



Captain Jason Simmons and Staff Sergeant Clinton Tips update anti-virus software for Air Force units to assist in the prevention of cyberspace hackers at Barksdale Air Force Base, Louisiana. Photo by the U.S. Air Force/Technical Sergeant Cecilio Ricardo.

## CULT OF THE CYBER OFFENSIVE

### Misperceptions of the Cyber Offense/Defense Balance

By Charles Smythe

#### INTRODUCTION

**A**growing consensus among U.S. military leadership and policy makers is that offensive strategies have an advantage over defensive strategies in cyberspace. However, this consensus is based on a series of misperceptions. The first misperception is the inflation of cyber threats. The second is the misperception that both disruption and espionage strategies

are the same as degradation strategies (deterioration in the operability of information systems). These misperceptions confuse the reality that the cost/benefit calculation of skills and expertise required in degradation operations favors the defense, not the offense. This article explains the logic behind these misperceptions and addresses how they influence assumptions indicating of offensive advantages. Next, the article presents two mechanisms which demonstrate the advantages of defensive strategies. Lastly, the dangers associated with offensive biases and the emergence of a new “cult of the offensive” current cybersecurity strategy are discussed.

#### THE MISPERCEPTIONS OF OFFENSIVE ADVANTAGE

Cyber strategy suffers from two misperceptions: an inflation of threats and a conflation of strategies. In their book *Cyber Strategy: The Evolving Character of Power and Coercion*, Brandon Valeriano, the Donald Bren Chair of Armed Conflict at the Marine Corps University, and Benjamin Jensen, associate professor at Marine Corps University, categorize cyber strategies into three groups: espionage, disruption, and degradation strategies.

Espionage operations seek to obtain advantageous positioning through the theft or manipulation of information. The 2015 hack of the Office of Personnel Management (OPM), which compromised the security of 22 million U.S. citizens’ personal information, is an example of how the Chinese government stole the personal information of U.S. government employees and their contacts.<sup>1</sup> Disruption operations are generally conducted to assess an adversary’s defenses and/or to limit or temporarily deny access to specific information or information systems, typically for propaganda purposes or for political statements. In 2007, Russian government and national hackers conducted a concerted Denial of Service (DDoS) campaign against Estonian government and banking information systems to protest the removal of a statue honoring Russian soldiers who died during World War II.<sup>2</sup> Lastly, there is degradation, which has the objective of damaging an enemy’s networks, operations, or physical information systems. To date, the most notable degradation operation was the U.S. Stuxnet virus which the U.S. employed to target and destroy Iranian centrifuges.<sup>3</sup> The misperception pertaining to the conflation of strategy is that espionage and disruption strategies are often considered to be the same as degradation.

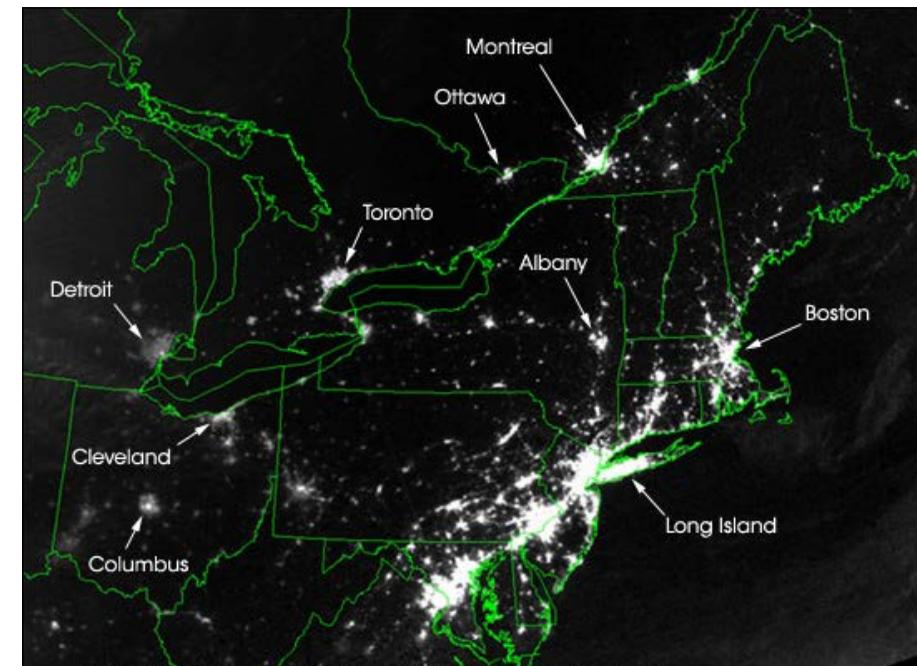
Before delving into the misperceptions surrounding offensive advantage, it is necessary to define cyberspace in order to provide insight into the objectives of cyber strategies. Daniel Kuehl, professor of military strategy and national security policy at National Defense University, considers the defining characteristics of cyberspace to be the utilization of electronics and the electromagnetic spectrum to distribute, cache, manipulate, share, and exploit information through the use of mutually dependent and connected systems of communication devices.<sup>4</sup> The objectives of cyber operations are information and information-based systems, as opposed to the traditional objectives of terrestrial-based warfare.

### Threat Inflation

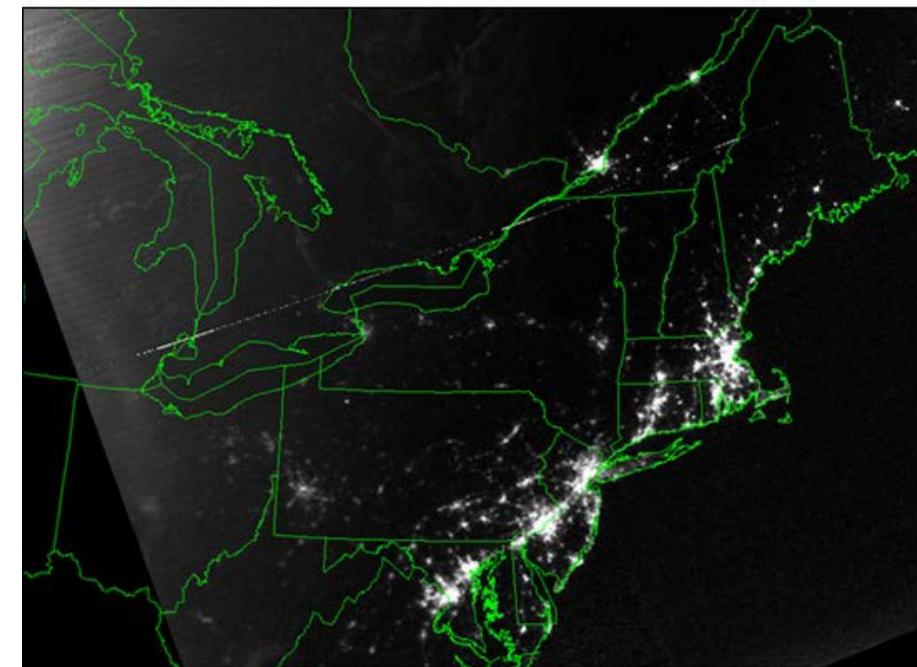
The first misperception that feeds incorrect assumptions of offensive advantage in cyber warfare, threat inflation, generates a fear of the destructive potential of cyberattacks. In 2012, Defense Secretary Leon Panetta warned that the United States faced the threat of suffering a “cyber-Pearl Harbor,” the effects of which could range from train derailments to power grids being shut down.<sup>5</sup>

While Panetta is correct in acknowledging vulnerabilities within infrastructure information systems that could be exploited, his comments echo a growing trend of inflating cyber threats beyond necessity and are problematic in several ways. First, the effects of degradation operations seek to mimic those of real-world effects. For example, a degradation operation targeting the U.S. electrical grid would produce similar effects to that of the 2003 blackout, which impacted a great portion of the northeastern U.S. and Canada. Despite nearly 50 million Americans being affected, power was restored within two days and no outage-related deaths occurred during this period.<sup>6</sup> Additionally, although power was out, satellite imagery of the affected area shows that most affected areas – primarily large population centers – retained power via backup generators, therefore mitigating the impacts of the loss of power [See Figure 1]. Had this scenario been the result of a degradation operation, it fails to paint the catastrophic picture that Panetta’s Pearl Harbor comparison evokes.

As a result, the second problem is that Panetta’s warnings present a fallacy in establishing causal links between opportunity and outcome. In arguing that the existence of certain vulnerabilities could lead to a Pearl Harbor-like catastrophe, he is exaggerating the effects of degradation operations and blurring the lines



August 14, 2003 • 9:29 p.m. EDT • About 20 hours before blackout



August 15, 2003 • 9:14 p.m. EDT • About 7 hours after blackout

Figure 1: Satellite Imagery of the affected area just before and during the 2003 blackout. Note that major population centers still retained significant amounts of electrical power due to backup generators.<sup>7</sup>

between what is possible versus what is actually feasible.<sup>8</sup> Lastly, overstating cyber threats to this degree contributes to threat inflation. Exaggerating the effectiveness or severity of cyberattacks, even to increase awareness of vulnerabilities, distorts both the threat and the needed response. In the case of Panetta's Pearl Harbor scenario, his exaggeration of the threat and the United States' vulnerabilities obscures the reality that the only actors with sufficient resources to even possibly shutdown significant portions of the U.S. electrical grid are Russia or China and even then, neither possess the capabilities required to cause the level of physical destruction Panetta fears through cyber means alone.<sup>9</sup>

To understand the real danger of cyber threats, it is necessary to begin with understanding what constitutes an act of force in cyberspace. When assessing what constitutes advantages for the offense in terrestrial warfare, Robert Jervis, the Adlai E. Stevenson Professor of International Politics at Columbia University, states that offensive advantage is determined when it is easier to destroy the enemy and occupy their territory than it is to defend against attack.<sup>10</sup> The inverse is also true when determining defensive advantages. Although the objectives differ between the type of warfare Jervis refers to and warfare in cyberspace, the notion of force underpins offensive strategies. Determining an advantage between the offense and defense is measured by the relative ease with which force either destroys or can be defended against.

Nineteenth century Prussian general and military theorist, Carl von Clausewitz, observes force as central to warfare in his book *On War*, stating "war is thus an act of force to compel our enemy to do our will."<sup>11</sup> Clausewitz's conception of force is physical and violent in nature. Thomas Rid, Professor of Strategic Studies at Johns Hopkins University's School of Advanced International Studies, lists three criteria<sup>12</sup> which he asserts constitute the essence of warfare and claims that no existing offensive cyber capability meets all three criteria.<sup>13</sup> Going further, Rid states that, to date, only a small number of cyberattacks even meet one of the criteria. The question then is, if offensive strategies and capabilities in cyberspace are incapable of exerting force and do not meet the criteria for warfare in the cyber domain, then how are offensive actions and strategies in cyberspace classified? The answer is complicated. It is well-documented that most actions and strategies in cyberspace are incapable of generating any type of physical force by which adversaries can be compelled.<sup>14</sup> However, degradation strategies and operations arguably pos-

sess the most destructive potential of all cyber strategies and come the closest to producing what resembles an act of physical force in cyberspace.

This analysis will focus exclusively on degradation when discussing cyberwarfare and the offense/defense balance. While espionage and disruption strategies are intertwined with degradation, they are given less weight in their impact on the offense/defense balance as their offensive potential is not capable of producing the same type of physical effects as degradation. In other words, not all cyber strategies are created equally.

#### **Conflation of Strategies**

Combinations with synergistic effects are important. Nearly all recorded instances of degradation have had correlating espionage activities associated with them.<sup>15</sup> Espionage is required to infiltrate a network to degrade it by exploiting key vulnerabilities within the system. The reason these strategies are often conflated is because the general assumption, as Panetta demonstrates, is that the objectives of all cyber strategies are to degrade. While espionage and disruption often precede degradation, they have independent objectives that make them distinct from degradation. The danger in conflating espionage and disruption with degradation is that the conflation generates fear and misperceptions which can result in overreactions and aggression.

The primary objectives of espionage strategies are to infiltrate a network in order to monitor activity and steal or manipulate information. They are relatively easy as there are countless ways to covertly gain access to a network and steal information with little monetary expense. Disruption strategies seek to inhibit or prevent either individual or group access to a network, network function, or information. While disruption can be a more complex operation, depending on the objective, they are still relatively easy to conduct. For example, in the denial attacks against Estonia in 2007, lines of code and in-

---

*Degradation strategies and operations arguably possess the most destructive potential of all cyber strategies and come the closest to producing what resembles an act of physical force in cyberspace.*

---

structions on how to use them to conduct DDoS attacks were found in such innocuous places as forum pages. However, these strategies do not degrade networks or network systems to any lasting or physical degree.

Degrading a network is very costly in terms of time, money, and skills and expertise, explaining their infrequent use. Furthermore, degradation operations, contrary to what many believe, rarely result in either short- or long-term effects equal to the costs necessary to carry out an operation of this type.<sup>16</sup> For example, Stuxnet, one of the most well-known degradation attacks in recent time, cost the United States an estimated \$300 million dollars over a six-year period of research, development, and implementation.<sup>17</sup> Despite becoming the foremost example of a degradation operation's destructive potential, its success has been largely exaggerated. The Stuxnet virus only succeeded in shutting down 984 Iranian centrifuges, a mere 30% of Iran's total production capacity, and only setback Iran's enrichment timetable by one to two years. In addition, the International Atomic Energy Agency believes that Iran was able to supplement the loss of production

---

*Of the 272 recorded cyber operations between opposing states from 2000 to 2016, only 40 (~14%) degraded or sabotaged networks or systems in any significant manner.*

---

by overworking its remaining centrifuges, resulting in overall positive enrichment production estimates.<sup>18</sup> As this example demonstrates, despite degradation operations being the only type of cyber operation capable of manifesting physical effects, its destructive potential is often overstated. The danger in placing espionage and

disruption in the same category as degradation is that it generates the perception that conducting operations in cyberspace that have the potential destructive capability of degradation are cheap, easy, and that nearly anyone can do it.

Of the 272 recorded cyber operations between opposing states from 2000 to 2016, only 40 (~14%) degraded or sabotaged networks or systems in any significant manner. Each of these 272 operations, were likely to have thousands, if not millions, of individual activities, none of which resulted in a

single casualty.<sup>19</sup> In contrast to the reality of these numbers, seventy percent of Americans fear that the United States will suffer a devastating cyberattack that cripples critical infrastructure or destabilizes financial institutions.<sup>20</sup> The side-by-side comparison of these figures highlights how conflation of strategies has generated a disproportionate amount of fear around the possibility of danger, which in reality is unlikely. Much of this problem relates to how we talk about cyberspace and what occurs within the domain. Harvard University International Relations Professor Stephen Wal, in addressing threat inflation, states, "putting the phrase 'cyber' in front of almost any noun makes it sound trendy and a bit more frightening."<sup>21</sup> He's not wrong. The perception of offensive advantage has been unduly influenced by threat inflation and the conflation of espionage and disruption strategies with degradation. The following section will discuss the advantages defense has over offense, making it the dominant and preferable cyber strategy.

## THE DEFENSE IN CYBERSPACE

The offense-defense balance plays an integral part in the stability or instability of the security dilemma. Determining an offensive or defensive advantage is one of two variables Jervis observes as influencing the balance. The objective of this section will be to apply the two mechanisms Jervis uses to ascertain an offensive or defensive advantage to demonstrate how the defense has the advantage in cyberspace.

### Geography

Terrestrial borders and boundaries do not exist in the information domain, at least not in any manner that mirrors what we see when looking at a map or how Jervis conceptualizes geography and its importance as a contributing factor to the offense-defense balance. Most who have written on the offense-defense balance in cyberspace believe geography is a seemingly irrelevant measurement when determining offensive or defensive dominance. However, geography is an important factor in cyberspace and benefits the defense, a utility which many have been overlooked and dismissed.

While geography has value throughout all the levels of war, Jervis summarizes that anything which serves to increase the distance which an attacker must traverse, or makes the attacker vulnerable while traversing, subsequently in-

creases the advantage for the defense.<sup>22</sup> Increasing time and distance is easily done by developing firewalls, encrypting data, utilizing air-gap networks, etc. However, these are passive defensive measures which usually only serve to delay a persistent attacker.

---

*The benefit of geography within cyberspace is that it is synthetic. The defender is able to create the “ground” they fight on and can continually shape the “terrain” to their advantage.*

---

affected portion of the network could be contained, even disconnected, all while maintaining the integrity of the data and the network’s function, given proper coordination and planning.<sup>23</sup> The malleable geography of networks and information systems creates an inherent defensive advantage. Adopting an active and integrated defense within cyberspace, where networks and network components can continually be reconfigured and redesigned, significantly increases the cost of resources and time attackers would have to dedicate to find and exploit a breach.

### **Technology and Skills**

The matter of technology is another mechanism that Jervis applies to determine an advantage between the offense and defense. Jervis states that the security dilemma is most dangerous when alliances, strategy, or technology dictate that security can only be assured through aggression and offensive action.<sup>24</sup> The general consensus is that technology favors the offense. However, the matter of technology suffers from many of the same misperceptions listed above.

### **THE DIFFERENCE BETWEEN TECHNOLOGY, SKILLS, AND EXPERTISE**

Some analysts infer that the nature of technology, its speed and ease of use, denote an offensive advantage.<sup>25</sup> However, this is an incomplete assessment as it assumes these traits of technology are naturally occurring phenomena. The qualities listed and technology’s effectiveness are derived from the interaction between technology and human ingenuity. Cyber weapons, unlike conventional weapons, are inseparable from skills.<sup>26</sup> The development and production of conventional weapons require a distinctive set of skills and expertise than those necessary to deploy them within a battlespace. Conversely, the skills and expertise required for developing and producing cyberweapons are the same used to employ them. In regards to cyberweapons, Alan Paller, founder of the Escal Institute of Advanced Technologies (SANS) claims the inverse to be true; “Skills are the weapon.”<sup>27</sup> Paller is correct in noting that skills, more than the capabilities themselves, are what matter when discussing cyberweapons. Absent from skills, cyberweapons suffer from impermanence. In other words, most cyberweapons only work once. This makes skills and expertise, more than the technological capability, the unit of analysis when determining whether technology benefits the offense or defense.

A problem that emerges is that skills and expertise are neutral. They can influence the effectiveness of both the offense and the defense. A dependent variable when ascertaining an advantage between the offense and defense, in relation to skills, is cost. Do skills and expertise cost the offense or defense more? This question returns to the earlier distinction between the type of strategies and operations that can be employed in cyberspace. It is widely accepted that espionage and disruption strategies often employ cheaply conducted operations and as a result the balance of costs favors the offense. However, the effects that these operations produce, both in means of coercive force and more physical force, are severely limited, arguably negating their advantage to the offense. The strategy which does apply in accurately measuring the offense-defense balance is degradation.

## SKILLS AND EXPERTISE APPLIED TO THE OFFENSE/DEFENSE DEBATE

The consensus is that the offense is heavily favored regarding degradation operations. This view stems from the perception that in order to be successful, the defense must counter all attacks, whereas the attacker merely needs to find a single entry point to exploit in order to be successful.<sup>28</sup> While this perspective is technically correct in a broad sense, it suffers from the same conflation mentioned earlier. Espionage and disruption strategies dominate the offensive advantage perspective, creating pessimism surrounding the effectiveness of the defense. However, it must be reiterated that these strategies and operations are actually less impactful to the offense/defense balance debate due to their low-cost, low-payoff dividends. This misperception of offensive advantage attributes the cost efficiency of espionage and disruption operations to those of degradation as well. The reality is that the cost/benefit calculation of skills and expertise required in degradation operations actually favors the defense.

The cost/benefit and the requisite skills and expertise needed to carry out a degradation operation are nearly identical to those of the defense. Computer security expert Matthew Monte, observes this equilibrium in his book *Network*

---

*The reality is that the cost/benefit calculation of skills and expertise required in degradation operations actually favors the defense.*

---

*Attacks and Exploitation*, stating, “Breaking into a particular network may be cheap after the tools and infrastructure are in place,” but “building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and training. This is not cheap.”<sup>29</sup>

Simply put, degradation strategies and operations require the same, if not more, skills, expertise, and money than it does to defend against them. This logic stands to reason that if the costs of the offense and defense are similar, then why is the security dilemma in cyberspace worsening? Robert Jervis observes that if the costs of the offense and defense are comparative then arms races are less likely to occur, making it

possible for states to provide for their own security without overtly threatening the security of other actors, lessening the severity of the security dilemma.<sup>30</sup> The answer is that the absence of stabilization is due to a “cult of the offensive” which has developed amongst leading military leadership and policy makers around the world.

## THE CULT OF THE CYBER OFFENSIVE

In examining the outbreak of World War I, Jack Snyder, international relations professor at Columbia University, observes a similar instance of the security dilemma worsening when it ought to have stabilized. Prior to World War I, defensive strategies and operations were heavily favored, and yet war still occurred in 1914. The roots of the cyber “cult of the offensive” are threat inflation and the conflation of strategy. Conversely, Snyder’s conclusion is that the “cult of the offensive” precipitating World War I was due to poor civilian-military relations.<sup>31</sup> However, the similarities lie in that they both influence policy and affect state output. Preceding World War I, the General Staffs throughout Europe succumbed to an offensive bias preventing them from accurately assessing the offense/defense balance which resulted in the pursuit of recklessly offensive planning. As this section will demonstrate, although the antecedent conditions may not be identical, a new “cult of the offensive” is forming in cyberspace, manifesting in present-day policy directions put forth by military leadership.

Valeriano and Jensen assert that, until recently, activities within the cyber domain have primarily been related to ideological political conflict and coercive diplomacy.<sup>32</sup> However, developing policy in the United States is seemingly changing the nature of action within the domain from covert espionage to militarized operations.<sup>33</sup> As of 2018, United States Cyber Command (USCYBERCOM) released its vision of what its posture in cyberspace ought to be, which advocated for the United States to pursue a policy of “persistent action.”<sup>34</sup> USCYBERCOM’s vision has the stated objective of improving “the security and stability of cyberspace,”<sup>35</sup> which will be accomplished by “scaling to the magnitude of the threat, removing constraints on our speed and agility, and maneuvering to counter adversaries and enhance our national security.”<sup>36</sup> USCYBERCOM’s vision for the United States’ cyber posture is troubling due to its seemingly blasé inference of preemptive action. A closer examination of USCYBERCOM’S vision shows the influence that many of the misperceptions addressed throughout this analysis have on its strategies. In addition,

USCYBERCOM's vision reflects some of the beliefs<sup>37</sup> about the course of a war where the offense is dominant or perceived as dominant. USCYBERCOM's equivocation of couching offensive preemptive action as integral to its defensive plans demonstrates its offensive bias, which is generally an antecedent condition for the development of a "cult of the offensive."

## CONCLUSION

In addressing the misperceptions surrounding offensive advantage, this analysis has sought to dispel the notion that offensive strategies are dominant in cyberspace. This analysis has also demonstrated how the geography of cyberspace and the requisite skills and expertise needed to operate in the cyberspace domain favor the defense. It has also been suggested that much of U.S. policy in cyberspace has been influenced by misperceptions resulting in a "cult of the offensive" that generates a bias for offensive strategies. The coming months and years are crucial in confronting and addressing the misperceptions which generate a "cult of the offensive." If these misperceptions are allowed to persist in influencing policy, it increases the risk of moving warfare out of the cyber domain and into the physical world. Sometimes the best defense is simply a good defense. ■

## ABOUT THE AUTHOR

**Charles Smythe** is an MA candidate at Georgetown University's School of Foreign Service. He is a decorated United States Marine Corps combat veteran of Operation Enduring Freedom where he served as an infantry vehicle commander. His research and academic interests focus on the regional security of the Korean Peninsula and security issues affecting regional stability.

## ENDNOTES

1. Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *The Washington Post*, July 9, 2015, <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.

2. Andrew Radin "Hybrid Warfare in the Baltics: Threats and Potential Responses," RAND Corporation (Santa Monica, CA: Rand Publishers, 2017), 19.
3. Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (Winter 2016/17): 95, doi:10.1162/isec\_a\_00267.
4. Daniel T. Kuehl, "From Cyberspace to Cyberpower," in *Cyberpower and National Security*, by Franklin D. Kramer et al., (National Defense University Press, 2009), 28.
5. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack," *The New York Times*, October 11, 2012, <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>.
6. William O'Neil, "Cyberspace and Infrastructure," in *Cyberpower and National Security*, by Franklin D. Kramer et al., (National Defense University Press, 2009), 122-124.
7. Image obtained from National Aeronautics and Space Administration's (NASA) Earth Observatory, August 17, 2003, available online at: <https://earthobservatory.nasa.gov/images/3719/blackout-leaves-american-cities-in-the-dark>.
8. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth," *International Security* 38, no. 2 (Fall 2013): 43, doi:10.1162/isec\_a\_00136.
9. The United States Department of Energy, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," *Mission Support Center Analysis Report*, August 2016, 10; Robert K. Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations Center for Preventative Action, Contingency Planning Memorandum No. 31, April 2017, 2-3.
10. Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 187, doi:10.2307/2009958.
11. Carl von Clausewitz, Michael Howard, Peter Paret, and Bernard Brodie, *On War* (Princeton, NJ: Princeton University Press, 1984), 75.
12. Rid lists the criteria for force: the action must be violent, instrumental, and political.
13. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 10, doi:10.1080/01402390.2011.608939.
14. Gartzke, "The Myth of Cyberwar," 43.

15. Valeriano et al, *Cyber Strategy*, 19.
16. Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense," *Issue Brief no. 862*. Policy Analysis, Cato Institute. Washington, D.C.: Cato Institute, 2019. 5. <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>.
17. Slayton, "What is the Cyber Offense-Defense Balance?" 97-98.
18. Valeriano, Jensen, and Maness, *Cyber Strategy*, 198.; William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011. <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.
19. Valeriano and Jensen, "The Myth of the Cyber Offense," 4-5. <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>.
20. Aaron Smith, "Attitudes about Cybersecurity Policy," last modified January 26, 2017, <https://www.pewinternet.org/2017/01/26/3-attitudes-about-cybersecurity-policy/>.
21. Stephen Walt, "Is the Cyber Threat Overblown?" *Foreign Policy*, March 30, 2010, <https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/>.
22. Jervis, "Cooperation," 194.
23. David T. Fahrenkrug, "Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy," NATO CCD COE (2012): 199.
24. Jervis "Cooperation," 187.
25. Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (March 11, 2013): 43-44.
26. Slayton, "Cyber Offense-Defense Balance," 83.
27. Anna Mulrine quotes Alan Paller in her piece, "Cyber Security: The New Arms Race for a New Front Line," *Christian Science Monitor*, September 15, 2013, <https://www.csmonitor.com/USA/Military/2013/0915/Cyber-security-The-new-arms-race-for-a-new-front-line>.
28. Daniel Geer et al., "Cyberinsecurity: The Cost of Monopoly—How the Dominance of Microsoft's Products Poses a Risk to Security," *Computer & Communications Industry Association Report*, September 24, 2003. 14. Accessed April 24, 2019. <https://www.flyingpenguin.com/wp-content/uploads/2016/02/cyberinsecurity.pdf>.
29. Matthew Monte, *Network Attacks and Exploitation: A Framework* (Indianapolis: Wiley, 2015), 56.
30. Jervis, "Cooperation," 186-88.
31. Jack Snyder, "The Cult of the Offensive in 1914," in *The Use of Force: Military Power and International Politics*, ed. Robert J. Art and Kenneth N. Waltz (Lanham: Rowman & Littlefield Publishers, 2015), 121-137.
32. Valeriano and Jensen, "The Myth," 2.
33. Ibid.
34. United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," June 2018, 6, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.
35. Ibid.
36. Ibid., 2.
37. Jervis lists a series of beliefs of which two apply here, the first being that "war will be profitable for the winner" and the second that "wars are expected to be both frequent and short." (Jervis 189). In cyberspace, the first belief is found in the perception that espionage and disruption strategies are profitable as they are both cheap. The second belief stems from the fact that most conflict in cyberspace is measured in mere seconds or shorter spans of time.