AIR WAR COLLGE

AIR UNIVERSITY

CYBER DETERRENCE

by

Brian Harding, CDR, USN

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Clinton Mixon, COL, USAF

Date: 11 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

CDR Harding is a native of Virginia Beach, VA. He enlisted in the Navy in 1988, promoted to Chief Petty Officer in 1997 and was commissioned an Ensign via Officer Candidate School in 1998.

He is currently attending Air War College at Maxwell Air Force Base. CDR Harding began his Information Warfare Officer career at the Naval Security Group Activity Menwith Hill, located in Harrogate, England. There he served as operations watch officer and completed direct support officer deployments in the Mediterranean Sea and the Arabian Gulf. His next tour was at the Naval Security Group Activity Rota, Spain and performed duties as Special Evaluator onboard the EP-3E, and was assigned as Operations Officer until reassignment as NSGA Rota Executive Officer.

In 2005, he returned to the United States and was assigned to the USS IWO JIMA as the SSES Division Officer. His next tour in 2007 was at the Naval Information Operations Command Bahrain as Executive Officer. In 2008 he served on the Staff of Naval Network Warfare Command. In May 2010 he was assigned to U.S. 7th Fleet Staff as Intelligence Collection Manager and Cryptologic Resources Coordinator. In 2012 he was assigned as the Information Warfare Officer Junior Officer detailer. In 2014 he was assigned as Team Lead for Navy Cyber Unit Six.

His personal awards include the Defense Military Service Medal, Meritorious Service Medal, the Navy and Marine Corps Commendation Medal, the Joint Service Achievement Medal, the Navy and Marine Corps Achievement Medal, and various unit and service awards.

Abstract

This essay will present a current review of writings on the viability of Cyber Deterrence. By researching deterrence theory definition the author was able to identify the importance of credibility, capability and attribution. This paper will highlight the importance of credibility, capability and attribution as they relate to the US creating an effective cyber deterrence strategy for employing all elements of national power to protect the US from cyber attacks in a highly technical and complex future.

Introduction

The new U.S. Cyber Strategy dated 17 April 2015 states, “In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyber attacks against U.S. interests.”[1] Admiral Michael S. Rogers, commander of U.S. Cyber Command and Director of the National Security Agency described the concept of deterrence in the cyber domain as relatively immature. "We're going to have to work our way through this by developing and accepting norms of behavior in cyberspace that will underlie and support the notion of deterrence.”[2] Cyber deterrence will be effective when we can determine what a non-state cyber actor or state cyber actor values, threaten it, know what each will risk, and effectively communicate our position and a credible threat to the non-state cyber actor or state cyber actor.[3] This paper draws attention to the importance of credibility, capability and attribution as they relate to the US creating an effective cyber deterrence strategy for employing all elements of national power to protect the US from cyber attacks in a highly technical and complex future.

Thesis

In the fog of overly complicated cyberspace technology, attribution of cyber operations seems difficult, but cyber deterrence can still be a viable strategy if the United States can increase its status as a credible and capable global cyber power.

From General Deterrence to Cyber Deterrence

Deterrence causes a psychological effect on an individual or group no matter what domain we consider. By reviewing history and understanding the strengths and weaknesses exposed during the application of deterrence theory, we can better understand a way forward for deterring cyber attacks. In the eighteenth century Italian philosopher, Cesare Beccaria, described the goal of criminal deterrence, "Prevent the criminal from doing further injury to society and to prevent others from committing the like offense."[4] Lawrence Freedman defines deterrence as, "The attempts to manipulate the behaviors of others through conditional threats."[5] After the first use of nuclear weapons Bernard Brodie stated, "The chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."[6] Joint Pub 1-02 defines deterrence as, "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.[7]" Many of the fundamental assumptions that were the basis of deterrence thinking during the cold war regarding nuclear deterrence will have to be reevaluated for usefulness in the cyber era and be debated by current strategists.[8]

The successful use of nuclear deterrence creates significant debate between deterrence theorists. In *Deterrence and Saddam Hussein*, Barry Schneider lays out five important criteria to achieve via nuclear weapons during the Cold War. He argues that allies with a strong retaliatory force that could inflict unacceptable damage in an adversary's view was important; that the allies needed to make sure the adversary was aware of our lethal capabilities and our willingness to use it; attribution to the original attacker would be required; allies would need to survive a surprise attack and fight

through it with a mix of forces to retaliate.[9] Finally, Barry Schneider's fifth criterion points out the need for an adversary to have complete understanding of the global situation and that they will act rationally. Without one of the above five important criteria being met nuclear deterrence would fail in a deadly way.[10]

The current risks to our national security from malicious cyber actors requires us to review basic deterrence theory and ensure its proper understanding and use in the cyber domain by military strategists. Dr. Jabbour and Dr. Ratazzi show similarities between cyber deterrence and nuclear deterrence writing, "The threat of assured mutual self-destruction of cyberspace assets and approaches that manipulate the adversary's cost benefit equation seem to hold the most promise."[11] They expand the thought stating, "Even precision attacks can have widespread unintended effects, possibly against the interests of the attacker."[12] If we value a network service and its operations, the adversary might also and they would most likely consider this in their plans and targeting to decrease damage to items of mutual dependence, value, and interest.[13] The above points on general deterrence theory and nuclear deterrence theory allow us to now discuss what constitutes a cyber attack.

Martin Libicki defines a cyber attack as the deliberate disruption or corruption by one state of a computer system of interest to another state.[14] Passive spying via the Internet, through local networks and into individual computers and devices defines computer network exploitation and not a cyber attack since it does not disrupt or corrupt a computer system.[15] Expanding on Martin Libicki's definition, we know cyber attacks against the US can originate from computer systems of both state and non-state actors. Both have a varying level of intelligence and rationality. Lawrence Freedman described

the main complaint against deterrence. Freedman evaluated strategic theories that depend on the intelligence and rationality of others as an unwise strategy.[16] This appears to be more of a concern in cyber deterrence due to the high number of non-state hackers and potential attackers. Dorothy Denning provides another reason why the concept of cyber deterrence raises so many challenges. She states, "In no other domain of warfare do we address the topic of deterrence across an entire domain. We have no notion of "land deterrence," "sea deterrence," "air deterrence," or "space deterrence." Rather, we direct our attention to particular weapons and activity."[17] Accepting that both Freedman and Denning's complaints on cyber deterrence are valid, we must ensure they are considered in cyber strategy discussions.

The critical aspects of any future cyber deterrence theory remain the same as past deterrence strategies. Lawrence Freedman described all deterrence as self-deterrence because it ultimately depends on the calculations made by the deterred, whatever the quality of the threats they receive.[18]

Another aspect of developing a cyber deterrence strategy that will prove difficult derives from the application of cyber across the range of military operations. This does not vary from Clausewitz's comments when he described strategy as the use of engagement for the purpose of the war and the strategist must maintain control throughout.[19] Cyber deterrence strategists must understand the technical capabilities and risks in the cyber domain to maintain control throughout all phases of war. Cyber deterrence strategy must focus on the cost to benefit ratio. Future cyber strategies must deliver a change from today's model of high benefits versus the low cost and risk to the cyber adversary to a new expectation where the costs and risks outweigh the benefits of a

cyber attack on the U.S.[20] The psychological effect from the adversary review of the cost to benefit ratio depends on how our cyber adversary views our cyber warfare credibility and capabilities.

Credibility

Ideas on credibility vary between theorists. In his book *Deterrence,* Lawrence Freedman described a problem with credibility coming from whether or not our adversary believes threats will be enforced and how past commitments had been honored.[21] Daryl G. Press argued a lengthy view on how adversaries evaluate credibility in his book *Calculating Credibility.* Dr. Press explained the importance of credibility in building alliances, deterring enemies, and preventing costly wars. Dr. Press identified the relationship of a country's credibility during a crisis with its current power and interests and not by past behavior. During crisis, a leader should focus on the here and now not on their adversary's past behavior.[22] Dr. Press stated, "Future commitments will be credible if they are backed up by sufficient strength and connected to weighty interests."[23] Press described the best way to make threats credible writing, "Wielding enough power to carry out the threats successfully at costs that are commensurate with the interest at stake." [24] Press concluded, "The key to maintaining credibility in military crisis, therefore, lies in possessing military power."[25] Having a known ability to recover from and generate a quick, effective and overwhelming response to an attack in cyberspace will also prove critical in deterring an adversary's initiation of a cyber attack.[26] Increasing the cost of a cyber attack to the point where an adversary no longer calculates a positive outcome requires an understanding of the adversary's cost model and the level of its relative cyber expertise.

Credibility and Culture

Cyber deterrence as a strategy depends on the assumption that behaviors of potentially hostile others can be manipulated through issuing timely and appropriate threats.[27] Cyber deterrence could fail to work due to the cyber adversary's cultural interests and objectives. The cyber deterrence goal to convince would be attackers that any action against the U.S. just brings risk, but some cyber adversaries do not receive or value the early deterrence message due to cultural bias or backgrounds. Understanding the cultural interests and objectives of a cyber adversary will decrease the number of adversaries who cannot be deterred by our cyber military power.[28] "Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior."[29] Cyber deterrence's chance of success increases when we understand the cyber adversary's culture and we can convince them that their actions will not succeed. The cyber adversary must receive and believe the message that retaliation from any of our instruments of national power, at a time of our choosing will ultimately deny them from their objectives and they will instead incur an increase in cost and pain.

Our internal measuring of credibility ensures we reach our vision. We need to know how well we are doing in leading and training our cyber workforce. We can get this data through inspections and reporting mechanisms. Beeker, Mills, Grimaila, and Haas made similar points on how much credibility relies on being operationally responsive in cyberspace. To be credible we must develop principles, lessons learned, and best practices to better help the nation prepare and respond to attacks in and through

cyberspace.[30] As these principles are implemented, exercised and promoted, they will have an increasing deterrent effect upon an adversary's desire to attack the nation's cyberspace infrastructure because of a demonstrated ability to reconstitute quickly.[31] Very similar ideas to ensure we have a credible cyber force were recently captured in the Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I) signed by SECDEF and CJCS in September 2015. The DC3I directed USSTRATCOM and USCYBERFCOM to, "Lead and manage the implementation of recently identified elements that include the need to create, manage, oversee, and assess improved Cyber Leader Development, Training, and Education programs; a much more robust and intensive Cyber Inspections regime; and a more complete Cyber Reporting and Accountability Program, as well as working the detailed technical issues associated with overcoming materiel deficiencies that prevent the successful implementation of a robust cyber culture."[32] Future cyber policies and our national strategy must be clarified so that adversaries have a basis for decision-making and consequence evaluation.[33]

Capability

To increase our cyber power the U.S. government continues its efforts to build a strong and capable cyber military workforce that professionally operates highly defended networks with guidance and direction from well thought out and continuously updated cyber policies. Mike McConnell, former director of the NSA, described moving our intent into capabilities in his February 2010 Washington Post article. He stated, "We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options and we must be able to do this in milliseconds. More specifically, we

need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment; who did it, from where, why and what was the result more manageable."[34] Despite Mike McDonnell's efforts five years earlier, in a recent article, *Beyond the Build*, current director of the NSA, Admiral Mike Rogers, described remaining capability gaps in the current situation, "The necessary cyber workforce, defensible architecture, situational awareness, operational concepts, authorities, and capabilities are not fully in place. The nation needs a motivated, fully trained, and well-led cyber workforce that understands evolving technologies and adversary TTPs."[35] To execute the Department of Defense 2015 Cyber Strategy, the Pentagon committed to building a 6,000-person cyber mission force and creating 133 teams across the nation by 2016 to defend against threats to US critical computer networks and respond with computer attacks when directed.[36]

Protected systems operating on secure networks will weigh into the adversaries calculus of risk and cost of their actions versus this decreased chance of reward from their malicious cyber actions. In a November 2013 report to President Obama titled "Immediate Opportunities for Strengthening the Nation's Cybersecurity," the President's Council of Advisors on Science and Technology reported, "Future architectures will need to start with the premise that each part of a system must be designed to operate in a hostile environment."[37] While we wait for new systems, part of the total vision today includes consolidating our current information technology infrastructure from many individual networks to as few as required in order to reduce attack surfaces, decrease interfaces, simplify network operations, and improve command and control. The concept decreases the number of separate networks with different security administrators and

firewalls. Bryan Clark, a senior fellow at the Center for Strategic and Budgetary Assessments said, "If they all have their own IT shop, they're only as good as the people in there." Clark continued, "Whereas if you bring it into a larger network, the IT people can use the infrastructure and can protect all the systems in there and move toward protecting the data as opposed to just the network."[38] Overwhelming military cyber power and strong network defenses will deter cyber adversaries' malicious activity.[39] In the Net Force Maneuver concept described by Hunt, Bowes and Gardner, the objective to provide the adversary a confusing picture of our cyberspace infrastructure, thereby causing them to have an incorrect picture of how portions of our cyberspace infrastructure tie to certain missions and operations tasks.[40] The above points on importance strong defense to support deterrence are made clear in Thomas Schelling's *Arms and Influence*. Schelling describes that for a defender to be credible in deterrence they also need a "coercive defense, which inflicts costs and pain on the adversary in hopes of convincing it not to proceed further."[41]

Attribution

Normal criticisms of deterrence strategy are amplified in the cyber domain due to the difficulty of attribution. If we want to be seen as a credible and capable cyber power we have to be able to demonstrate our ability to detect and attribute cyber attacks for retaliation. Assumptions about identity, intent, nature or rationality of a typical cyber adversary can be called into question when forming the basis for retaliation.[42]

Attribution when possible can be very costly and time consuming. This can be best explained in reviewing the Mariposa botnet. The Mariposa botnet slaved together 13 millions computers for malicious criminal behavior. Attempting attribution of the

mariposa botnet highlights the amount of research and work force hours that can be required to track the source IP or cyber actor.[43] The US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team reported that the Mariposa botnet started in May 2009, finally stopped in December 2009, and then much later in February 2010 Spanish authorities arrested three suspects in Spain.[44]

One key challenge in deterring cyber attacks with threats of retaliation stems from any perception by cyber adversary of difficulty or delay by our cyber mission forces of attributing cyber attacks to a specific cyber attacker. Attribution appears difficult because cyber attacks are often very difficult to identify. The U.S. must be able to move past probable assessments of attribution to facts and hard evidence. To be ahead of the cyber adversary in the find and fix portions of the targeting cycle we will partially depend on our cyber mission forces intelligence efforts to predict when a cyber attack will occur, but this intelligence tip-off will not always happen. If our intelligence teams are not able to warn us of an attack or confirm non-action by other state actors, we must at a minimum be able to quickly identify true cyber attacks from other computer network issues.

Case Study on Attribution

When cyber attacks are identified they are still difficult to attribute to a specific cyber actor or even to a state adversary. The STUXNET worm that slowed the Iranian nuclear weapons program remains non-attributed. David Aucsmith narrows the cyber attribution problem down to two issues that make it difficult, but not impossible. He first states, "The design of cyberspace itself, the nature of the technology that created the computer and communications network we know as cyberspace, does not support an

irrevocable mapping between individuals, addresses, routing and actions." His second point, "The implementation of cyberspace does not prevent someone from spoofing the origin, the route, or the accountability of such actions."[45] David Aucsmith identified the following techniques that are available now for our cyber mission forces to attempt attribution in the cyber domain. Collecting information at the crime scene, infrastructure providers cooperating to pull the evidence together from ephemeral data in saved logs, law enforcements legal access to cyber nodes, data collection, non-cyber information related to the information, and close access intelligence techniques all increase possibilities of accurate and timely cyber attribution.[46]

Effective Communication

Effective communication within a cyber deterrence scenario supports U.S. capability and credibility strategy. Effective communications will convince the adversary of the U.S. ability to conduct decisive operations and the national leadership willingness to employ that force.[47] We must be able to provide strategic public, or sometimes private, statements about our capabilities to quickly detect and attribute cyber attacks to a specific cyber attacker to make our threats or cyber punishment believable.[48] This communication can be written or oral. A well written policy toward an intended audience can clearly communicate desired actions for the audience to take or to stop taking. It will also clearly identify the risk or negative results for them if they do not follow the policy. Communicating a cyber deterrence policy has value beyond the malicious adversary. Currently, honest and ethical computer users are deterred from violating organizational policy concerning their use of cyberspace. This

example shows that deterrence by threat of retaliation does exist in cyberspace, but only against users who have a tangible risk and fear certain retaliation.[49]

U.S leadership must see the importance of effective communication during the cyber attribution process. The deterrence message we send during an attack must clearly aim at stopping an attack by targeting the adversary's psychology and making them recalculate the cost to benefit ratio. Speaking on the importance of deterrence messaging and attribution Secretary of Defense Ash Carter said, "We like to deter malicious action before it happens and we like to be able to defend against incoming attacks as well as pinpoint where an attack came from."[50]

To deter cyber actions before they occur, we must communicate persuasive information on the military power our cyber mission forces possess. A great example of public communication that showed the U.S. military as a credible cyber power capable of attribution and retribution came during an October 2010 NATO Defense Ministers meeting from then U.S. Secretary of Defense Leon Panetta stated, "Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for actions that may try to harm America." "If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us," he said. This was a clear message that the U.S military was willing and capable to act preemptively if it detects an imminent threat of cyber attack.[51] Success of our cyber deterrence strategy will rely on our ability to manipulate the actions of potentially hostile cyber actors through issuing timely and appropriate threats that include

employment of all elements of national power to protect the US from cyber attacks in a highly technical and complex future.

Recommendations

1. Strategist need to believe that cyber deterrence will work. Too often during the research I came across passages from early researchers that felt it necessary to compare cyber deterrence with nuclear deterrence and make the point that cyber deterrence would not work due to the issues with attribution and difficulties of increasing the cost and risk ratio. Cyber deterrence will work like all other types of deterrence by making an adversary believe it will not achieve their goal and the cost and risk outweigh any possible positive outcome of their actions. The basic understanding of how deterrence works should not be lost on framework changes in the cyber environment or other advances in technology.
2. Execute the build and training of cyber forces. For cyber deterrence to be a successful strategy we must have a capable and credible cyber mission force ready to fight through attacks in cyberspace and carry the fight to the adversary when required. Our cyber force must be able to provide precise attribution for malicious cyber operations against our critical infrastructure. A quick and credible total government response, not just a cyber response, needs to be communicated and acted on. This will deny an adversary benefits should it desire to attack and increase the odds that they stop.
3. Strengthen defense of our critical networks. US cyber deterrence strategy will benefit from or can be totally achieved through a strong computer network defense. Defending a critical network compares closely with a descriptive image of defending

a kingdom. Just like a deterring an attack on a kingdom it easy to describe actions to protect and deter malicious actions against our critical networks. Castles need to be strongly guarded at the gate. High walls and a moat will deter adversaries from attacking. Strong and well trained soldiers that outnumber all adversaries that would consider an attack on the kingdom are needed. Our superior weapons and our dependable allies that the adversaries fear will immediately influence the risk calculus deterring them from attack. Our extended defense with forts and lookouts searching outside the perimeter providing current intelligence of any enemies still in the distance that are forming and preparing to move toward the castle. The castle image relays how cyber deterrence will work if you stick with the basic elements of deterrence theory. If we can successfully deter an adversary's cyber attack plans and operational goals by regularly and randomly changing our critical networks nodes, devices, and security tactics, techniques, and procedures (TTP) it leaves our adversaries previously captured knowledge of our network vulnerabilities worthless and thereby increases the cost and difficulty of a cyber attack enough to deter them.[52] Every cyber adversary can be convinced that our strong network defense combined with our overwhelming response in military power, best trained forces and full stockpile of weapons choices from knifes to nuclear weapons, or from diplomacy and economic sanctions will ultimately deny them any benefit from malicious cyber activity against the US.

4. Deliver clear strategic messages regarding cyber attacks. For the cyber adversary to be deterred the US needs to clearly communicate desired actions for the adversary to

take or to stop taking. The message needs to encourage adversary restraint or quickly suffer costs and ultimately gain no benefit from their malicious activity.

5. If deterrence fails. The U.S. and its allies should never completely rely on any type of deterrence and we must have a plan to address failure of cyber deterrence.[53] Joint doctrine identifies the concern that deterrence might not work. Joint Pub 5.0 describes six different phases of an operation or campaign plan. Phase I reflects current doctrine to deter undesirable adversary action by demonstrating the capabilities and resolve of the joint force. It includes activities to prepare forces and set conditions for deployment and employment of forces in the event that deterrence fails.[54] Knowing a cyber adversary will not always be deterred from using their forces for a cyber attack on the U.S or its allies, we must have a credible cyber force that will make them choose to stop the attack with a coercive defense. To be credible our cyber force training and exercising must ensure that our forces can defend the cyber domain, reconstitute our damaged networks, operate safely and continue the mission with minimal time lost and data and equipment casualties.[55]

Conclusion

Cyber deterrence provides a viable strategy. Cyber deterrence can prevent current or future malicious actors from attacking our critical infrastructure because of the severe risk. Criminal deterrence, conventional warfare deterrence, nuclear warfare deterrence and cyber deterrence all are similar in that they all are in place to cause the prevention from action by fear of the consequence. The above examples of deterrence all are successful by making an adversary believe it will not achieve their goal and the cost and risk outweigh any possible outcome of their actions. Cyber deterrence requires overt

messaging. Clear signals are required of our intent and capability to carry out threats. Clear messaging provides the cyber adversary enough information to consider and weigh the cost and risks of their actions correctly. Commitment to capability and credibility must be reflected in our future cyber military build-up as well as the other dimensions of our military. We must possess a strong and capable military to maintain credibility in a cyber crisis. In the fog of overly complicated cyberspace technology, attribution of cyber operations seems difficult, but cyber deterrence can still be a viable strategy if the United States can increase its status as a credible and capable global cyber power. The importance of credibility, capability and attribution as they relate to the US creating an effective cyber deterrence strategy for employing all elements of national power to protect the US from cyber attacks in a highly technical and complex future needs to be understood and incorporated in future U.S. strategy.

[1] Secretary of Defense Ash Carter, *Department of Defense Cyber Strategy*, April 2015, pg 10 http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, (last accessed 30 January 2016)
[2] Cheryl Pellerin, *Rogers Discusses Cyber Operations, ISIL, Deterrence.* DOD NEWS, Defense Media Activity, March 2015. http://www.defense.gov/News-Article-View/Article/604201, (last accessed 30 January 2016)
[3]"Understanding Deterrence." Chapter 3 in *Deterrence in the Twenty-first Century.*, edited by Anthony Christopher Cain, by Adam Lowther, London, UK: Proceedings, pg 39.
[4] Cesare Beccaria, *Of Crime and Punishment*, Chap 12, http://www.constitution.org/cb/crim_pun.htm (last accessed 30 January 2016)
[5] Lawrence Freedman, *Deterrence*. Cambridge, UK: Polity Press, 2004, pg 6.
[6] Bernard Brodie and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co, 1946. pg 31
[7] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, pg 67. (As Amended Through 15 January 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (last accessed 31 January 2016).
[8] "Deterrence in Cyberspace." *In Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, edited by Adam Lowther, by Kamal T. Jabbour and E. Paul Ratazzi. Air University Press, 2013, pg 43.
[9] "Deterrence and Saddam Hussein." Chapter 11 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, by Barry Schneider, May 2009, 159-160
[10] Ibid.
[11] Jabbour, *Deterrence in Cyberspace*, 47.
[12] Jabbour, *Deterrence in Cyberspace*, 47.
[13] Jabbour, *Deterrence in Cyberspace*, 45.
[14] Martin C. Libicki, Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND, 2009, pg 23.
[15] Ibid., 23-24.
[16] Freedman, *Deterrence*, 29,
[17] Dorothy E. Denning, *Rethinking the Cyber Domain and Deterrence*, Joint Force Quarterly, NDU press, Issue 77 2nd Quarter 2015, pg 11. http://www.dtic.mil/doctrine/jfq/jfq-77.pdf (last accessed 30 January 2016)
[18] Freedman, *Deterrence*,30.
[19] Michael Howard and Peter Paret. Carl Von Clausewitz: *On War*, 8th Print. Ed. (Princeton, NJ: Princeton University Press, 1984, pg 178.
[20] Jason Andress and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd. ed. Amsterdam [etc.: Elsevier/Syngress, 2014, pg 269
[21] Freedman, *Deterrence*,36.
[22] Daryl G. Press, *Calculating Credibility: How Leaders Assess Military Threats.* Ithaca, N.Y.: Cornell University Press, 2005, page 1
[23] Ibid., 3
[24] Ibid., 6

[25] Ibid., 6
[26] "Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation." In *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, edited by Adam Lowther, by Kevin Beeker, Robert Mills, Michael Grimaila, and Michael Haas. Air University Press, 2013, pg 20
[27] Freedman, *Deterrence*, 31.
[28] "Framing Deterrence in the Twenty-First Century: Conference Summary" Chapter 1 in *Deterrence in the Twenty-first Century.*, edited by Anthony Christopher Cain, by Adam Lowther, London, UK: Proceedings, pg 4.
[29] Carter, *Department of Defense Cyber Strategy*,10.
[30] Beeker, Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation, pg 26.
[31] Beeker, Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation, pg 26.
[32] Department of Defense Cyber Security and Compliance Initiative (DC3I) September 2015. http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf (last accessed 30 January 2016)
[33] Jabbour, Deterrence in Cyberspace, 43
[34] Mike McConnell, "*Mike McConnell on How to Win the Cyberwar We're Losing,*" Washington Post, February 28, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html, (last accessed 30 January 2016)
[35] ADM Mike S. Rogers, *Beyond the Build*, June 2015 http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf, (last accessed 30 January 2016)
[36] Carter, Department of Defense Cyber Strategy, 6
[37] Executive Office of the President, PCAST. *Report to the President – Immediate Opportunities for Strengthening the Nation's Cyber Security*. November 2013, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf, (last accessed 30 January 2016)
[38] Daniel P. Taylor, *Under One Cyber Roof*, in Seapower Magazine. December 2014. http://www.seapower-digital.com/seapower/december_2014?pg=16#pg16 (last accessed 30 January 2016).
[39] Lowther, Understanding Deterrence, 27.
[40] Carl Hunt, Jeffrey R. Bowes, and Doug Gardner. "*Net Force Maneuver.*" Proceedings of the 2005 IEEE Workshop on Information Assurance and Security. West Point, NY: US Military Academy, 2005, pg 419-423.
[41] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 54-55.
[42] Jabbour, Deterrence in Cyberspace, 43.
[43] Steve Winterfeld and Jason Andress. *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham, MA: Syngress, 2012, pg 123.
[44] ICS CERT, *Advisory (ICSA-10-090-01)*, last revised Jan20,2014 https://ics-cert.us-cert.gov/advisories/ICSA-10-090-01, (last accessed 11Feb2016)

[45] "The Technology and Policy of Attribution." In *#Cyberdoc: No Borders – No Boundaries*, edited by Timothy R. Sample and Michael S. Swetnam, by David Aucsmith, Arlington, VA: Potomac Institute Press, 2012. pg 13-30.
[46] Ibid.
[47] Joint Publication 3.0, Joint Operations, 11 August 2011, page V-20, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (last accessed 11 February 2016)
[48] "Waging Deterrence in the Twenty First Century" Chapter 5 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, by Gen. Kevin Chilton, USAF and Greg Weaver, May 2009, pg 72.
[49] Jabbour, Deterrence in Cyberspace, 44.
[50] Cheryl Pellerin, *Carter Unveils New DoD Cyber Strategy in Silicon Valley*, DoD News, Defense Media Activity, April 2015, pg 1. http://www.defense.gov/News-Article-View/Article/604511. (Last accessed 30 January 2016).
[51] Phil Stewart, U.S. *Defense Chief says pre-emptive action possible over cyber threat*, Oct 11, 2012, http://www.reuters.com/article/net-us-usa-cyber-pentagon-idUSBRE89B04Q20121012#LPFMccqlsklxmtBV.99 (last accessed 30 January 2016)
[52] Jabbour, Deterrence in Cyberspace, 46.
[53] "Defining Deterrence" Chapter 2 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, by Michael Cosner, May 2009, pg 21.
[54] Joint Publication 5.0, *Joint Operations Planning*, 11August 2011, page III-42. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (last accessed 30 January 2016)
[55] Beeker, Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation, pg 20.

Bibliography

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd. ed. Amsterdam [etc.: Elsevier/Syngress, 2014.

Beccaria, Cesare. *Of Crime and Punishment*, Chap 12, http://www.constitution.org/cb/crim_pun.htm (last accessed 30 January 2016)

Brodie, Bernard and Frederick Sherwood Dunn. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co, 1946.

Cosner, Michael, "Defining Deterrence" Chapter 2 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, May 2009.

Denning, Dorothy E. *Rethinking the Cyber Domain and Deterrence*, www.dtic.mil/doctrine/jfq/jfq.htm, Joint Force Quarterly, NDU press, Issue 77 2nd Quarter 2015.

Department of Defense Cyber Security and Compliance Initiative (DC3I) September 2015 http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf (last accessed 30 January 2016)

"Deterrence and Saddam Hussein." Chapter 11 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, by Barry Schneider, May 2009,

"Deterrence in Cyberspace." *In Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, edited by Adam Lowther, by Kamal T. Jabbour and E. Paul Ratazzi. Air University Press, 2013.

Executive Office of the President, PCAST. *Report to the President – Immediate Opportunities for Strengthening the Nation's Cyber Security*. November 2013, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf (last accessed 30 January 2016)

"Framing Deterrence in the Twenty-First Century: Conference Summary" Chapter 1 in *Deterrence in the Twenty-first Century.*, edited by Anthony Christopher Cain, by Adam Lowther, London, UK: Proceedings,

Freedman, Lawrence. *Deterrence*. Cambridge, UK: Polity Press, 2004.

Howard, Michael, and Peter Paret. Carl Von Clausewitz: *On War*, 8th Print. Ed. (Princeton, NJ: Princeton University Press, 1984.

Hunt, Carl, Jeffrey R. Bowes, and Doug Gardner. "*Net Force Maneuver*." Proceedings of the 2005 IEEE Workshop on Information Assurance and Security. West Point, NY: US Military Academy, 2005.

ICS CERT, *Advisory (ICSA-10-090-01)*, last revised Jan20,2014 https://ics-cert.us-cert.gov/advisories/ICSA-10-090-01, (last accessed 11Feb2016)

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010 (As Amended Through 15 January 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (last accessed 31 January 2016).

Joint Publication 3.0, Joint Operations, 11 August 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (last accessed 11 February 2016)

Joint Publication 5.0, *Joint Operations Planning*, 11August 2011. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (last accessed 30 January 2016)

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

McConnell, Mike. "*Mike McConnell on How to Win the Cyberwar We're Losing,*" Washington Post, February 28, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (last accessed 30 January 2016)

"Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation." In *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, edited by Adam Lowther, by Kevin Beeker, Robert Mills, Michael Grimaila, and Michael Haas. Air University Press, 2013.

Pellerin, Cheryl. *Carter Unveils New DoD Cyber Strategy in Silicon Valley*, DoD News, Defense Media Activity, April 2015. http://www.defense.gov/News-Article-View/Article/604511. (last accessed 30 January 2016)

Pellerin, Cheryl. *Rogers Discusses Cyber Operations, ISIL, Deterrence.* DOD NEWS, Defense Media Activity, March 2015. http://www.defense.gov/News-Article-View/Article/604201 (last accessed 30 January 2016)

Press, Daryl Grayson. *Calculating Credibility: How Leaders Assess Military Threats.* Ithaca, N.Y.: Cornell University Press, 2005.

Rogers, ADM Mike S. *Beyond the Build*, June 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf (last accessed 30 January 2016)

Secretary of Defense Ash Carter, *Department of Defense Cyber Strategy,* April 2015.http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (last accessed 30 January 2016)

Stewart, Phil. *U.S. Defense Chief says pre-emptive action possible over cyber threat*, October 11, 2012, http://www.reuters.com/article/net-us-usa-cyber-pentagon-idUSBRE89B04Q20121012#LPFMccqlsklxmtBV.99 (last accessed 30 January 2016)

"The Technology and Policy of Attribution." In *#Cyberdoc: No Borders – No Boundaries*, edited by Timothy R. Sample and Michael S. Swetnam, by David Aucsmith, Arlington, VA: Potomac Institute Press, 2012.

Schelling, Thomas C. *Arms and Influence* (New Haven, CT: Yale University Press, 1966)

Taylor, Daniel P. *Under One Cyber Roof*, in Seapower Magazine, December 2014.

http://www.seapower-digital.com/seapower/december_2014?pg=16#pg16 (last accessed 30 January 2016).

"Understanding Deterrence." Chapter 3 in *Deterrence in the Twenty-first Century*., edited by Anthony Christopher Cain, by Adam Lowther, London, UK: Proceedings. September 2010.

"Waging Deterrence in the Twenty First Century" Chapter 5 in *Deterrence in the Twenty-first Century*: London, UK: Proceedings, edited by Anthony Christopher Cain, by Gen. Kevin Chilton, USAF and Greg Weaver, May 2009.

Winterfeld, Steve, and Jason Andress. *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham, MA: Syngress, 2012.