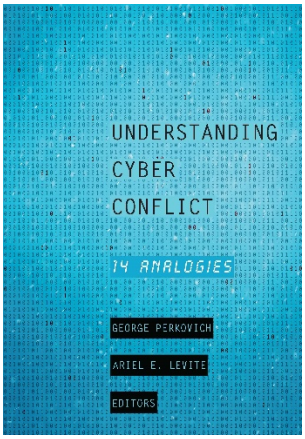

From Pearl Harbor to the “Harbor Lights”

John Arquilla

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



11 From Pearl Harbor to the "Harbor Lights"

JOHN ARQUILLA

The specter of a looming digital "Pearl Harbor"–style attack has been and remains a central element in the American discourse on cybersecurity. Clearly, the iconic example of a disabling surprise attack on an unsuspecting fleet, more than seventy-five years after the event, still speaks powerfully to the fresh threat posed by a cyberspace-based attack on a technology-dependent society and its equally vulnerable military. Given the deep emotional effect evoked by memories of that "day of infamy," one would expect significant steps would be taken to mitigate such a risk.

Yet, over the past twenty years, a time during which the notion of a digital Pearl Harbor has proved a useful analogy, little visible effective preventive public policy has been made. Writing in 2013, cyber experts P. W. Singer and Allan Friedman noted that in the United States "some fifty cybersecurity bills [are] under consideration," representing just a small portion of the total number that had been proposed in a decade. They also observed, "Despite all these bills, no substantive cybersecurity legislation was passed."[1] Since then only one bill, the Cybersecurity Information Sharing Act of 2015, which encourages voluntary information sharing with the government about cyber incidents in the private sector, has been enacted into law.

Among the difficulties experienced in efforts to pass good cybersecurity legislation, privacy concerns, ranging across the Right–Left political spectrum, have sparked and sustained very strong, steady resistance.[2] In the wake of the massive breach of the Office of Personnel Management's "secure" files that began (apparently) in March 2014, confidence in the government's ability to solve the riddles of cybersecurity remains quite low. Over twenty million members of the military and the civil service have been affected. The US government's dispute with Apple, Inc., in which the Federal Bureau of Investigation sought Apple's assistance in decrypting the information on a smartphone seized in the investigation of the 2015 domestic terrorism incident in San Bernardino, further strained public-private amity in cybersecurity-related matters.

Even worse, in addition to its inability to protect vital information under its control, the US government is also seen as obstructionist. Policymakers worry that more secure products will make it harder for law enforcement and intelligence

agencies to employ "cyber taps" on criminal and terrorist organizations. This concern has led, beyond the issues raised by the San Bernardino matter, to the US government's desire to be able to access any and all private communications via cyberspace as and when deemed necessary. The Cybersecurity Information Sharing Act, in the view of some leading cyber analysts, is thus seen as entailing two deleterious effects: it would make not only "any future data breach . . . far more catastrophic" but also "everything you do and say online less safe and more susceptible to government eavesdropping."[3]

As for market-driven solutions, consumers have a record of not demanding very secure products. For decades producers did not seriously try to make their systems more "hack proof." But given the string of costly attacks across a wide range of enterprises over the past few years—Anthem Blue Cross, Sony Pictures Entertainment, Target, and Yahoo are just a few of the most high-profile victims—US and other manufacturers have become determined to craft computers, cell phones, and other systems that are ever more secure.[4] They have done so while going against the wishes of some in government—with the notable exception of former president Barack Obama—to be able to outflank strong encryption by means of "backdoor" keys, which allow intrusion into anyone's system.[5]

Thus, it seems that Washington, which has trumpeted the Pearl Harbor metaphor, has failed to act in a helpful manner as defenses are developed against such a virtual bolt from the blue. As to Silicon Valley, and throughout the commercial information technology (IT) sector, the decades of neglect to produce more secure products have contributed to leaving cyberspace and its countless users quite vulnerable to hackers. If the government were somehow to cease its efforts to impede the launch of far more secure products, the situation would surely improve, at least at the margins. But much more is needed, as the United States and many other countries remain far from having a true ability to prevent, preempt, or counter the effects of a digital Pearl Harbor.[6]

An Alternative Analogy: "The Harbor Lights"

Despite its deep resonance in military and intelligence communities, the foregoing analysis of the Pearl Harbor analogy lacks traction in the political and economic arenas. Perhaps this is because military analysts do not speak directly to the commercial consequences of a major cyber attack. The Pearl Harbor imagery easily conjures visions of a stunned military, but it does little to illustrate how a surprise attack could affect the economy or could sway votes in an election. Thus, it is worthwhile to consider adding a cyber analogy that can engage decision makers in government and business—and the mass public—in political and economic ways. One does not have to look far beyond Pearl Harbor to find an analogy that serves this purpose very well.

Four days after the December 7, 1941, attack on Pearl Harbor, Axis partners Germany and Italy declared war on the United States. Strategic analysts criticized the move, given that Congress had authorized war against Japan only. This precipitate move by Adolf Hitler and Benito Mussolini brought America actively

into the European conflict much earlier than it might otherwise have done—if at all. On November 21, only a few weeks before the Japanese attack, nearly two-thirds of respondents to a Gallup poll opposed the very idea of war against Germany and Italy. But as the diplomatic historian Thomas Bailey once noted, with equal eloquence and irony, thanks to Hitler's taking the matter into his own hands and to Mussolini's following his lead, "American opinion was spared the confusion of a debate over fighting the European Axis."[7] Thus, the Allied coalition was forged by the aggressor.

The fight against Germany and Italy was for the most part conducted in theaters thousands of miles from the United States. Any sense of immediate danger was, to say the very least, lacking. To be sure, many Americans of Japanese descent—and some of German and Italian ancestry as well—were soon put in camps due to war paranoia. There was also belt-tightening and rationing, but for the most part, Americans' life patterns retained much of their normalcy. On the East Coast, this fact was manifested in how cities and harbors continued to light up at night, and most coastal maritime traffic sailed unescorted. All this occurred despite the German U-boats—the one enemy weapons system that could reach the United States—having done grievous harm to Britain's shipping since September 1939.[8]

Five weeks after Pearl Harbor, in mid-January 1942, Karl Doenitz, the commander of U-boat forces, had a handful of his submarines operating off the East Coast of the United States. Dispatched under the grand name *Paukenschlag* (Drumbeat), these U-boats—at most a dozen at any given moment—more than lived up to the operation's title, inflicting steady, heavy losses on coastal shipping. One member of the U-boat service recalled the time as the "American Shooting Season," during which the Germans could quietly lurk off "open anchorages and undefended harbors . . . a veritable Eldorado."[9]

For three long months, coastal cities refused even to dim their lights at night. The illumination helped U-boat skippers immensely. The eminent naval historian Samuel Eliot Morison labeled this inaction America's "most reprehensible failure."

In Morison's analysis of these events, "the massacre enjoyed by the U-boats along our Atlantic coast in 1942 was as much a national disaster as if saboteurs had destroyed half a dozen of our biggest war plants." Indeed, during this U-boat "happy time," Germany sank 2.5 million tons of shipping, or about half the total losses inflicted by German submarines in the first two years of the war. Morison's unsettling bottom-line assessment is quite biting: "Ships were sunk and seamen drowned in order that the citizenry might enjoy pleasure as usual."[10] And all this came at a minimal cost to the U-boat arm. Though the US Navy claimed twenty-eight kills of enemy submarines from January to March, in actuality these were all false claims made by overenthuisastic American skippers. *No* U-boats were sunk during this period, and only half a dozen were lost by July 1942.

How could it be that the harbor lights stayed on so long during this absolute crisis? The only reasonable reply to this question is to explain that very powerful political and economic interests trumped sound strategy. All along the Eastern

Seaboard, big-city mayors and local business leaders objected that blackouts would cause catastrophic economic losses. Florida, which was experiencing the height of its flow of winter visitors from the North, strongly resisted pressures to darken its coastal cities' lights, even though U-boat sinkings along this section of the coast were devastating. Naval historian Henry Adams has noted, for example, that "Miami especially was urged to employ a dimout to reduce the deadly glow, but its Chamber of Commerce refused, saying it would ruin the tourist season."[11]

By the spring of 1942, losses had grown heavy enough that President Franklin D. Roosevelt (FDR) ordered blackouts all along the seaboard and for miles inland. This action was accompanied by the US Navy's grudging willingness to start moving coastal ship traffic in convoys. From the start of the war, Adm. Adolphus Andrews, who oversaw the antisubmarine campaign on the East Coast, took the position that, thanks to air patrols, ships could "seek the protection daylight affords" and "break their passage by lying over in sheltered harbors at night."[12]

This approach failed miserably. Only when escorts could strike back at the U-boats did the latter begin to suffer growing losses. As Michael Gannon, another historian of submarine warfare, has summed the matter up: "What really broke the back of the U-boat campaign in U.S. waters was the coastal convoy."[13]

Clearly, blackouts, dimouts, and convoys helped solve the problem, but they did not really break the back of the U-boats. Between January and August 1942, only seven German submarines were sunk in US waters. But this number is the wrong metric by which to judge the outcome of the antisubmarine campaign; instead, the number of U-boat *attacks* should be considered. By March–April they had risen to ninety-eight; by July–August they had fallen to twenty-six, or a drop of 73 percent.[14] Attacks fell in part because Admiral Doenitz simply decided to stop investing in the long-transit, short-dwell time of U-boats in American waters.

As US defenses improved, it made little sense for a U-boat to spend two-thirds of its patrol time in transit to and from the target zone. Thus, protected convoy targets were to be found and attacked far closer to home, requiring much less transit time. One of Admiral Doenitz's aides, Wolfgang Frank, summed up the principal reason for ending *Paukenschlag*: "This was not because the A/S [antisubmarine] defenses off the American coast had grown too strong, but because with the end of independent sailings and the introduction of convoys it was no longer worthwhile to send boats so far out."[15]

Assessing the Harbor Lights Analogy

Perhaps the first and most important point to derive from the American experience on the Eastern Seaboard in the months after entry into the war is that just as far too few civil defense measures were taken then, the same is true today in the virtual domain. Throughout all too much of cyberspace, the "harbor lights" remain on and illuminate the commercial sector's intellectual property, sensitive data held by government and the military, and the personal information of

individuals. All have been exposed, providing rich targets for attack by the latter-day counterparts of the World War II–era U-boat raiders, hackers. Indeed, former US cyber czar Richard Clarke, along with his colleague Robert Knake, have rated US cyber defenses as worst among leading nations. They also note that the "senior government official charged with coordinating cybersecurity was . . . in an office buried several layers down in what was turning into the most dysfunctional department in government, DHS [Department of Homeland Security]."[16]

When he entered office in 2009, President Obama did try to elevate the cyber czar's role, affirming that the "cyberthreat is one of the most serious economic and national security challenges we face as a nation."[17] But his choice for leadership, Howard Schmidt, turned out to be skeptical about the gravity of security affairs in the virtual domain. As he once opined: "Anytime someone commits a denial-of-service attack or someone intrudes into a system to steal intellectual property, it's not a cyber war. This kind of hype is beneficial to no one."[18]

Schmidt left government service in 2012 to join a cybersecurity firm, partnering with, in a moment of true irony, the former head of DHS governor Tom Ridge. Michael Daniel, Schmidt's successor as cyber czar and a former congressional staffer with little actual expertise in computing or IT, suffered sharp criticism for being missing in action as waves of costly, debilitating hacks swept over US commercial and governmental sites.[19]

While part of the reason why the harbor lights are still on throughout the many sectors of cyberspace has to do with organizational dysfunction in Washington, some blame can also be placed on IT manufacturers, whom the consumer markets did not press to craft more secure products until recently. Then when manufacturers made efforts to produce far more secure products, the government—law enforcement in particular—expressed its concern that secure smartphones and other communications devices might impede their investigations.

A third culprit hearkens to the harbor lights metaphor as well—that is, the strategic paradigm employed by those charged with the defense of cyberspace. Central elements of this security paradigm are antiviral software and firewalls; together, it is much hoped, they are able to keep the cyber barbarians from breaking in. But they do not, at least not often enough. Good hackers break right through firewalls, which stop only the viruses, worms, and malware that they can already recognize.

Faith in firewalls has led to failure to adopt the most effective tool of cybersecurity, widespread use of very strong encryption. The reluctance to make end-to-end encryption the norm in cyber communications is analogous to the stubborn unwillingness to use convoys to protect vessel traffic on the Eastern Seaboard during the early months of 1942. And the unwillingness to keep stored data strongly encrypted is very much akin to keeping port cities illuminated.

Interestingly, the harbor lights analogy cuts both ways, providing lessons for the attacker as well. As noted previously, Doenitz had to calculate the factors of time, space, and force in determining the optimal use of his U-boats, and his

analysis ultimately led him to shift his forces away from the US Eastern Seaboard when its defenses improved. It may well be that cyber attackers will have similar incentives to redirect their own operations if security improves thanks, say, to the ubiquitous employment of strong encryption or the dispersal of targets in the Cloud, that place of places outside one's own system.[20]

Attackers' first inclinations under such circumstances—that is, when data is strongly encrypted or harder to find and exploit by virtue of being secreted in the Cloud—would likely be to search for "softer" targets elsewhere. Doenitz showed a penchant for doing exactly this; as shipping defenses firmed up along the East Coast, he shifted his subs to the Gulf of Mexico, the Caribbean, even to Panama. When defenses in these areas improved, becoming virtually equal to convoy protection in the North Atlantic, he pulled back and concentrated the U-boats on targets that took less time to reach from their home bases. Eventually, with the major advances in Allied radio direction-finding equipment, the substantial increases in escort vessels, and the breaking of the Nazi Enigma codes by the boffins working at Bletchley Park, the U-boats were defeated.[21]

But this happy ending is not necessarily going to be repeated in the case of cyberspace for two fundamental reasons. First, the possibility that cyber malefactors will simply decide to switch to softer targets when one's defenses improve may be slim, as the targets of greatest value may not be available in places that are easy to breach. The intellectual property of leading American firms is not to be found in soft targets in other places around the world. Doenitz could move his U-boats to the Gulf of Mexico and the Caribbean knowing full well that ample oil tanker targets were in each maritime zone; thus, his payoff was still good. The world's softer cyber targets do not come replete with such high-value assets of their own.

The second problem with the hope that improved defenses will send attackers away in search of easier prey is that it is not enough to provide better security relative to the starting point. Rather, improvements must be substantial in *absolute* terms. The absolute capabilities for cyber defense in the United States, for example, have been quite poor for decades. Indeed, as noted earlier, former cyber czar Clarke and his colleague Knake rate them the worst defenses among all the major cyber powers.[22]

Their judgment has been affirmed by the long trail of high-profile hacks of major US commercial firms, as well as of sensitive government sites, and even the personal account of the director of central intelligence. Thus, making substantial improvements in the relative level of cybersecurity will likely not do enough to drive away the intruders.

Clearly, what is needed at this point is a paradigm shift in the whole way of thinking about cybersecurity. Ample evidence shows firewalls, the latter-day equivalents of Admiral Andrews's "sheltered harbors," are as ineffective as were his faulty remedies back then. Instead, stored data can and should be "blacked out," and information flows can be well "escorted" by the employment of very strong encryption and evasively routed via the Cloud.

These sorts of steps are only now beginning to be regularly taken in the United States, but they are serious indicators of real progress. Still, the habits of mind of those who rely on massive data flows and their ready availability remain steeped in the old paradigm, one on which the existing cybersecurity consulting industry is itself all too dependent. New defensive methods simply must be considered.

Comparing the Pearl Harbor and Harbor Lights Analogies

In light of the abovementioned concerns, how are good cybersecurity legislation and regulation to be enacted and pursued? In the United States, the Obama administration relied heavily on the Pearl Harbor analogy; indeed, it was a main line of argument advanced by former secretary of defense Leon Panetta when he was in office.[23]

But as this chapter has argued, this analogy has a fundamental problem: Pearl Harbor speaks primarily to the strategic and military aspects of cybersecurity. Defending the virtual domain from costly, disruptive hacks, however, has profound economic and political dimensions. With these factors in mind, I propose adding "harbor lights" to Pearl Harbor in making an operative analogy.

In December 1941 a great deal of US naval power was concentrated at Pearl Harbor, and a sharp blow to it was inflicted, enabling Japan to pursue its expansionist aims for a while. Of the eight US Navy battleships berthed there, four were sunk and another four seriously damaged. And if the *Kido Butai,* the Japanese carrier strike force, had caught the three American aircraft carriers deployed to the Pacific in port—they were out to sea at the time of the attack—or had blown up the base's massive fuel storage tanks, the damage would have been catastrophic. Pearl Harbor was a true single point of failure. And if the Japanese had not been outfoxed and outfought at Midway, even those surviving aircraft carriers would have been of little moment in the Pacific war's strategic balance.[24]

Nothing quite like the sort of concentration of power in a battleship row now exists in cyberspace. Indeed, part of the logic behind the creation over forty years ago of an Advanced Research Projects Agency Network, which would prove to be a key building block of the Internet, was to ensure continued communications even in the wake of a nuclear war. Redundancy and resilience are the key notions that lie at the heart of the structure of cyberspace.[25] Yes, there are very important, even "critical" nodes here and there, but work-arounds and fallbacks abound too. Thus, cyberspace is similar to the oceans that cover two-thirds of the world in that it has its various choke points, but there are always alternate routes.

If the Pearl Harbor analogy is somewhat limited, perhaps even misleading, it is because it encourages the dangerous belief that defenses can be concentrated in one or a few major areas to provide strategic protection to most, if not the vast majority, of threatened spaces. The harbor lights analogy is both more expansive conceptually—in that it speaks to military, economic, and political factors—and

more accurately depicts the widely distributed defensive challenge that characterizes efforts to secure cyberspace.

This new analogy speaks in an interesting way to military matters, but its true value lies in engaging the range of politico-economic challenges. They are delineated in the harbor lights analogy by the costly failure of President Roosevelt to order a blackout along the East Coast, despite the growing depredations of the U-boat skippers, who were having their "happy time" teeing up targets for night attacks because they were so well illuminated.

Clearly, the harbor and other coastal lights stayed on far too long. In search of causation, this illustration leads us to the point that the failure, though ultimately FDR's, was driven by local political pressures, which were themselves the product of economic considerations. For several months in 1942, mayors of coastal cities resisted pressure to enforce blackouts because they feared a loss of business would ensue and plunge their economies, still not yet fully recovered from the Depression, into fresh downward spirals. It was only when the shipping losses grew to dangerously high levels that the blackout was finally put in place and merchant ships began to move in escorted convoys. This tactic didn't put an end to the U-boat menace, but it did bring it under control and encouraged Admiral Doenitz to send his submarines elsewhere in search of prey.

Today, the harbor lights are on—all over cyberspace. A wide range of targets is well illuminated and highly vulnerable to all manner of cyber mischief. Technologically advanced armed forces, all of which are increasingly dependent on their connectivity to operate effectively in battle, can be virtually crippled in the field, at sea, or in the air by disruptive attacks on the infrastructure on which they depend but that are often not even government owned.

As to leading commercial enterprises, they hemorrhage intellectual property to cyber snoops every day—a point Governor Mitt Romney made twice in debates with President Obama during the 2012 election campaign. Regarding mass publics, countless millions of people in the United States and around the world have had their personal security hacked and now serve unwittingly as drones, or zombies, impressed into service in the robot networks, or botnets, of master hackers. As do billions of their Internet-connected smart home appliances.

Why do the harbor lights remain on in cyberspace? Because rather than focusing on security, for decades IT manufacturers and software developers have been driven by market forces impelling them to seek greater speed and efficiency in their products—all at highly competitive consumer prices. In short, the virtual harbor lights have stayed on because the perceived economic costs of improved security—that is, of enforcing a virtual blackout—have been seen as too high. And, just as FDR did, American political leaders today have shied away from forcing the private sector's hand. In this current case, however, the motivations of those in government are a bit more mixed. Their reluctance to champion, or even to require, production of the most secure cyber products extends far beyond fealty to market forces. Instead, the government's intelligence and, even more, law enforcement departments fear that the improved security afforded by the ubiq-

uitous use of, say, strong encryption will curtail their own information-gathering capabilities.

Clearly, the harbor lights analogy speaks very powerfully to the economic and political dimensions of the cybersecurity challenge. But it has its limitations, as no analogy can address every aspect of a problem. One way the analogy breaks down is in its inability to speak to the "invisible" nature of many of today's cyber depredations. The mass ship sinkings of the early months of 1942 were tangible events that (eventually) horrified the nation and its civilian and military leaders. Today the ongoing compromise of highly sensitive military information systems, the theft of intellectual property, and the unwitting recruitment of men, women, and children into zombie armies all pass largely beneath our levels of awareness. Cyber warfare is a lot like Carl Sandburg's fog coming in on "little cat feet."[26]

Another problem is that whereas FDR had the authority to compel the darkening of coastal regions, it is not at all clear today that the president, or "government" more generally, has the same ability. Can the ubiquitous use of encryption, cloud computing, or other measures be dictated? Legislated? Likely not. Still, the presidency is a bully pulpit. If the chief executive were to use what presidential scholars such as Samuel Kernell and Richard Neustadt believe is the true power of the office—the power to persuade—then there would be a greater likelihood of gaining significant voluntary compliance.[27]

To be sure, senior civil and military leaders also know the gravity of the situation. For more than two decades, the National Academies of Sciences, Engineering, and Medicine have conducted deeply alarming studies of US cyber vulnerabilities and quite clearly conveyed the grave nature of the threat.[28] President Obama also expressed his desire to respond far more decisively to the cyber threat in Presidential Decision Directive 20. Reporting about the still-classified directive—partially "outed" first in a *Washington Post* article in 2012 and by Edward Snowden's revelations in 2013—suggests that the directive takes an expansive view of cybersecurity, even to the point of taking preemptive action against cyber threats.[29]

All this implies clear awareness of the problem, but the proactive recommendation to seek out and attack the attackers may prove problematic, given how well hidden so many of them remain. All these years after the Code Red and Nimda computer viruses were unleashed—shortly after the attacks of September 11, 2001—the identities of those perpetrators are still unknown. As is true of many—or perhaps most—cyber attacks, digital warriors and terrorists today hide in the virtual ocean of cyberspace as well as the U-boat skippers did during their happy time along the Atlantic seaboard seventy-five years ago. Efforts to track them in advance of their attacks, to hearken yet again to the harbor lights analogy, will be as fruitless as the US Navy's first strategy in 1942 of sending out hunter-killer squadrons to search the ocean for the U-boats.[30]

In 1942 the right answer from the start was to black out coastal cities at night and to have ships evasively routed and escorted by antisubmarine vessels when they sailed. Losses still occurred after adopting these strategies but soon fell to

acceptable levels. This is the lesson of the harbor lights. In cyberspace, the analogous way to embrace this approach would consist of far greater use of strong encryption and evasive routing of data via the Cloud, making it much harder for the virtual U-boat wolf packs that stalk them to find their targets.

We need not forget Pearl Harbor when thinking about cybersecurity. But surely we also need to remember the harbor lights. This is as true for the increasingly interconnected world community as it is for the United States.

Notes

1. Both quotes are from P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 8.

2. Jennifer Steinhauer, "Senate Rejects Measure to Strengthen Cybersecurity," *New York Times,* June 11, 2015, brings the record of failure up to the near present.

3. See Patrick G. Eddington and Sascha Meinrath, "Why the Information Sharing Bill Is Anti-Cybersecurity," *Christian Science Monitor,* July 22, 2015.

4. See the McAfee-Intel Security report, *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, DC: Center for Strategic and International Studies, 2014), which estimates the global cost of hacking at an amount ranging as high as $500 billion, with $100 billion lost in the United States alone.

5. Spencer Ackerman, "FBI Chief Wants 'Backdoor Access' to Encrypted Communications," *The Guardian,* July 8, 2015. This is a long-standing attitude, going back to the time when it was illegal for individuals to possess strong encryption technology. See the story of the "code rebels" who disseminated these tools, despite government opposition, in Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (New York: Penguin, 2002). See also Nicole Perlroth and David E. Sanger, "Obama Won't Seek Access to Encrypted User Data," *New York Times,* October 10, 2015.

6. See especially Richard A. Clarke and Robert A. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010) for a comprehensive exposition of the challenges to achieving a truly robust cyber security system in the United States.

7. Thomas Bailey, *A Diplomatic History of the American People* (New York: Appleton-Century-Crofts, 1955), 798. Gallup statistics cited from the same page.

8. Axis submarines sank nearly five million tons of Britain-bound merchant shipping from 1939 to 1941. See statistics in John Ellis, *Brute Force: Allied Strategy and Tactics in the Second World War* (New York: Viking, 1990), 138–46.

9. Harald Busch, *U-Boats at War: German Submarines in Action, 1939–1945,* trans. L. P. R. Wilson (New York: Ballantine Books, 1955), 44.

10. The quotes are taken from Samuel Eliot Morison, *The Two-Ocean War: A Short History of the United States Navy in the Second World War* (Boston: Little, Brown, 1963), 109.

11. Henry H. Adams, *1942: The Year That Doomed the Axis* (New York: David McKay, 1967), 77.

12. Cited in Homer H. Hickam Jr., *Torpedo Junction: U-Boat War off America's East Coast, 1942* (Annapolis: US Naval Institute Press, 1989), 116.

13. Michael Gannon, *Operation Drumbeat: The Dramatic True Story of Germany's First U-Boat Attacks along the American Coast in World War II* (New York: Harper & Row, 1990), 385.

14. Statistics are from official German war records, cited in the appendix to Hickam, *Torpedo Junction,* 296–305.

15. Wolfgang Frank, *The Sea Wolves: The Story of German U-Boats at War,* trans. R. O. B. Long (New York: Rinehart & Company, 1955), 173.

16. Clarke and Knake, *Cyber War,* 113 for the quote, 148 for the defense rating.

17. Cited in Lolita C. Baldor, "Obama Announces U.S. Cyber Security Plan," NBC News, May 29, 2009, http://www.nbcnews.com/id/30998004/ns/technology_and_science-security/t/obama-announces-us-cyber-security-plan/#.WPJvEbGZOf4.

18. Howard Schmidt, "Defending Cyberspace: The View from Washington," *The Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 50. His article was part of a debate in that same issue, to which my contribution was "The Computer Mouse That Roared: Cyberwar in the Twenty-First Century," 39–48.

19. See, for example, "Obama's 'Cybersecurity Czar' Is MIA as Hackers Run Wild," *Investor's Business Daily,* June 5, 2015. The piece reflects the opinion of the influential journal's editors.

20. On cloud security, see Vic Winkler, *Securing the Cloud: Cloud Security Techniques and Tactics* (Waltham, MA: Elsevier, 2011); and Madhin Srinavasin et al., "State-of-the-art Cloud Security Taxonomies," in *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, ed. Sabu M. Thampi, El-Sayed El-Afry, and Javier Aguiar (New York: ACM, 2012), 470–76.

21. One of the best accounts of the factors leading to Doenitz's defeat can be found in Michael Gannon, *Black May: The Epic Story of the Allies' Defeat of the German U-Boats in May 1943* (New York: HarperCollins, 1998). On breaking the Enigma codes, see David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes* (Boston: Houghton Mifflin, 1991).

22. Clarke and Knake, in *Cyber War,* 148, rate US cybersecurity relative to others' cybersecurity; but the authors also make clear throughout their study that they consider the absolute level of American cyber defenses to be poor as well.

23. See my critique of the Obama administration's central focus on this analogy, "Panetta's Wrong about a Cyber Pearl Harbor," *Foreign Policy*, November 20, 2012.

24. The Japanese were under no illusions about the consequences of their defeat at Midway. See Mitsuo Fuchida and Masatake Okumiya, *Midway: The Battle that Doomed Japan* (Annapolis: US Naval Institute Press, 1955). Fuchida was the flight leader in the attack on Pearl Harbor.

25. The first public demonstration of the ARPANET took place in October 1972. One of its founding fathers, Jacques Vallee, in his memoir *The Heart of the Internet: An Insider's View of the Origin and Promise of the On-Line Revolution* (Charlottesville, VA: Hampton Roads Publishing, 2003), notes that resilience was crucial to the ability of cyberspace to "grow organically" (77).

26. "Fog" is a short poem that fits the harbor lights analogy well: "The fog comes / on little cat feet. / It sits looking / over harbor and city / on silent haunches / and then moves on." A good link to and analysis of the poem is found at "Fog (poem)," Wikipedia, last modified March 31, 2017, https://en.wikipedia.org/wiki/Fog_(poem).

27. Samuel Kernell, *Going Public: New Strategies of Presidential Leadership,* 4th ed. (Washington, DC: Congressional Quarterly Press, 2006); and Richard E. Neustadt, *Presidential Power and the Modern Presidents* (New York: Free Press, 1991).

28. See especially three studies from National Academies Press (Washington, DC) that have addressed key issues raised in this chapter: Kenneth W. Dam and Herbert S. Lin, eds., *Cryptography's Role in Securing the Information Society* (1996); *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (2002); and *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (2014).

29. Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *Washington Post,* November 14, 2012. In January 2013 the Obama White House also issued a condensed "fact sheet" about the directive. See also Office of the Press Secretary, "Fact Sheet: Presidential Policy Directive on Critical Infrastructure Security and Resilience," the White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/fact-sheet-presidential-policy-directive-critical-infrastructure-securit.

30. Hickam, *Torpedo Junction,* provides a full narrative of this initial effort.