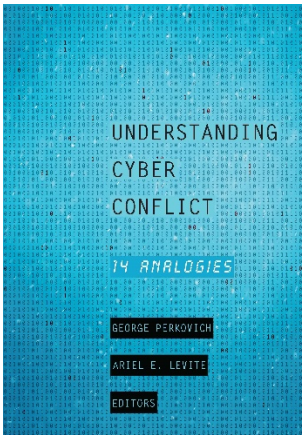

Why a Digital Pearl Harbor Makes Sense . . . and Is Possible

Emily O. Goldman and Michael Warner

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



9 Why a Digital Pearl Harbor Makes Sense . . . and Is Possible

EMILY O. GOLDMAN AND MICHAEL WARNER

Emerging technologies are changing how people create, share, protect, and store data; intellectual property; and wealth. New lines of operation have emerged for governments and businesses to pursue along with new weaknesses and vulnerabilities for adversaries to exploit. The unevenly governed spaces of the cyber domain have become the newest front line for military and economic confrontation because cyber attacks fit conveniently into adversarial strategies to counter superior conventional military capabilities. Cyber weapons enable even relatively unsophisticated actors to project power and operate deep within virtual and physical territory of the United States and other countries. They target the domain where the United States and other technologically advanced states are most vulnerable: our interconnected society, economy, and networked military, all of which rely on a digital architecture constructed for speed and convenience, not security.

For these reasons, a "cyber Pearl Harbor" has been one of the most prevalent and familiar analogies used by American officials, experts, and pundits to raise awareness of the dangers in this new realm of competition. The analogy conjures up grainy newsreel footage of burning battleships and the nation's entry into World War II. It evokes a devastating bolt from the blue that leaves an indelible imprint on the US psyche. In 2012 then secretary of defense Leon Panetta raised the specter of a cyber Pearl Harbor when he warned of attacks that could cripple the United States or its military. "Remember Pearl Harbor" is a call to mobilize support for increased cyber preparedness.

In spite of its critics, the Pearl Harbor analogy has endured because it usefully frames how dependence on cyberspace generates vulnerabilities that adversaries can exploit. Like all analogies, it must be applied with care. It gives less purchase when treated as a case of strategic surprise because the idea of a crippling bolt from the blue is an inaccurate characterization of historic events as well as an unlikely harbinger of future ones. But the analogy does provide insight into how an adversary could gain leverage over a conventionally superior military by avoiding areas of stronger states' military dominance and by launching cyber attacks against critical military infrastructure. It is also a warning that much of the current, tactical war-fighting capability of the United States and its allies

depends on their ability to navigate and secure cyberspace, where their forces and weapons systems are linked and controlled.

What Happened at Pearl Harbor

Pearl Harbor was not a strategic, bolt-from-the-blue surprise for the United States. Diplomatic relations between Japan and America had reached their nadir in late 1941. The United States was exercising coercive power to contest Japan's occupation of China and other Asian states, and Washington expected war. Pearl Harbor was a logical, if misguided, result of Imperial Japan's long-term strategy to expand its Pacific empire and blunt the United States' effort to stop it. Japanese expansionism focused on establishing an exclusive zone of influence, the Greater East Asian Co-Prosperity Sphere. By mid-1941, however, Japan's aggression in China and its larger aims in the southwest Pacific were hampered by President Franklin D. Roosevelt's embargoes and freezing of Japanese funds in US banks, which Tokyo saw as tantamount to economic warfare. Japanese naval planners in response sought to stymie Washington's ability to frustrate Tokyo's seizure of the resources that its military and economy desperately needed. Since America had moved aggressively to frustrate Japan's military aims in China and impede its economy, the Japanese reasoned they had to hit back.

Adm. Isoroku Yamamoto, Japan's top naval strategist, understood the risks of fighting America's industrial might, which he had seen firsthand as a young officer. For Japan to win and retain the upper hand, he believed, it had to strike a decisive blow at the outset of hostilities—one that would preclude the possibility of the United States going on the offensive while Japanese forces consolidated a defensive perimeter in the western Pacific. Japan would have to eliminate US forces in the Philippine Islands (astride Japan's key supply routes) and crush the US Pacific Fleet near Hawaii to prevent its advance toward Japanese home waters before Japan was ready for the great naval clash that would decide the struggle once and for all.

Yamamoto's strategic objective was not to conquer the United States or even to seize (much) US territory but to delay the inevitable American counteroffensive. He judged that destroying the Pacific Fleet's offensive power, even temporarily, would allow Japanese forces to take control of oil supplies in the Dutch East Indies and erect a barrier chain of island bases, thereby enabling Japan to delay the Pacific Fleet's westward progression and perhaps even force negotiations from a position of strength. A model for the attack was Germany's successful blitzkrieg strategy in France: hit hard and demoralize the adversary so its people would reject a long and costly war. It would take years for the United States to recover, Yamamoto hoped, and by then the Americans would face a fait accompli, with Japan's control extending from the Indian to the Pacific Oceans.

Although the Americans possessed ample strategic warning, they had little tactical warning because Japanese operational deception worked. American leaders knew full well that Pearl Harbor was vulnerable and explicitly considered the possibility of attacks by Japanese submarines, saboteurs, or carrier-

based aircraft.[1] Leaders in Washington and Hawaii did not, however, consider such attacks at Pearl Harbor to be either inevitable or imminent. US Army analysts had plentiful diplomatic signals intelligence from reading Japan's Foreign Ministry ciphers, but Japanese diplomats were not informed of the day and hour that war would begin until the last possible moment. US Navy analysts misread the intelligence clues they possessed (and failed to realize how many indicators they lacked) partly because the Japanese fleet practiced simple but effective deception and denial methods. Better management of intelligence analysts in Washington and Hawaii might well have revealed additional clues to Tokyo's intentions and spotted the Japanese deception efforts, thus providing another vital indicator of impending hostilities.

Pearl Harbor with its strong defenses proved vulnerable because the Americans lacked situational awareness and tactical control. Japanese aerial and submarine scouting of the harbor at dawn on December 7 should have prompted the base to go to battle stations, but as the US Army and Navy failed to coordinate their watches, clear indicators went unheeded. Also, had the radar system sent to guard Pearl Harbor been fully operational, the Japanese attack could have been blunted. Radar operators in training informed their chain of command of incoming planes that morning, but they were told the radar returns represented a US Army Air Forces flight from California.

The Japanese decision to attack Pearl Harbor looks logical only when one ignores its absurd premise: the island nation of Japan, already enmeshed in a war against the world's most populous country (China) and having recently fought another neighbor (the Soviet Union), could better its lot by attacking the world's foremost naval powers (the United States and Britain). Such a suspension of common sense was possible only in Tokyo's militarized political climate, in which the army dominated the prime minister, who could not form a government without the army's support.[2]

What Did Not Happen at Pearl Harbor

Japan hoped to buy time and present the United States with a fait accompli, but the Pearl Harbor operation was operationally and tactically flawed. The Imperial Japanese Navy's striking force easily reduced the Pacific Fleet's aging dreadnoughts on Battleship Row to smoking hulks, but it missed the fleet's more important aircraft carriers, heavy cruisers, and submarines. Japanese pilots had been ordered to hit these ships, but most of them, including all the carriers, were at sea to keep them away from Pearl Harbor. This represented a huge missed opportunity for Japan, as US Navy aircraft carriers and submarines would play a key role in strangling Japan's supply lines from 1942 onward and largely determine the outcome of the Pacific war.

The attack also did little damage to the Pacific Fleet's vital supplies and servicing components: fuel depots, dry docks, repair facilities, and undersea cable landings. This factor looms large in our analysis when considering the decision-making that had already occurred in Washington. Although Japanese planners

saw the fleet as their main objective, the US Navy's leadership believed the facilities at Pearl Harbor were more important. Pearl Harbor was not the Pacific Fleet's main base. In May 1940 the US Navy (under firm orders from the White House) had temporarily shifted the main base of its Pacific Ocean fleet from San Diego to Pearl Harbor.[3] Admiral Yamamoto described this move as "tantamount" to a declaration of war. American admirals, in contrast, worried that the Japanese would target the harbor's "critical infrastructure" while the fleet was at sea.[4] Pearl Harbor's oil stocks, in particular, were obvious from the air and highly vulnerable. Hitting them along with the ship repair facilities might have sent the fleet back to San Diego, to which the navy already wanted to return.

Had that happened, the course of the Pacific war could have been much different. The importance of Pearl Harbor's facilities is difficult to overestimate. Oil tanks can be rebuilt and refilled, and dockyards can be repaired. But when? Not for weeks at a minimum and perhaps for months—that is, if Washington decided to rebuild and reinforce its already ruined and exposed Hawaiian base. In the event, surviving US warships had plenty of fuel to operate in the central Pacific, and indeed they were operating there and harassing the Japanese within days of the Pearl Harbor attack. Salvage operations on the sunk and damaged ships at Pearl commenced immediately. And the harbor was open for business when it mattered most, in May 1942. The aircraft carrier USS *Yorktown* had received serious damage in the Battle of the Coral Sea (May 8) but was hastily repaired at Pearl Harbor. Experts estimated a two-week spell in dry dock for *Yorktown*, but technicians did enough work in forty-eight hours for it to sail again. If those vital repair facilities had been destroyed and those workers sent back to San Diego, *Yorktown* would have been unavailable for the pivotal Battle of Midway on June 4, leaving the Imperial Japanese Navy with a much freer hand.

Japan's surprise attack might have disabled the US Pacific Fleet for a year or more, giving Japanese forces time to dig in for a lengthy conflict. But Japan's intended knockout blow didn't succeed, and it ensured the United States would fight to the end of Japanese militarism.

The Logic of a Digital Pearl Harbor

Theories of surprise attack can account for the pattern of a weaker state lashing out at a stronger opponent to gain time to consolidate its ill-gotten gains. It might involve a direct attack on the stronger party or instead a seizure of something of interest to the stronger party but not worth enough to merit a protracted conflict to regain it. The latter, less provocative fait accompli is still a half step toward war. It promises a greater chance of political victory than quiet diplomacy, but (being violent itself) it also raises the risks of escalatory warfare.

The Pearl Harbor analogy is a warning to study the calculations of adversaries. Some, like Japan in the 1930s, might consider a surprise attack a viable preemptive option to temporarily blunt superior military capabilities. Do other people actually think this way? They have and they do. Saddam Hussein of Iraq certainly

did in 1990. He mounted a surprise mobilization of his best divisions and invaded neighboring Kuwait as soon as his forces were ready. Kuwait fell to Iraqi troops in hours, giving Hussein an oil-rich "nineteenth province" with a fine harbor on the Persian Gulf and changing at a stroke Iraq's strategic position with respect to Iran, its enemy in a grim eight-year war that had recently ended. A lesson for our time is that adversaries who feel their backs against the proverbial wall might lash out in new and unexpected ways.

Conditions exist today that resemble the East Asian crisis in the 1930s and could entice an adversary to strike a similar blunting attack against the United States or one of its allies in the hope of a quick victory that presents it with an undesirable strategic fait accompli. A power with a high tolerance for risk and, perhaps, a growing sense of desperation—especially one that perceives the United States or other adversaries to be seriously threatening its political and strategic fortunes—could use cyber means to shape the preconflict environment and delay or deter America's response. In such an aggressor's calculus, the United States (or other potential adversaries) might be induced to stay out of a regional conflict, in effect letting an aggressor keep his gains. Once an aggressor gained what it wanted, it might even have the ironic temerity to call on the international community to intervene and stop its opponent's pressure and retaliation. If an adversary's objective is to convince Washington or another state to leave it alone, or to allow it to pursue its aims against its neighbors, then Admiral Yamamoto's intellectual heirs in such a situation could be tempted to mount a quick strike.

But unlike Yamamoto's pilots, a contemporary adversary might either strike mobilization and logistical networks, impeding the adversary's ability to operate militarily, or manipulate information to blind and confuse it, much like China's strategy in Peter Singer's novel *Ghost Fleet*. From the adversary's perspective, a cyber attack has the virtue of damaging its opponents' ability to respond in the physical domain while not provoking public cries for retribution the way a terrorist attack on a city would.

In the 1991 Gulf War, Iraqi leaders did not fully appreciate the significance of highly advanced surveillance planes or networked computer communications. A future opponent will not likely make the same mistake.[5] Dependence on cyberspace for shared battlespace awareness may provide a decisive advantage for higher-tech militaries today, but the data infrastructure and data themselves make exceedingly valuable targets. The incentive to contaminate or disrupt the information flows on which the US military depends, for example, is enormous. A cyber-savvy adversary with outsized goals could find this type of effect attractive. Adversary countries need not even be risk acceptant to adopt this strategy. They may in fact be risk averse, but like Japan in 1941, their decision-making processes may give disproportionate weight to the most bellicose and paranoid leaders and factions. It does not take the resources of a state to mount a damaging cyber attack, and such an attack can be formulated in secrecy even from other parts of the attacking state. Or, as recent events suggest, national governments may find it challenging to exert control and oversight over all

potential hacker communities within their military cyberspace apparatus, not to mention industry or patriotic hacktivists outside state control.

The Pearl Harbor analogy reinforces the maxim that while "amateurs focus on tactics, professionals study logistics." Targeting critical military cyber infrastructure today might succeed where Japan failed in 1941. This is so not because of any quality inherent in the attacker or in the political environment but because of the dependence of advanced militaries on cyberspace.

The Current Environment

These concerns are not far fetched. The adversaries of the United States, and those of other states, have invested in asymmetric means—such as anti-access and area-denial capabilities—to counter traditional US strengths and to prevent it from projecting power abroad. They are preparing the future cyber battlefield now by stealing intellectual property, conducting industrial espionage, and exploiting government networks and those of defense, financial, and communication industries. Through intelligence, surveillance, and reconnaissance against US and allied networks, they have gained penetration and established persistent access. These activities can be verified by perusing the continuous and alarming public statements made by a host of independent computer and software security experts in recent years. Of course, adversaries might believe that the United States and its allies also engage in cyber operations to gather intelligence and perhaps to conduct attacks.

US adversaries have also shown an increasing capability and intent to target its industrial control systems recently. Since 2011 known or suspected hackers in several countries have run supervisory control and data acquisition (SCADA) exploitation attempts against US critical infrastructure. In September 2015 in testimony before the House Permanent Select Committee on Intelligence, Director of National Intelligence James Clapper revealed that unknown Russian cyber actors had compromised the supply chains of at least three industrial control system vendors. He warned, "Politically motivated cyber-attacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems."[6] Cyberspace threats also headlined Clapper's February 2016 testimony to the Senate Select Committee on Intelligence on worldwide threats.

In subsequent hearings before the House Armed Services Subcommittee on Emerging Threats and Capabilities in March 2016, Adm. Mike Rogers, commander of US Cyber Command and director of the National Security Agency (NSA), testified that "industrial control systems and SCADA probably is the next big area for us because we've got to transition from a focus purely on the network structure."[7] He noted that the Department of Defense (DOD) has already begun looking at data concentrations and focusing more on industrial control systems and SCADA. Rob Joyce, chief of the NSA's Tailored Access Operations unit, complains that SCADA security keeps him up at night. Joyce understands how to exploit such systems;[8] he also appreciates how vulnerable the United States is,

in turn, and that the "Internet of things" will multiply those vulnerabilities exponentially.[9]

Supply chain vulnerability, another dimension of the problem, was raised during Admiral Rogers's hearings before the Senate Armed Services Committee in April 2016. Specific processes exist in the US government to address these issues for some components of DOD infrastructure, particularly nuclear systems, but not for other major systems or components. The DOD's focus on network security is now expanding to focus on the risks to individual combat platforms, weapons systems, and individual data concentrations. In the National Defense Authorization Act of 2016, Congress directed the secretary of defense to complete an evaluation of the cyber vulnerabilities of every major weapons system by December 2019.

Perhaps the starkest exemplar of military vulnerability involves cyber attacks against US Transportation Command (USTRANSCOM), the command responsible for moving US troops and military equipment around the world. In September 2014 the Senate Armed Services Committee made public the results of its investigation into hacking activities targeting US military contractors. It reported that hackers sponsored by the Chinese government accessed contractors' computer systems "at least twenty times in a single year."[10] Targeted cyber attacks against USTRANSCOM persisted longer than a year with fifty cyber events documented between June 2012 and May 2013. According to the committee's report, USTRANSCOM is targeted more than any other combatant command because it is particularly vulnerable. It relies on commercial partners to deliver 70 percent of its military equipment, supplies, and personnel around the world and to keep the US military running. Ninety percent of USTRANSCOM's communications, distribution, and deployment transactions are conducted on unclassified networks because the companies it relies on cannot access the Pentagon's secured network. This truly is the Achilles' heel for US power projection.

Lessons for Today

The purpose of Japan's Pearl Harbor attack was to delay, not annihilate, US power. How long might a state take to recover from attacks on critical infrastructure systems on which its society, economy, and military depend today? Would that delay buy an adversary time to operate without fear of retaliation? Is there a contemporary analogue to the decisive blow against Pearl Harbor, or are we more secure by having a distributed infrastructure? In cyberspace a "Pearl Harbor" might consist of numerous national systems and institutions critical to the economy. They include but are not limited to undersea cables, power grids, water supplies, classified networks, electronic voting systems, banking systems and electronic funds transfer (those that enable Internet commerce, for instance), and heavy reliance on a single operating system. Recent examples of inadvertent interruptions in these systems have resulted in large consequences. The effects of intentional disruptions can only be imagined.

The first lesson is to take seriously telltale warning signs to avoid being caught tactically off guard as the US Navy and Army were in 1941. US government officials have been very public about seeing multiple cyber actors penetrating US systems. These events are not isolated but rather parts of sustained campaigns, indicating a long-term commitment to understanding systems and to ensuring the intruders possess the capability to potentially impair the country's ability to operate. Their purpose for now appears to be conducting reconnaissance and surveying systems, their vulnerabilities, and the control points that someone would want to access. But intent could change quickly. Cyber actors want to ensure they have technical options should they make the political decision to interfere with their competitors or send a message to deter them. Threat is composed of capability and intent, and multiple actors are demonstrating their ability to gain access to critical infrastructure. A premium must also be placed on watching for clues to their intent.

The December 2015 events in Ukraine, where multiple electric companies were hacked—the first power outage known to be caused by a cyber attack—should serve as a wake-up call. Hackers used malware to gain access to the Ukrainian utilities' business networks and, from there, maneuvered to their production networks and on to operator stations. The hackers then remotely disconnected the breakers of thirty substations. According to Robert M. Lee of Dragos Security, "Every bit of this is doable in the U.S. grid." Although the US grid is more hardened than Ukraine's, the former's recovery would be more difficult because if the SCADA systems are lost, the fully automated US systems cannot switch to manual control as the Ukrainians' system did.[11]

Vulnerable states and enterprises must strengthen their defensive capabilities both for government networks and for the critical infrastructure nodes that are outside government control and in the hands of the private sector. Corporate leaders in the United States and elsewhere are working hard to correct those deficiencies. The US power sector is looking at microgrids and other techniques to try and break the grid into smaller and thus potentially more defensible segments. But overcoming decades of investment in capital infrastructure—in which defensibility was never a core design characteristic—is a huge challenge.

Going forward will require a culture change as well. Expecting zero system penetrations is unrealistic because it is less a question of if than when attackers will get through the perimeter. The measure of success thus rests on how one responds when a penetration occurs. In the summer of 2015, after an intrusion into the US Joint Staff's unclassified systems, the DOD quickly disconnected the network and ensured no data was extracted or a long-term presence was established. While this action is a good model for defensive response, disconnection is not always feasible. It is necessary to learn how to retain the capability and the mission of the network while maneuvering and fighting to drive the opponent out. This work requires a different skill set and mind-set.

Culture change must extend to the entire workforce. In the United States, the DOD is working to create a culture where cyber hygiene and cybersecurity are as foundational to a DOD employee as the accountability expected of every affiliate

who is issued a weapon. That weapon, of course, must be appropriately treated, appropriately used, and always secured. Traditionally, cyber and cybersecurity have been viewed as very specialized and highly technical work that only a small segment of the workforce (the information technology [IT] personnel) did. Cyber was the purview of the chief information officer or chief technologist. Senior military and defense officials, like their private sector counterparts in the C-Suite—that is, the corporations' senior executives and board members—looked to the IT experts to take care of problems they were uniquely trained to do. Increasingly they have recognized that everyone in this domain is a point of vulnerability as cyber behavior shapes the ability to defend networks. On September 28, 2015, the secretary of defense and chairman of the Joint Chiefs of Staff authorized the Department of Defense Cyber Culture and Compliance Initiative. It intends to transform DOD cybersecurity culture by improving the individual human performance and accountability of every member of the DOD cyber enterprise: leaders, service providers, cyber warriors, and users.

Another takeaway is the importance of public-private partnerships. The private sector can generate insights into what is happening online that governments cannot. The reverse is also true. Thus, the capabilities of intelligence infrastructure must be augmented by insights from the private sector to fill respective information gaps and to better understand what is happening, who the actors are, and what tactics, techniques, and procedures they are using. Defeating an enemy starts from the premise that one is aware of and understands it. Developing this knowledge reflects the power of partnership. With a legal framework that engenders confidence and enhances the free flow of information in both directions, government can push actionable information to the private sector. The US Congress in 2015 passed the Cybersecurity Information Sharing Act, which enables industry to increase its sharing of threat information with the federal government (and vice versa) without fear of losing competitive advantage or risking additional legal liability. It has established a key element in the government's efforts to improve the cybersecurity of critical infrastructure.

Connecting the dots is critical, but planning responses to attacks is also necessary. What would have been the US response if the right dots had been connected in December 1941? International law permits nations to conduct preemptive strikes in self-defense. Seeing six Japanese aircraft carriers north of Hawaii and headed for Oahu at top speed on December 6, for example, US Army bombers might well have been ordered, with clear legal justification, to launch attacks against that fleet. Currently few clear guidelines, however, exist for preemptive strikes to blunt or prevent cyber attacks against national infrastructure.

American political leaders and scholars have typically viewed cyber operations as wartime measures undertaken only during a conflict and therefore as inherently escalatory. Yet cyber conflict has been increasing for years, and cyber interference with US and other states' interests occurs daily. Cyber operations are an extension of policy and strategy, increasingly a normal part of state behavior.

Gen. Darren W. McDew, commander of USTRANSCOM, raised questions before the House Armed Services Committee's Readiness Subcommittee in March 2016 that all nations dependent on IT and computer technology networks must address: "When can I defend my network, how far out can I defend? What constitutes an attack on a commercial provider? What do they have to report as an attack, because the definition may be not as clear with every single person?"[12] After blunting an adversary attack, moreover, states must have the capability to maneuver to conduct operations that neutralize and disrupt the adversary's ability to conduct follow-on cyber operations.

Conclusion

The Internet is inherently redundant and resilient. But technologically advanced states would be foolish to rule out a lucky hit that cripples them, just as the Pearl Harbor attack would have crippled the Pacific Fleet if the Japanese pilots had hit the fleet's oil supplies and dockyards instead of its old battleships. The United States had little up-to-date experience in maneuvering large sea, air, and ground forces at the outset of World War II. The critical infrastructure of many states today likewise remains unprepared for cyber attacks.

Critics of this analogy could argue that adversaries probably would not, or could not, launch a cyber Pearl Harbor–style attack against the United States. But one could have said the same about the prospect of an air raid on Pearl Harbor in 1941. The Japanese attack was strategically foolhardy, but nonetheless it happened. The ease of applying mass and achieving surprise in the new cyber domain means that numerous competitors are in this space. Threats to national and economic security in cyberspace are increasing in complexity and destructiveness as well. Thus, given the lack of traditional warning and the absence of immediately visible consequences for malicious cyber behavior, adversaries could believe they face few costs and yet stand to reap huge benefits.

Notes

This chapter is an adaptation and extensive revision of the chapter by the coauthors (along with John Surdu) that appeared in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014). Drs. Goldman and Warner serve in US Cyber Command, but the opinions expressed herein are their own and in no way represent official positions of the Department of Defense or any other US government entity.

1. Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor*, with Donald M. Goldstein and Katherine V. Dillon (New York: McGraw-Hill, 1981).
2. Ibid., 213.
3. Ibid., 38, 93, 97.
4. Ibid., 42, 66, 97.
5. Richard J. Harknett and the JCISS Study Group, "The Risks of a Networked Military," *Orbis*, Winter 2000, 127–43, https://www.comw.org/rma/fulltext/00harknett.pdf.

6. James Clapper, director of National Intelligence, Statement for the Record, "Worldwide Cyber Threats before the House Permanent Select Committee on Intelligence," September 10, 2015, https://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015.

7. Testimony of Michael Rogers, commander, US Cyber Command, at the hearing on US Cyber Command's FY 2017 budget request, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, 114th Congress, March 16, 2016.

8. While the head of TAO at NSA, Joyce was tapped to become the White House cybersecurity coordinator for President Donald Trump.

9. Tom Simonite, "NSA Hacking Chief: Internet of Things Security Keeps Me Up at Night," *MIT Technology Review*, January 27, 2016.

10. Senate Armed Services Committee, *Inquiry in Cyber Intrusions Affecting US Transportation Command Contractors*, 113th Cong., 2d sess. (Washington, DC: Government Printing Office, 2014).

11. Kim Zetter, "Everything We Know about Ukraine's Power Plant Hack," *Wired*, January 2016.

12. Darren McDew, commander, US Transportation Command, testimony on the FY17 US Transportation Command FY 17 budget request, House Committee on Armed Services, Subcommittee on Readiness, 114th Congress, March 15, 2016.