Lessons for Cyber Policymakers

by James Torrence

> ***Critical infrastructure keeps our food fresh, our houses warm, our trade flowing, and our citizens productive and safe. The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.***
>
> ***—2017 U.S. National Security Strategy***

Cyberspace is the newest domain of warfare.[1] In cyberspace, the attacker has the advantage over the defender.[2] Cyberspace is unique because it "offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests" without requiring a physical presence.[3] In the 2006 U.S. National Security Strategy, the word "cyber" was mentioned one time in parentheses.[4] By 2017, the U.S. National Security Strategy states that: "America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."[5] This rapid rise of cyber means policymakers have had little time to develop cybersecurity strategies. To develop an effective foundation for the creation of a cybersecurity strategy, cyber policymakers must learn from Cold War deterrence theory and application. The Cold War dealt with a new type of warfare, rapidly evolving technology, and an environment dominated by the offense, which mirrors the current challenges in cyberspace. Analysis of Cold War deterrence theory identifies specific principles of deterrence and strategy cyber policymakers can apply to cyber defense.

James Torrence is an Army officer in the Signal Corps. He is a graduate of the United States Military Academy. He is currently the battalion operations officer for the 41st Signal Battalion in Camp Humphreys, Korea. He holds five master's degrees including cybersecurity, military art and science, and strategic design. He is currently working towards his doctorate in strategic security.

Defining and Categorizing Cyber Deterrence

Cold War deterrence theorists such as Schaub, Quackenbush, Morgenthau, Huth, and Russet assert that deterrence necessitates a threat on the part of the defender.[6] The problem with a threat-based deterrence theory in cyberspace is that success requires the defender to communicate the threat to all potential attackers, which is not possible. Smoke, George, Brodie, Nye, and Kahn all contend that deterrence does not necessitate a threat, but the defender must still dissuade the potential attacker from initiating action through some form of communication.[7] Furthermore, Smoke, George, Payne, and Freedman argue that effective deterrence requires state-specific communication strategies that take into account unique aspects of each potential attacker.[8] Communication of threats, or cost to potential attackers, is not possible in the current cyber operating environment, which creates the first of two dilemmas for cyber policymakers.

The first cyber deterrence dilemma facing U.S. cyber policymakers is, How can the U.S. deter cyberattacks on infrastructure critical to its national security from the range of potential attackers in cyberspace without being able to communicate the threat or cost to potential attackers? The answer is general strongpoint cyber deterrence. General strongpoint cyber deterrence is the implementation of cyber-specific defensive measures that deny state and nonstate actors with limited resources the ability to attack infrastructure critical to national security without requiring any communication from the defender. Kennan argued that strongpoint defense "allowed the United States to choose the most favorable terrain upon which to confront the Soviet Union."[9] Nye further argued that "by chewing up an attacker's resources and time, a potential target disrupts the cost-benefit model that creates an incentive for attack."[10] General strongpoint cyber deterrence takes lessons from Kennan and Nye because it involves a focused defense on critical infrastructure that creates a high cost for the attacker, forcing him to expend more resources than anticipated. General strongpoint cyber deterrence also forces the attacker to move on to an easier target that is favorable digital terrain for the U.S. No deterrent can stop all attacks, but general strongpoint cyber deterrence can limit the pool of potential attackers to state actors with enough resources for a prolonged cyberattack. With the pool of potential initiators limited, the state-specific communication strategies championed by Smoke, George, Freedman, and Payne can be used by cyber policymakers for further deterrence against resourced state actors looking to harm critical infrastructure.[11]

Communication of threats, or cost to potential attackers, is not possible in the current cyber operating environment...

The second cyber deterrence dilemma facing U.S. cyber policymakers is, How can the U.S. further deter state actors who have the resources to circumvent defenses erected for general cyber deterrence from attacking infrastructure critical to national security? The answer is specific cyber strongpoint deterrence. Unlike general cyber strongpoint deterrence, specific cyber strongpoint deterrence strategies must account for communication with potential initiators, potential attacker rationality, the limits of attribution, and the regional and political contexts in which an attack may occur.[12] The definition of specific cyber strongpoint deterrence, which borrows heavily from Keith Payne, is the focused application of elements of national power against a specific actor accounting for: 1) the potential object of his friction; 2) his motivation and goals (expected gain from attacking); 3) his level of determination; 4) his likelihood of attacking; 5) how he makes decisions; 6) the regional political and security context in which the attack will occur; and 7) the likelihood of attribution if he attacks.[13] Unique, state-focused strongpoint cyber deterrence can be effective in communicating the costs of potential attacks to a finite number of actors. Furthermore, using the right mix of elements of national power against potential attackers can prolong the length of time a cyberattack takes, which increases the chance of attribution. Concentrating defensive efforts against specific actors also increases the chance of diverting potential initiators away from attacking infrastructure critical to national security.

Cyber policymakers must implement general and specific strongpoint cyber deterrence to effectively defend critical infrastructure from cyberattacks.

Cyber policymakers must implement general and specific strongpoint cyber deterrence to effectively defend critical infrastructure from cyberattacks. Data is the critical infrastructure in cyberspace, which means cyber policymakers must account for the protection of data to create effective general cyber deterrence policies that can enable specific cyber strongpoint deterrence. Encryption, decentralization, and concealment are three principles that require application to data critical to national security for effective general cyber strongpoint deterrence.

Encryption

Herman Kahn recognized that shelter is an important component of protecting infrastructure critical to national security.[14] Kahn argued that "shelter tends to be a good deal more stable than quick reaction alone as a defense" and that "the number of ways in which it can fail seem relatively low."[15] Finally, shelter is part of a broader defense strategy for strategic nuclear forces (SNF) that also includes mobility, concealment, and dispersion. By itself, shelter is not a complete deterrent, but when combined with mobility, concealment, and dispersion, it creates uncertainty for the enemy regarding the location and disposition of SNF. Shelter for nuclear forces parallels encryption in cyberspace where data critical to national security requires protection and hardening from direct enemy attacks. Encryption means "to cipher or encode," which helps protect data from brute-force enemy attacks.[16] Encryption must be used to protect Supervisory and Control Data Acquisition (SCADA) systems that are currently vulnerable and often unprotected.

Cybersecurity researchers Thomas Marsden, Nour Moustafa, Elena Sitnikova, and Gideon Creech highlight that "research into the security of SCADA systems has grown in recent years, as the potential damage to critical infrastructure including gas, electricity, water, traffic and railway, and/or loss of life and subsequent risk to state security have been realized."[17] Though the risks of attacks to SCADA systems have been identified, most studies have unveiled that security is an afterthought at best in SCADA systems.[18] Supervisory control systems are vulnerable because they were built on an assumption that "SCADA infrastructure is a closed control ecosystem of sufficiently complex technologies to provide some security through trust and obscurity."[19] Supervisory control systems, like the internet, do not operate in a closed system and are thus vulnerable to cyberattacks from malicious actors. Not only are legacy SCADA systems (e.g., power grids) vulnerable to attack, but future supervisory control systems involving transmitting data through lasers are also neglecting cybersecurity during research and development.

At the Sixteenth International Conference on Accelerator and Large Experimental Control Systems, a team of sixteen scientists and cybersecurity experts, led by Leonce Mekinda, presented a paper in which they argued that cybersecurity aspects are often not thoroughly addressed in the design of light source SCADA systems currently built on "vulnerable" off-the-shelf software.[20] The most high-profile, light-source, supervisory control system is the European X-Ray Free Electron Laser contained in a 1.4 billion-euro facility that produces 15 TB of data each beam.[21] The European X-Ray Free Electron Laser represents the future of SCADA systems, and there should be special care regarding its security.[22] The thread that connects legacy and future supervisory control systems is the lack of effective encryption. If malicious actors can remotely access U.S. SCADA infrastructure, then the threat of a cyberattack against infrastructure to national security will remain high. If encryption can be implemented that forces actors to devote more time and resources to access the data in cyber systems in the form of a general deterrent, then it affords the U.S. more time to implement specific cyber strongpoint deterrence.

In a 2004 report conducted by the Congressional Research Service, Dana Shea made it clear that:

> Encrypting the information transmitted between remote units and their controllers would inhibit inclusion of false information to and from industrial control systems. Current encryption technology may not be compatible due to the time required to process the encrypted data and the level of technology built into control system components. Industrial control systems have stringent timing requirements and tend to be built out of less computationally robust components, which complicate the use of current encryption technologies. While a prototype encryption method for industrial control systems has been developed, it is still in the validation process and is only recently being evaluated for implementation in industry. Further research into encryption techniques for these processes could provide efficient, market-driven technology for securing industrial control systems information.[23]

Policymakers must learn from Shea's suggestions of investing in the research of encryption techniques to secure SCADA systems.[24] Shea recognized that the injection of false information into SCADA systems could be a major problem, and that current encryption technologies might not be able to control the flow of information in SCADA systems.[25] Shea's suggestions in 2004 are just as relevant in 2019 where SCADA systems are susceptible to enemy attacks because of ineffective encryption.[26] Encryption is not a single solution to protecting SCADA systems, but it should be the first step in a general strongpoint cyber deterrence to create a cost that is beyond the resources of nonstate actors and even some state actors. Policymakers cannot forget the importance of encryption when developing policy for infrastructure critical to national cybersecurity because data in SCADA systems requires protection.[27] After protecting data with encryption, policymakers must understand, as Kahn cautions, that shelter is weakest when the enemy can overwhelm it with an attack that is "larger than the shelters were built for."[28] Encryption, like shelter, can also be overwhelmed by overpowering enemy resources in the form of a brute-force attack, which means it must not be located in a single place for the enemy to concentrate its resources.[29]

Policymakers cannot forget the importance of encryption when developing policy for infrastructure critical to national cybersecurity...

Decentralization

Herman Kahn argued that: "One way to prevent the attacker from mounting too large an attack is to disperse shelters to many distinct target points. This forces downward the number of missiles the enemy can shoot at each point."[30] Lawrence Freedman argued that "mobility and concealment" would "discourage an arms race."[31] The 1958 report, *National Policy Implications of Atomic Parity*, also said: The numbers of missiles will avail the enemy nothing, if he does not know the location of the target. We in effect take an initiative which he can overcome only by maintaining hour-to-hour fire-comb surveillance of all our land areas and vast oceans [for SNF]."[32] The principles of mobility directly applies to SCADA systems in cyberspace where "today's centralized information infrastructure is not resistant (to faults or cyber-attacks), extensible or scalable to accommodate the emerging power grid requirements."[33] In particular, the U.S. power grid is deployed with a largely, centralized information infrastructure, with the Energy Management System acting as the main control center.[34] Cyber policymakers must understand how decentralization applies to cybersecurity strategy to protect infrastructure critical to national security from malicious enemy attacks.

Cyber policymakers must understand how decentralization applies to cybersecurity strategy to protect infrastructure critical to national security from malicious enemy attacks.

Network decentralization describes the use of distributed systems and the externalization of software system components.[35] Decentralized networks are the foundation of the cloud which "describes a network-based computer system, which can be used for organizational and technological integration into decentralized information systems, based on cloud computing technology."[36] Florian Kelbert, a research engineer that specializes in information security and privacy, and software engineer Alexander Pretschner argue that "due to the ever-increasing value of data, the continuous protection of sensitive data throughout its entire lifetime has drawn much attention" and that a "decentralized infrastructure overcomes many problems omnipresent in a centralized approach."[37]Kelbert and Pretschner also argue that decentralized networks are superior to the current centralized structure because "deploying all components locally and by replicating data to different locations, there is no single point of failure and no need for a central component to be always available for all clients."[38] Furthermore, Kelbert and Pretschner contend that while a solution to data security "could naively be implemented in a centralized fashion, such a solution imposes drawbacks such as being a single point of failure, and "a centralized solution is also expected to impose significant performance and network communication overhead."[39] Decentralization of data that controls and resides within infrastructure critical to national security must be a tenet of any cybersecurity deterrence strategy to add an additional layer of complexity to encrypted data and create uncertainty for the attacker.

Young-Jin Kim, Marina Thottan, Vladimir Kolesinkov, and Wonsuck Lee, a group of experts ranging from electrical engineering to cryptography, argue that an "important differentiator for the next generation power grid is the massive amounts of measurement data that will be made available at distributed locations that can and must be leveraged optimally to operate the power grid."[40] The arguments of Kim, Thottan, Kolesinkov, Lee, Kelbert, and Pretschner are the cyber equivalent to arguments for decentralization made by Brodie, Kahn, Freedman, and the Naval Warfare Group.[41] Cybersecurity policymakers must incorporate decentralization into their general and specific deterrence strategies because it creates uncertainty as to the location of data that is critical to national security. When the defender can ensure that data critical to national security is never centralized and constantly moving, the attacker never has the opportunity to mass his offensive capabilities against one particular location. Decentralized data also makes encryption even more important because it adds a layer of security that increases the cost for the attacker. Not only do attackers need to find the location(s) of data critical to national security, they must also defeat the defender's encryption at each location that contains portions of the data. Cyber policymakers that understand the necessity of data centralization can shape an environment that is advantageous for the defender. Cyber policymakers must also understand how to augment the effects of encryption and decentralization by concealing the whereabouts and type of encryption of data critical to national security.

Concealment

Bernard Brodie, Herman Kahn, Martin Van Creveld and Lawrence Freedman championed concealment for SNF.[42] Brodie argued that concealed SNF (along with sheltered and dispersed) made it more likely that SNF would survive a first strike and less likely that the attacker would surprise the defender.[43] Kahn thought that concealment by "continuous mobility or reasonably frequent changes of position" challenged the enemy's intelligence and created confusion and force them to expend resources creating a larger attacking force.[44] Van Creveld highlighted multiple courses of action considered by the U.S. for concealment of SNF to include subterranean tunnels with tracks, missiles dug thousands of feet deep and launched from underground after surviving an attack, and platforms that would "crawl over the bottom of the lakes."[45] Freedman thought concealment (and mobility) discouraged an arms race because "numbers of missiles will avail the enemy nothing, if he does not know the location of his target."[46] Analysis of concealment by Brodie, Kahn, Van Creveld, and Freedman directly applies to cyberspace because "infrastructure that causes the greatest concern in the cyber war literature, industrial control systems, can also be protected by deception."[47]

Even with a general cyber deterrent in place, one must assume an adversary will breach border controls and establish footholds within the defender's network...

Even with a general cyber deterrent in place, one must assume an adversary will breach border controls and establish footholds within the defender's network, so studying and engaging the adversary on the defender's turf will influence any future moves.[48] Dr. Kristin E. Heckman, lead scientist at The MITRE Corporation in McLean, VA, and a team of MITRE scientists argued that a key component in an environment in which an attacker will enter the defender's network even with the most elaborate security measures is "cyber denial and deception."[49] Furthermore, Heckman and her team said:

> The goal of D&D [denial and deception] is to influence another to behave in a way that gives the deceiver an advantage, creating a causal relationship between psychological state and physical behavior. Denial actively prevents the target from perceiving information and stimuli; deception provides misleading information and stimuli to actively create and reinforce the target's perceptions, cognitions, and beliefs. Both methods generate a mistaken certainty in the target's mind about what I s and is not real, making the target erroneously confident and ready to act.[50]

Heckman and the scientists at MITRE made it clear that adding a layer of deception in the form of concealing information for which the attacker is searching adds another layer of complexity to deterrence by denial.[51] Political scientists Erik Gartzke and Jon R. Lindsay further discuss deception in the cyber domain and claim:

> Deception is logically different from denial even though they are often combined. Pure defense is the act of physically confronting attackers so that they cannot cause harm to the assets that are being defended. Deception, by contrast, conceals assets and pitfalls from the enemy."[52]

Gartzke and Lindsay further argue that "cyberspace heightens the effectiveness of deception" and "an adversary that wanted to complain about defensive deception would also have first to revel its identity."[53]

Cyber deception can augment general strongpoint cyber deterrence by further concealing information even if an attacker makes it through a cyber defense.

In an experiment involving cyber deception, Gartzke and Lindsay found "in one real-time red-team versus blue-team cyber war game experiment, a honeypot[54]system failed to deny red-team hackers access to the command and control mission system, but decoys and disinformation did succeed in preventing the adversary from obtaining sensitive data."[55] Heckman and scientists from MITRE also found that "traditional denial and deception techniques were effective in denying the adversary access to real information on the real command and control mission system, and instead provided the adversary with access to false information on a fake command and control mission system."[56]

Gartzke, Lindsay, Heckman, and MITRE scientists make it clear that deception will have a major impact on a defender's ability to deter in cyberspace.[57] Jeffrey Pawlick, U.S. Army Research Laboratory, Edward Colbert, U.S. Army Research Laboratory, and Quanyan Zhu, New York University Tandon School of Engineering, further researched cyber deception and developed a taxonomy that defined six types of deception, "perturbation, moving target defense, obfuscation, mixing, honey-x, and attacker-engagement."[58] Pawlick, Colbert, and Zhu's analysis does not argue that any one type of deception is the best in cyberspace, but rather break methods of concealing information through deception down into different categories.[59] Cyber deception can augment general strongpoint cyber deterrence by further concealing information even if an attacker makes it through a cyber defense. Concealment of information can drive up the cost, time, and complexity for the attacker; create more time for the defender to attribute an attack; and filter out more potential attackers. Cyber policymakers must understand how to incorporate concealment in conjunction with encryption and decentralization into a general strongpoint cyber deterrent to create a layered approach that limits the number of potential attackers and affords the U.S. an opportunity to implement a specific strongpoint cyber deterrence against a manageable number of initiators.

Conclusion

Cybersecurity deterrence requires a forward-thinking approach and not a reliance on specific solutions. Analysis of Cold War deterrence theory results in the following lessons from which cybersecurity policymakers must learn and incorporate to develop a forward-thinking approach to defending critical infrastructure in cyberspace:

1. The initial layer of cyber deterrence must be focused on denying potential attackers because it is not possible to communicate with all potential initiators.

2. Threat-based deterrence is not possible in cyberspace unless the range of potential attackers is greatly reduced.

3. Cyber deterrence must be focused on strongpoints because a perimeter defense will be costly for the defender, and not effective against potential initiators. Strongpoints in cyberspace are infrastructure critical to national security.

4. Critical infrastructure in cyberspace should be encrypted, decentralized, and concealed to increase the cost for the attacker, buy time for the defender, and increase the chance of attribution of the attacker.

5. Resources must be allocated to researching emerging and future capabilities to create innovation opportunities for long-term cyber defense.

6. A technology-focused general strongpoint cyber deterrent creates the opportunity for an actor-specific specific strongpoint cyber deterrence strategy that leverages the elements of national power beyond just cyber defense technology.

7. Specific strongpoint cyber deterrence that leverages the elements of national power and actor-specific considerations can be used following the employment of a general strongpoint cyber deterrent to target a limited number of potential initiators with the resources to target U.S. infrastructure critical to national security.

The long-term approach to cyber defense must use a framework with the lessons identified from Cold War deterrence theory and implementation. A framework is a set of adaptable principles that can be applied to evolving problem-sets. Cybersecurity is an evolving problem-set that must have adaptable policymakers capable of simultaneously addressing current and long-term threats through the implementation of general and specific strongpoint cyber deterrence. General and strongpoint cyber deterrence that leverages the lessons identified during the Cold War and applies them to cyberspace will have a foundation on which to build iterative cyber defenses that continually incorporate new technology to address evolving threats. ***IAJ***

NOTES

[1] Christos Athanasiadis and Rizwan Ali, "Cyber as NATO's Newest Operational Domain: The Pathway to Implementation," *Cybersecurity: A Peer-Reviewed Journal*, Vol. 1, No. 1, p. 2017, p. 48, <http://www.ingentaconnect.com/content/hsp/jcs/2017/00000001/00000001/art00006>, accessed on January 26, 2018.

[2] *The Department of Defense Cyber Strategy*, Department of Defense, Washington, D.C., April 2015, p. 10, <https://www.defense.gov/Portals/1/features/2015/0415_cyber strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>, accessed on September 16, 2017; Defense Advanced Research Projects Agency Director Regina E. Dugan, testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Washington, D.C., March 1, 2011, pp. 16–17, <https://www.darpa.mil /attachments/TestimonyArchived%20(March%201%202011).pdf>, accessed on January 17, 2018; Kristin M. Lord and Travis Sharp (eds.), "America's Cyber Future: Security and Prosperity in the

Information Age: Volume 1," project report, June 2011, Center for a New American Security, Washington, D.C., 2011, p. 28, <https://s3.amazonaws.com /files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238>, accessed on November 25, 2017.

3 Donald Trump, *National Security Strategy of the U.S.*, The White House, Washington, D.C., p. 12.

4 George W. Bush, *National Security Strategy of the U.S.*, p. 44, <https://www.state.gov /documents/organization/64884.pdf>, accessed on December 30, 2017.

5 Ibid.

6 Gary Schaub, Jr., "Deterrence, Compellence, and Prospect Theory," *Political Psychology*, Vol. 25, No. 3, 2004, pp. 389–411, <https://www.jstor.org/stable/3792549, accessed on August 25, 2017; Stephen Quackenbush, "Deterrence Theory: Where Do We Stand?" *Review of International Studies*, Vol. 37, No. 2, 2011, p. 741, <https://www.jstor.org/stable/23024618>, accessed on August 25, 2017; Han J. Morgenthau, "The Four Paradoxes of Nuclear Strategy," *The American Political Science Review*, Vol. 58, No. 1, 1964, p. 24, <https://www.jstor.org/stable/1952752>, accessed on August 31, 2017; Paul Huth and Bruce Russett, "Testing Deterrence Theory: Rigor Makes a Difference," *World Politics*, Vol. 42, No. 4, 1990, p. 469, <https://www.jstor.org/stable/2010511?seq=1#page_scan_tab_contents>, accessed on August 25, 2017.

7 Alexander L. George and Richard Smoke, "Deterrence and Foreign Policy," *World Politics*, Vol. 41, No. 2, 1989, p. 182, <https://www.jstor.org/stable/2010406?seq=1#page _scan_tab_contents>, accessed on August 25, 2017; Bernard Brodie, *Strategy in the Missile* Age, Princeton University Press, New Jersey, 1959, p. 179; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3, 2017, p. 52, <https://www.mitpressjournals.org /doi/abs/10.1162/ISEC_a_00266>, accessed on September 26, 2017; Herman Kahn, *On Thermonuclear War*, Princeton University Press, NJ, 1960, p. 285.

8 Lawrence Freedman, "Deterrence and the Balance of Power," *Review of International Studies*, Vol. 15, No. 3, 1989, p. 201, <https://www.jstor.org/stable/20097179>, accessed on August 25, 2017; Keith Payne, *The Fallacies of Cold War Deterrence and a New Direction*, The University Press of Kentucky, 2001, p. 31; George and Smoke, p. 181.

9 John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War*, Oxford University Press, New York, 2005, p. 58.

10 Ibid.

11 Freedman, "Deterrence and the Balance of Power," p. 201; Payne, p. 31; George and Smoke, p. 181.

12 Freedman, p. 201; Payne, p. 31; Quackenbush, p. 749; George and Smoke, p. 172; Morgenthau, p. 34; Nye, p. 47; Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*, Rowman and Littlefield, MD, 2017, p. 154.

13 Payne, p. 102.

14 Kahn, p. 262.

15 Ibid.

16 Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, New York, 1999, p. 392.

17 Thomas Marsden et al., "Probability Risk Identification Based Intrusion Detection System for SCADA Systems," p. 1, <https://arxiv.org/ftp/arxiv/papers /1711/1711.02826.pdf>, accessed on February 19, 2018.

[18] Ibid.

[19] Leonce Mekinda et al., "Securing Light Source SCADA Systems," paper presented at 16th International Conference on Accelerator and Large Experimental Control Systems, October 8–13, 2017, p. 1142, <http://icalepcs2017.vrws.de/papers/thbpa02.pdf>, accessed on February 19, 2018.

[20] Ibid., p. 1142.

[21] Ibid.

[22] Ibid.

[23] Dana A. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat," project report, February 2003, Congressional Research Service, Washington, D.C., p. 17, <https://fas.org/irp/crs/RL31534.pdf>, accessed on February 19, 2018.

[24] Ibid.

[25] Ibid.

[26] Marsden et al., p. 2.

[27] Shea, p. 17.

[28] Shea, p. 17.

[29] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996, p 8.

[30] Kahn, p. 263.

[31] Ibid.; Lawrence Freedman, *The Evolution of Nuclear* Strategy, St. Martin's Press, New York, 1981, p. 167.

[32] The quotation is from an unclassified summary of *National Policy Implications of Atomic Parity*, Naval Warfare Group Study, Number 5, 1958, and a speech by Admiral Burke to the Press Club on January 17, 1958, cited in Lawrence Freedman, *The Evolution of Nuclear Strategy*, p. 167.

[33] Young-Jin Kim et al., "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," *IEEE Communications Magazine*, November 2010, p. 58, <https://pdfs.semanticscholar.org/9480/60f857bf4363c2e388ab0b1d1740c42b799c.pdf>, accessed on February 29, 2018.

[34] Ibid., p. 59.

[35] André Müller et al., "Data Security in Decentralized Cloud Systems—System Comparison, Requirements Analysis and Organizational Levels," *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 6, No. 15, 2017, p. 2, <https://link.springer.com/content/pdf /10.1186%2Fs13677-017-0082-3.pdf>, accessed on September 5, 2017.

[36] Ibid.

[37] Florian Kelbert and Alexander Pretschner, "A Fully Decentralized Data Usage Control Enforcement Infrastructure," paper presented at the proceedings of the 13th International Conference on Applied Cryptography and Network Security, June 2015, pp. 1 and 18, <https://www.doc.ic.ac.uk/~fkelbert/papers/acns15.pdf>, accessed on February 17, 2018.

[38] Ibid.

[39] Ibid., p. 2.

[40] Kim et al., p. 59.

[41] Brodie, pp. 76 and 88–91; Kahn, p. 264; Lawrence Freedman, *The Evolution of Nuclear Strategy*, p. 167.

[42] Brodie, p. 181; Kahn, pp. 263–264; Van Creveld, p. 9; Freedman, *The Evolution of Nuclear Strategy*, p. 167.

[43] Brodie, p. 181.

[44] Kahn, pp. 263–264.

[45] Van Creveld, p. 9.

[46] Freedman, *The Evolution of Nuclear Strategy*, p. 167.

[47] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2, 2015, p. 341, <http://dx.doi.org/10.1080/09636412.2015.1038188>, accessed on February 19, 2018.

[48] Kristin E. Heckman et al., "Denial and Deception in Cyber Defense," *Computer*, Vol. 3, No. 4 2015, p. 32, <https://www.researchgate.net/publication/275270540 _Denial_and_Deception_in_Cyber_Defense>, accessed on February 20, 2018.

[49] Ibid.

[50] Ibid.

[51] Ibid., p. 32.

[52] Gartzke and Lindsay, p. 337.

[53] Ibid., pp. 338 and 339.

[54] A honeypot is a program, machine, or system put on a network as bait for attackers. The idea is to deceive the attacker by making the honeypot seem like a legitimate system. A honeynet is a network of honeypots set up to imitate a real network. Honeynets can be configured in both production and research environments. A research honeynet studies the tactics and methods of attackers. This definition was retrieved from the SANS Institute at https://www.sans.org/reading-room/whitepapers/detection/hands-honeypot-365.

[55] Ibid., p. 341.

[56] Kristin E. Heckman et al., "Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment," *Computers and Security*, Vol. 37, September 2013, p. 72, <https://www.sciencedirect.com/science/article/pii/S016740481300076X55>, accessed on February 10, 2018; Kristin E. Heckman et al., "Denial and Deception in Cyber Defense," p. 32.

[57] Ibid.

[58] Jeffrey Pawlick et al., "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy," Submitted for review to ACM Computing Surveys, p. 1, <https://arxiv.org/abs/1712.05441>, accessed on January 18, 2018.

[59] Ibid.