Manual on the International Law Applicable to Cyber Warfare*: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." Yannakogeorgos refers to actions that fall below the threshold of cyber attack as aggressive incidents. For instance, he categorizes the distributed denial-of-service disruptions to US financial services as aggression and the incidents of Chinese hackers stealing US intellectual property as cyber espionage—not as cyber attacks. Yannakogeorgos concludes that while the acts of disrupting business services or stealing data are not an armed attack, they may—under the right political circumstances—cause the national leadership to act.[7] The United States Cyber Command (USCYBERCOM) groups cyber activity into the three categories of access, disruption, and attack (see figure).

Based on these categories, therefore, a cyber attack must cause physical damage to property or injury to persons. I agree with Dr. Yannakogeorgos's and USCYBERCOM's definition of an attack. However, some activities categorized as a "disruption" or "aggressive incident" could also rise to the level of a cyber attack, depending on the economic impact of the disruption. In 2015 Defense Secretary Ashton Carter told the Senate Committee on Armed Services that a "cyber attack on critical infrastructure, the economy or U.S. military operations" is "an act of cyber warfare" and that "theft of intellectual property through cyber means" jeopardizes our national security and economic prosperity.[8] I believe that cyber activity resulting in an appreciable financial loss to a US private company or US government office/agency should also be considered an attack against our critical national interest. Therefore, the following definition of a *cyber attack* is provided for the purposes of this paper: the deliberate damage, destruction, or corruption of critical private systems or critical/noncritical government systems or any cyber activity that results in a significant financial loss to a US private company or US government office/agency or that results in death, destruction,

or serious injury. The focus of any national-level cyber deterrence strategy should be to prevent these types of cyber attacks.

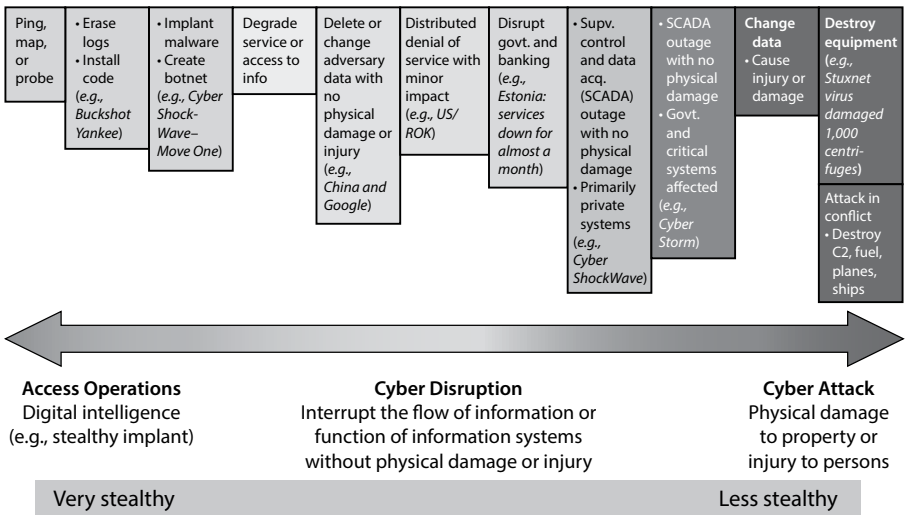


Figure. Spectrum of cyber operations. (Adapted from USCYBERCOM/Judge Advocate, briefing, subject: Assessing Actions along the Spectrum of Cyberspace Operations, slide 18, no date.)

Analysis of Current US Cyber Policy

The first step in defining an effective deterrent strategy is establishing policy at the national and DOD levels. One of the most important policy documents is the 2010 *US National Security Strategy* (*NSS*) signed by the president.[9] The *NSS* is intended to outline the president's national priorities and provide high-level guidance for US agencies and departments to follow. This document also serves as an indicator to our international partners and adversaries of areas where we plan to focus our attention. It addresses several of the seven attributes necessary for effective deterrence. First, the *NSS* defines our national "interest." It makes clear that the US digital infrastructure is a "strategic national asset, and protecting it . . . is a national security priority." These statements make evident the critical role of cybersecurity in our national security. However, the deterrent declaration in the *NSS* is extremely weak: "we will deter,

prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by . . . investing in people and technology . . . [and] strengthening partnerships."[10] It makes virtually no reference to a deterrent penalty of any significance. It states only that the United States will "strengthen our international partnerships on . . . the development of norms for acceptable conduct in cyberspace . . . [and] laws concerning cybercrime." It adds, "We will work with all the key players . . . to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents."[11] While the document says that we want to deter attacks against our infrastructure, it makes no strong declarations of severe penalties if an adversary makes such attempts.

The next policy document that gives us insight into a US strategy on cyber deterrence is the 2011 White House document *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Its stated goal for the United States in the future cyberspace environment is to

> work internationally 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. To achieve that goal, [the United States] will build and sustain an environment in which *norms of responsible behavior* guide states' actions, sustain partnerships, and support the rule of law in cyberspace (emphasis in original).[12]

This strategy outlines how the United States plans to deter cyber threats. It specifically addresses two of the seven attributes necessary for deterrence: denial and defining penalty measures. A key part of the international strategy is deterrence by denial. The president's plan is to build robust network defenses and the "ability to withstand and recover from disruptions and other attacks."[13] This capability is a key part of a deterrent strategy but is extremely difficult to do in practice. New vulnerabilities are identified on a daily basis, and protecting all systems against these vulnerabilities is nearly impossible. Building secure and defensible systems is a worthy goal and logical part of any good system engineering or operating process. Nevertheless, our networks are so complex and extensive that preventing attacks through defensive measures is not likely to be a strong deterrent. Regarding the attribute of defining penalty measures, the strategy states that the United States will work with national and international law enforcement organizations to prosecute hackers. Further, when warranted, the United States will respond with "all necessary means—diplomatic, informational, military, and economic [DIME]—consistent with applicable international law."[14] Thus, this document unequivocally affirms that the United States will pursue legal action against individuals and is willing to use military force against state and nonstate actors, such as terrorist groups.

The final fundamental policy document that clarifies US strategy on cyber deterrence is the 2011 *Department of Defense Strategy for Operating in Cyberspace*. It acknowledges that the DOD is particularly concerned with three areas of potential adversarial activity: (1) theft or exploitation of data; (2) disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and (3) destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.[15]

The DOD strategy for cyberspace complements that of the president's by continuing the theme of denial by defense. A key part of this strategy is to defend and protect critical cyber infrastructure. However, as discussed above, while denial by defense is paramount, it is difficult in practice and not likely to be a great deterrent by itself. The DOD also indicates that the United States will treat cyber as a war-fighting domain and maintain the capability to operate effectively in it. Doing so includes organizing, training, and equipping forces to conduct both offensive and defensive operations in cyberspace. Thus, another priority is maintaining an offensive cyber capability.

While offensive capabilities comprise an effective military strategy, they are not likely to act as a strong deterrence against cyber attacks. Here's why. To serve as an effective deterrent, the use of offensive cyber tactics as a potential penalty measure in response to a cyber attack must be credible. The United States will likely be judicious in its use of offensive cyber weapons, defined as "digital objects that can be used to achieve military objectives by disabling key functions of computer systems and networks."[16] When employed, these weapons will identify which vulnerabilities are being exploited in adversary networks and thus expose US capabilities. As a result, the adversary can then patch those vulnerabilities; the offensive weapon then becomes useless against that particular adversary and potentially others. Offensive cyber weapons have a limited shelf life and may take years to develop. The United States would be wise to explore other instruments of national power before it exposes a fragile offensive cyber weapon.

Challenges for Cyber Deterrence

Attribution

Now that we have a basic definition of deterrence and the attributes necessary for success, the next step is to look at the challenges associated with applying those principles to cyberspace. One of the biggest barriers to effective cyber deterrence is the concept of attribution. Intelligence expert Bob Gourley

maintains that "you cannot deter unless you can punish and you cannot effectively punish unless you have attribution."[17] Attribution in the cyber domain is possible, but in some circumstances it can be difficult and time-consuming. The complex structure of the Internet, immature political and legal policies, and global nature of the cyber domain make operating anonymously possible. Adversaries can exploit any number of system or protocol vulnerabilities to hide or spoof their location and can operate from nearly any physical location. The more sophisticated the attacker, the more difficult attribution becomes. These attackers will take actions to hide their true location and make it appear that another attacker or nation-state may have conducted the attack. Additionally, legal and political hurdles may make attribution difficult and time-consuming—especially when international cooperation among multiple organizations, agencies, and governments is required to determine the source of an attack. Any organization that chooses not to assist in the investigation (or that does not have the technical capacity to assist) can prevent or hinder positive identification of the attacker. As a result, obtaining certain attribution in a timely manner can, at times, be extremely difficult (especially against a sophisticated attacker). To deter criminal cyber actions, US law enforcement agencies must rely on technical attribution to prosecute and impose appropriate penalty measures. Technical attribution is the ability to associate an attack with a responsible party through technical means based on information made available by the cyber operation itself—that is, technical attribution is based on clues available at the scene(s) of the operation.[18]

At the national level, the United States has additional tools at its disposal to aid in the attribution of a cyber attack against terrorist or nation-state cyber actors. At this level, it isn't necessary to determine attribution at a level that will hold up for a conviction in a court of law. In this case the United States will use all-source intelligence products to identify the party that should be held responsible for a cyber attack. According to Dr. Herbert Lin, *all-source attribution* "is a process that integrates information from all sources, not just technical sources at the scene of the attack, to arrive at a judgment (rather than a definitive and certain proof) concerning the identity of the intruder."[19] Data collection includes more traditional intelligence gathering sources and methods that may allow us to overcome some of the technical or political hurdles that hinder the timely and certain attribution of cyber activity.

Using such sources, however, leads to another difficulty with attribution. At some point, the United States must publicly declare—and prove beyond a reasonable doubt—that it knows who has attacked our system. Such verification is a crucial step prior to gaining support to impose penalty measures from US policy makers, US citizens, and/or any desired or required international

entities. In so doing, we may have to reveal classified sources and methods that we may not be willing to share. The United States may find itself in a difficult situation since demonstrating to those it wants to deter that it has the ability to attribute attacks is key to a credible cyber deterrence strategy.

Understanding Adversary Motives and Level of Risk Tolerance

Another challenge to cyber deterrence is understanding the adversary and how it will react to a given deterrence strategy. Cyber threats can be categorized in many ways, and each category will have different motivations and levels of cyber skills or capabilities. Our ability to deter each group of cyber adversaries will vary. For this paper, I group threats into the three categories of criminal actors, violent nonstate actors, and state or state-sponsored actors.

Cyber-criminal activity is the largest group of cyber threats and one of the most difficult to effectively deter. This group of hackers ranges in sophistication from low ability (i.e., script kiddies) to elite-level hackers motivated by financial gain. Our ability to punish and deter this group is sometimes limited and largely dependent on law enforcement and effective cooperation from foreign nations. Sophisticated hackers will seek out places where governance and policy conditions facilitate masking their identities.[20] Punishing this group can be complex for several reasons. First, as discussed, accurately attributing the source of cyber attacks is problematic and sometimes time-consuming. Second, the sheer volume of activity makes prosecuting all cases impractical. According to a 2013 US Government Accountability Office report on cybersecurity, the number of computer security incidents that federal agencies reported to the United States Computer Emergency Readiness Team (US-CERT) over a six-year period increased from 5,503 in 2006 to 48,562 in 2012 (a 782 percent increase).[21] According to the Internet Crime Complaint Center's *2010 Internet Crime Report*, the Federal Bureau of Investigation received 303,809 Internet crime complaints resulting in 1,420 prepared criminal cases—which led to a mere six convictions.[22] In addition to the low conviction rate, cybercrimes are among the most underreported forms of criminality. One estimate suggests that only 17 percent of companies report cybercrime-related losses to law enforcement.[23] Hackers with criminal or financial intent have to weigh the possibility of being caught and prosecuted for their crimes against the potential profits. Skilled hackers who know how to hide their identities and locations will continue to conduct these crimes until identification, attribution, and prosecution of cybercrimes increase. Our ability to deter political hacktivist groups is low for all the same reasons. Hacktivists are activists motivated by politics or religion or the desire to expose that of a wrongdoing or exact revenge. The DOD will

have a minimal role in deterring these groups since the threat of military action is not a likely or credible response. Until we can discernibly increase the risk of prosecution, we cannot expect to have an effective US national-level cyber-deterrence strategy against criminal hackers or political hacktivists.

The next adversary group is violent nonstate-sponsored organizations such as terrorist groups. This group may be more organized and have a clear goal to inflict harm against the United States or its key interests. Again, our ability to deter this group from attacking our networks is currently low. This group is intent on causing harm to the United States at almost any cost and would likely publicize its success at wreaking havoc on our systems. A nonstate-sponsored terrorist group understands that it cannot fight the United States in a force-on-force battle so it resorts to irregular forms of warfare. Attacking the United States in the cyber domain certainly falls within the realm of modern irregular warfare. The cost of entry is low when compared to that of obtaining traditional weapon systems capable of defeating US forces. Cyber weapons and techniques are more readily available than advanced traditional weapon systems, and cyber weapons give terrorists an ability to attack the US homeland. We have seen these groups successfully recruit people who are willing to die as suicide bombers for their causes. It's not hard to envision one of these groups recruiting skilled hackers to support its fight against the United States. Since we are so heavily networked and these groups are so determined, a reasonable possibility is that—at some point in the future—one of these groups will impact US interests. It is unlikely that a terrorist group currently has the ability to launch a cyber attack that will elicit mass fear in the general public. However, it is very possible that a group could attack private and government infrastructure, causing significant financial loss to individuals or corporations. When these groups perform the "cost-benefit calculation" associated with cyber attacks, they will certainly see that the potential gain far exceeds the minimal risk of immediate retribution. Unlike for criminal attacks, the DOD has a role in attempting to deter activity from these groups. It can attempt to passively deter attacks against DOD infrastructure through defensive measures and actively by responding militarily (not necessarily a cyber response) against a terrorist action.

Unlike criminal hackers or nonstate-sponsored adversaries, state-sponsored groups can be effectively deterred. The difference between this group and the others is our ability to inflict an appropriate level of punishment on a nation-state to deter unfavorable behavior guided by that state. In this case, the United States can use its full DIME instruments of national power to shape foreign nations' behaviors. The threat of economic sanctions, military action, or other political/diplomatic responses by the United States could markedly affect certain

states. A nation-state will have to weigh the risk of escalating hostilities with the most powerful nation on Earth with the potential gains of a cyber attack. We should expect most nation-states to develop offensive cyber weapons for use against the United States due to their low cost and our reliance on networked systems. If we go to war against one of these nations, we should expect that they will use cyber weapons against us. An effective cyber deterrence strategy should make it clear to any nation that a cyber attack against US interests will be seen as a form of aggression and is no different than a kinetic or armed attack. The goal is to have a deterrent strategy that prevents a nation from employing cyber weapons outside of a declared war against the United States.

We must bear in mind that a state actor's conduct of cyber access operations should not be considered an act of aggression against the United States. We cannot punish those actions that we plan to execute ourselves. For example, the United States has openly stated that it will maintain an offensive cyber capability. Having this capability requires it to gather intelligence against foreign systems. This collection can be done in many ways but will likely include some sort of computer network exploitation (CNE) of adversary systems during times of peace. CNE is intrusive to adversary systems, but it does not damage or corrupt those systems. If the United States chooses to conduct CNE outside of a declared war or conflict, then it must expect that others will do the same. We must therefore be willing to accept foreign nations gaining access to our systems and installing implants for persistent access. This tactic is simply a modern form of espionage as long as their actions do not disrupt or cause damage. Consequently, we are left with deterring actions that cause data corruption, damage, financial loss, or physical injury (i.e., a cyber attack).

Final Analysis

Recommendations for the United States and DOD

Current US strategy falls short on several key attributes necessary for effective deterrence: deterrent declaration, penalty measures, credibility, and fear. National strategy does a decent job of making clear to our adversaries that we have a strong interest in protecting and defending our networks but falls short with its deterrent declaration. While designing, acquiring, and operating more secure systems are essential, deterrence by denial is a passive strategy—and insufficient on its own to achieve cyber deterrence. A critical part of a deterrence strategy is, first, promoting a strong deterrent declaration that makes clear to adversaries the severe penalties of attacking our interests. Second, and most importantly, the United States must be willing to inflict severe penalty measures against

those who attack. Classic deterrence theory demands that penalty measures be certain, severe, and immediate. Although the United States certainly has the means to threaten severe penalties (through diplomatic, military, and economic actions), it continues to allow adversaries to attack our networks with little or no consequences. The United States must add credibility to its deterrence strategy as it is allegedly hacked routinely by foreign states such as China, Russia, North Korea, and Iran. We continue to allow these nations to penetrate our systems and do nothing about it. At this point in time, the United States' threats to impose penalties are not believable. Without the ability to enforce consequences, we cannot create a situation in which an adversary fears our penalty measures and therefore chooses not to attack our systems.

The problem, as noted above, is that the strategy has no credibility. Cyber deterrence is possible if the United States is willing to punish those who conduct activities we wish to deter. It is not possible to deter adversaries from conducting CNE against our systems (since the United States will likely be conducting CNE against their systems), but it is possible to deter those activities that cause data corruption, damage, financial loss, or physical injury. The United States can have a viable deterrence strategy by enforcing a set of penalty measures on a nation-state conducting unwanted cyber activity against US networks. As discussed, such measures are the offensive aspect of deterrence and consist of a form of retaliation. A perfect example would be the United States taking proportionate political and economic actions toward China for the extensive corporate espionage it conducts in the cyber domain. A recent report to Congress by the United States–China Economic and Security Review Commission observes that China's "professional state sponsored intelligence collection not only targets a nation's sensitive national security and policy-making information, it increasingly is being used to collect economic and competitive data to aid foreign businesses competing for market share with their US peers."[24] China goes beyond what the United States considers acceptable state-sponsored espionage and crosses into state-sponsored corporate espionage. This activity has a clear and significant impact on the US economy and the future of US economic dominance. US cyber deterrence strategy would have credibility if we stood up to China with economic and political sanctions and were successful in stopping cyber-related corporate espionage against US companies. This topic, however, is one for another paper. A useful exercise would be to evaluate potential gains to the US economy by preventing China's cyber corporate espionage versus potential economic and political losses that may occur by playing hardball with one of our most valuable trade partners.

Conclusion

While a US strategy to deter cyber attacks is possible, current US strategy lacks credibility. It will be effective only if we can swiftly and adequately punish malicious cyber actors such that aggression against our systems is not worth the potential reward. US strategy lacks a clear definition of what actions constitute a cyber attack and will result in some form of US retaliation. Corporate cyber espionage should be at the top of the list of cyber attacks that will elicit severe penalty measures from the US government. These attacks pose an unequivocal risk to our national security and economic prosperity. Since the United States plans to conduct offensive cyber operations during times of peace, we can only expect to deter actions that actually inflict damage to our systems, result in financial loss, or cause physical injury.

A strong US cyber deterrence strategy will have the most immediate effect on nation-states whose actions can be influenced by US instruments of national power. However, nations such as North Korea and Iran have shown an incredible resistance to US political and economic pressure and may be difficult to deter without credible threats of military actions. The United States should also pursue a strategy to deter common hackers, criminals, violent nonstate actors, and other non-nation-state actors. The success of this strategy will be limited until the prosecution rate increases to a level that swings the cost-benefit calculus in favor of the United States. To be effective, US strategy must be multilayered and use all instruments of US national power. We must understand the motives and levels of risk tolerance of all malicious cyber actors and tailor the strategy toward each group.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. White House, *National Security Strategy*, 27.
2. Smith, "Hackers Cost U.S. Economy."
3. Joint Publication 3-0, *Joint Operations*, GL-9.
4. Libicki, *Cyber Deterrence*, 7.
5. Trujillo, "Limits of Cyberspace Deterrence," 45.
6. Miles, "Transcom, Partners Secure Networks."
7. Yannakogeorgos, "Keep Cyberwar Narrow."
8. Gertz, "Ashton Carter Outlines Acts."
9. The White House updated the 2010 *NSS* in February 2015 (after this paper was written). However, the basic premise of the revised document remains the same.
10. White House, *National Security Strategy*, 27–28.
11. Ibid., 28.
12. National Security Council, *International Strategy for Cyberspace*, 8.

13. Ibid., 12.
14. Ibid., 14, 20.
15. DOD, *Strategy for Operating in Cyberspace*, 3.
16. Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace*.
17. Gourley, "Towards a Cyber Deterrent," 1.
18. Lin, "Escalation Dynamics and Conflict," 49.
19. Ibid.
20. Yannakogeorgos, *Cyber Attribution Challenge*.
21. US Government Accountability Office, *Cybersecurity*, 7.
22. Grimes, "Internet Crime Goes Unpunished."
23. Kshetri, " Simple Economics of Cybercrimes," 35.
24. Krekel, Adams, and Bakos, *Occupying the Information High Ground*.

Abbreviations

CNE	computer network exploitation
DIME	diplomatic, informational, military, and economic
DOD	Department of Defense
NSS	*National Security Strategy*
US-CERT	United States Computer Emergency Readiness Team
USCYBERCOM	United States Cyber Command

Bibliography

Beidleman, Lt Col Scott W., USAF. "Defining and Deterring Cyber War." Strategy Research Project. Carlisle Barracks, PA: US Army War College, 2009. http://www.dtic.mil/dtic/tr/fulltext/u2/a500795.pdf.

Betts, Richard K. "The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can—and Can't—Do Now." *Foreign Affairs*, March/April 2013. http://www.foreignaffairs.com/articles/138846/richard-k-betts/the-lost-logic-of-deterrence.

Crosston, Mathew D. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 100–116. http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, July 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. *Quadrennial Defense Review 2014*. Washington, DC: Department of Defense, 2014. http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

Executive Order 13636. Improving Critical Infrastructure Cybersecurity, February 2013. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

Gertz, Bill. "Ashton Carter Outlines Acts of Cyber War." *Washington Times*, 4 February 2015. http://www.washingtontimes.com/news/2015/feb/4/inside-the-ring-ashton-carter-denies-north-korea-c/?page=all.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–35. http://www.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf.

Gourley, Bob. "Towards a Cyber Deterrent." *Social Science Research Network*, 29 May 2008. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542565.

Grimes, Roger A. "Why Internet Crime Goes Unpunished." *InfoWorld*, 10 January 2012. http://www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html.

Hayes, Richard E., and Gary Wheatley. "Information Warfare and Deterrence." *Strategic Forum* no. 87. Washington, DC: National Defense University Directorate of Advanced Concepts, Technologies, and Information Strategies, October 1996. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA394173.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (Summer 2011): 1–24. http://scholarcommons.usf.edu/jss/vol4/iss2/2/.

Jensen, Eric Talbot. "Cyber Deterrence." *Emory International Law Review* 26, no. 2 (29 May 2012): 772–824. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438.

Joint Publication 3-0. *Joint Operations*, 11 August 2011. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

"Key Issues: Cybersecurity." *US Government Accountability Office*. Accessed 2 June 2016. http://www.gao.gov/key_issues/cybersecurity/issue_summary.

Korns, Stephen W. "Cyber Operations: The New Balance." *Joint Force Quarterly* 54 (3d Quarter 2009): 97–102. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA515580.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books, 2009.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Prepared for the US-China Economic and Security Review Commission. McClean, VA: Northrop Grumman Corp., 7 March 2012. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

Kshetri, Nir. "The Simple Economics of Cybercrimes." *IEEE Security and Privacy* 4, no. 1 (January/February 2006): 33–39.

Libicki, Martin C. *Cyber Deterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. http://www.au.af.mil/au/ssq/2012/fall/lin.pdf.

Lukasik, Stephen J. "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains." In National Research Council, *Workshop on Deterring Cyber Attacks*, 99–122. http://www.nap.edu/read/12997/chapter/9.

McConnell, Mike. "How to Win the Cyber-War We're Losing." *Washington Post*, 28 February 2010. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf.

Miles, Donna. "Transcom, Partners Secure Networks against Cyberattacks." *Department of Defense News*, 7 March 2013. http://archive.defense.gov/news/newsarticle.aspx?id=119468.

National Research Council. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: National Academies Press, 2010. http://www.nap.edu/catalog.php?record_id=12997.

National Security Council. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: Executive Office of the President of the United States, May 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Nye Joseph S., Jr. *Cyber Power*. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010.

———. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18–38.

Rosenzweig, Paul. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." In National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 245–69. Washington, DC: National Academies Press, 2010. http://www.nap.edu/read/12997/chapter/18.

Siciliano, Robert. "7 Types of Hacker Motivations." *Family Safety Blog*, 16 March 2011. http://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations.

Smith, Gerry. "Hackers Cost U.S. Economy up to 500,000 Jobs Each Year, Study Finds." *Huffington Post*, 25 July 2013. http://www.huffingtonpost.com/2013/07/25/hackers-jobs_n_3652893.html.

Taipale, K. A. "Cyber-Deterrence." In *Law, Policy and Technology: Cyberterrorism, Information Warfare, Digital and Internet Immobilization*. Hershey, PA: IGI Global, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045.

Trujillo, Clorinda. "The Limits of Cyberspace Deterrence." *Joint Force Quarterly*, no. 75 (4th Quarter 2014): 43–52. http://ndupress.ndu.edu/Portals/68/Documents /jfq/jfq-75/jfq-75_43-52_Trujillo.pdf.

US Government Accountability Office (GAO). *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*. GAO-13-187. Washington, DC: US GAO, 14 February 2013. http://www.gao.gov/products/gao-13-187.

White House. *National Security Strategy*. Washington, DC: White House, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Yannakogeorgos, Panayotis A. "Keep Cyberwar Narrow." Commentary. *National Interest*, 17 May 2013. http://nationalinterest.org/commentary/keep-cyber war-narrow-8459.

———. *Strategies for Resolving the Cyber Attribution Challenge*. Cyber Power Paper no. 1. Maxwell AFB, AL: Air Force Research Institute, Air University Press, May 2013.

Yannakogeorgos, Panayotis A., and Adam B. Lowther. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton: Taylor and Francis Group, 2014.

AUP
AIR UNIVERSITY PRESS
A DIVISION OF THE AIR FORCE RESEARCH INSTITUTE
http://aupress.au.af.mil

ISBN 978-1-58566-273-9
ISSN 2329-5821