Cyber's Cost
The Potential Price Tag of a Targeted "Trust Attack"

Ian T. Brown

Abstract: In 2015, Chinese hackers breached the Office of Personnel Management (OPM) and stole sensitive information on millions of federal employees. This article speculates how the Chinese government might use this information to construct a tailored cyberattack designed to paralyze an American military response to aggression in the South China Sea. This includes an assessment of potential second- and third-order economic impacts of such a cyberattack.

Keywords: cyber, cyberattack, China, South China Sea, trust attack, Office of Personnel Management, hack, OPM

> *What is the quickest way you can destroy an organization? . . . Mistrust and discord.*
>
> ~ Colonel John Boyd[1]

The cyberattack—both real and imagined—has come a long way since Matthew Broderick nearly caused World War III with a 1,200 bit-per-second modem and rotary phone in 1983.[2] In the fictional realm, Broderick's duel with the War Operation Plan Response computer has given way

Maj Ian T. Brown is a U.S. Marine Corps Sikorsky CH-53E Super Stallion helicopter pilot. He has previously written about conflict theory and cyberwarfare in the *Marine Corps Gazette*, *War on the Rocks*, *The Strategy Bridge*, and he has discussed it in the *Professional Military Education* podcast. He recently published *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare* with MCU Press; it is a reexamination of the development of maneuver warfare doctrine in the Marine Corps. This article was adapted from an article previously published in May 2018 in *War on the Rocks* and the material was used with permission, for which the author is grateful to present the adapted material to a broader venue. The opinions expressed here are the author's alone and do not reflect those of the U.S. Marine Corps, the Department of Defense, or any part of the U.S. government.

to the infrastructure "fire sale" from *Live Free or Die Hard* and, most recently, the multilayered sabotage of everything from GPS to stealth fighters in the book *Ghost Fleet*.[3] The real world has seen cyber surprises only a step removed from fantasy, with various actors disrupting civil networks and infrastructure, subverting military research projects, and using preparatory cyber fires as a precursor to physical military activity.[4]

However, even as authors, screenwriters, and policy makers grapple with the potential fallout from cyber vulnerabilities in the physical realm—the blinding of sensors, the degradation of communications networks, or deliberate infrastructure malfunctions—modern cyberattacks are increasingly aiming at the adversary's less tangible mental and moral capabilities. The starkest example of this can be seen in Russia's interference in the 2016 American presidential election, which significantly damaged those intangibles—faith in social and traditional media, transparency in political campaigning, even confidence in the integrity of the election results themselves—that will take a long time to repair.[5]

This author had these ideas in mind, along with Boyd's words about the best way to destroy an organization, while participating in a working group hosted by the Center for Strategic and International Studies (CSIS) on the topic of surprise in great power conflict.[6] The author expanded on this topic in a later article by envisioning a hypothetical "trust attack" directed against Department of Defense (DOD) personnel as the opening salvo to conventional military operations.[7] In their valuable article on the subject, Neal A. Pollard, Adam Segal, and Matthew G. Devost defined a cyber *trust attack* as seeking to make "an individual . . . lose faith both in the specific computer systems and in the institutions and values that rely on those networks."[8] The author's initial examination of cyberwar specifically targeting American servicemembers focused on the immediate mental and moral impact of such a strike. Yet, that type of attack also would likely have significant economic repercussions, both on the individual warfighter and those institutions used to target them. Indeed, a cyber adversary could deliberately include fiscal fallout as a secondary target. The economic damage of a trust attack might both heighten the confusion across the DOD and delay an effective response, acting as a feedback loop to exacerbate the mental and moral impact of the initial strike. This article will first explore the mental and moral aspects of a cyber trust attack, and then examine how the second- and third-order economic effects would magnify the impact of the initial strike.

Envisioning a Chinese Trust Attack

The author's initial hypothetical and fictional vignette or scenario—entitled "Assassin's Mace"—is appended to CSIS's final report.[9] "Assassin's Mace" envisions how China might seek to exploit its 2015 hack of the United States

Office of Personnel Management (OPM) database in conjunction with a wider military operation.[10] By the time OPM security engineers detected the intrusion, hackers had enjoyed access to the OPM records—including millions of background checks, personnel files, and digital fingerprints—for almost a year. The OPM hack was by no means the first large-scale breach of a protected database, but it was unique in two aspects.[11] First, these records contain by far the most detailed personal information yet accessed by a cyber intruder; second, the hackers have not yet attempted traditional data exploitation by a widespread ransoming of the data back to the agency or selling it to third parties.[12] These facts suggest that the hackers have plans for the data beyond a quick payday. A widespread trust attack on DOD personnel would be one of the few things that could justify sitting on a goldmine of exploitable data. Moreover, knowing that it could only exploit this information for so long before American countermeasures came into play, the author believes this implied the Chinese government would want to attack as many targets as possible at once, generate maximum confusion, and then use that window of confusion to quickly achieve goals it could not otherwise achieve with a smaller attack. "Assassin's Mace" imagines a Chinese cyberattack using the sensitive and detailed OPM records—not to disrupt or degrade American military or intelligence systems—but rather to spread fear, mistrust, and discord among the men and women in uniform who operate those systems. During such a strike, hackers would lock out medical records, wipe away financial information, manipulate social media, and spread lies and half-truths about personal misconduct.

How might China shape such an attack? First, it is difficult to understate the value of the records China stole. Background investigations, personnel files, digital fingerprint images, former addresses, phone numbers, Social Security numbers, lists of family members, dependents, and friends: these are all nuggets of unique information—and frequently the answer to security questions—that a motivated attacker could turn into keys unlocking virtually any digital account owned by the targeted individual or group. An intruder seeking to impersonate another person could not ask for a more comprehensive data set.

Second, a concerted attack exploiting OPM data would avoid patterns making it obvious that an attack was happening. "Assassin's Mace" incorporates many variations. Navy sailors at a strategic port in Japan would find their families' bank accounts emptied.[13] Others would receive death threats on their Twitter feeds, with hackers adding further confusion by posing as third parties.[14] "Assassin's Mace" even imagines military spouses having intimate photographs blasted across social media and this was before the latest revelation of military-sourced revenge porn.[15] Illustrating how effective even a single hacker can be, one man using a phishing scheme managed to hack the login credentials of 250 celebrities to access their most intimate photos.[16] A dedicated team of cyber

intruders with the wealth of OPM records at their fingertips would find their phishing expeditions much simpler, and they would be able to harm people who are vital to national security.

An attacker could wreak further havoc by locking out digital medical records with ransomware, as North Korea allegedly did in the WannaCry episode in 2017.[17] That intrusion alone canceled surgical operations and delayed appointments across the entirety of Britain's National Health Service (NHS). Medical hackers could also steal private records and threaten to sell the material on the dark web.[18] A few well-publicized penetrations of personal devices belonging to senior officials—such as the hack of former White House chief of staff John F. Kelly's cell phone—could spread further fear.[19]

These efforts would strike at the individual level. But as Boyd explained, the overall goal is destroying the cohesion of the organization. Thus, an attacker could combine individual confusion with undermining key trusted leadership. The best way to do this is to mix lies with the truth. Unfortunately, scandals such as Marines United, Fat Leonard, and other harassment claims have already sown mistrust in the public mind and among the ranks.[20] It is entirely possible to envision China's People's Liberation Army Strategic Support Force using personal information from OPM records to gain access to the accounts of senior leaders and hijacking them to plant and spread incriminating material.[21]

An adept cyber competitor also might seek to weaken America's alliances. "Assassin's Mace" describes the viral dissemination of a YouTube video showing American servicemembers stationed on Okinawa sexually assaulting local citizens. Uniformed Americans have a dark history of sexual misconduct on the island, and the U.S. military's presence there is fraught with other tensions.[22] Using bots, trolls, voice clones, artificial intelligence, and generative adversarial networks, China could create fake videos to turn the Okinawan population and Japanese government against America.[23] Such *deepfake* videos—which use parallel artificial intelligence algorithms available in the public domain to match and swap photographed facial expressions from source pictures onto a different target body—have been used to create increasingly realistic pornographic videos.[24] Again, exploiting personal information from OPM records, it does not strain credulity to imagine Chinese hackers accessing a servicemember's personal social media images, deepfaking and posting an explosive video, and then letting mistrust and confusion poison the relationship.

The Price Tag

The original "Assassin's Mace" vignette ends at this point, with China's cyber onslaught against DOD personnel disrupting their personal lives, poisoning command relationships, and corrupting key alliances to keep the American military from responding effectively to any follow-on conventional action by Chi-

na in the South Pacific. Yet, the history of recent hacking operations—as will be highlighted below—has often included a significant economic component, both in the immediate aftermath of a breach and in the days and weeks that followed, as impacted organizations and the public gained awareness of the attack's scope. This would inevitably hold true in the case of a broad trust attack; indeed, a shrewd, experienced cyber adversary such as the Chinese government would likely count on the financial fallout to act as a feedback loop for the original attack. This feedback loop would cause cascading second- and third-order effects, amplifying the impact of the initial attack and further disrupting the United States' ability to respond to any conventional Chinese military aggression.

Real-world attacks provide a useful benchmark for gauging potential fiscal damages from the hypothetical breaches described in the previous pages. As of 2017, the OPM hack had already cost the U.S. government more than $1 billion, with much of that cost coming from identity theft protection offered to the 21 million federal employees affected.[25] That cost could balloon further, as this summer American legislators proposed a bill that would provide the victims lifetime identity protection, past the currently approved 2026 expiration date.[26] Multiply that initial $1 billion price tag across the lifetimes of 21 million federal workers, and even with some age variation among affected employees, the cost alone of lifelong identity monitoring could easily exceed hundreds of billions of dollars. A future trust attack against those federal employees exposed by the OPM hack, along with their dependents, would have additional costs in nongovernmental identity protection and in potential lawsuits filed against federal agencies.

Examples of these costs in other real-world examples include the 2006 hack of TJX Companies, which cost the company and affected banks and insurers more than $200 million in litigation and insurance payouts; the 2011 breach of Sony PlayStation Network cost the company $15 million in lawsuits, on top of the $171 million lost during the month the gaming network was down. In the same year, RSA Security was hacked and forced to pay $66 million in remediation; and in 2014, when hackers exposed the financial information of 56 million Home Depot customers, the company paid out $161 million in lawsuits and insurance.[27] It does not stretch credulity to imagine an explosion of lawsuits filed against the government were its employees to discover that, once again, the agency charged with safeguarding sensitive personal information had failed them.

Cyberattacks targeting more intimate data repositories, such as social media and medical records, also have caused extensive economic loss. The WannaCry ransomware breach cited above cost the NHS almost $100 million in rescheduled medical procedures and repairs to the NHS information technology net-

work.[28] Globally, WannaCry cost affected countries more than $8 billion, and a similar ransomware attack called NotPetya generated another $850 million in losses in 2017.[29] Stunning as these numbers are, they came from relatively limited target sets; a recent exercise that simulated the deep breach of a cloud-based service—capable of striking a high volume of targets—resulted in an estimated loss of more than $53 billion.[30]

When investigators determined that data provided by Facebook to the firm Cambridge Analytica had then been improperly shared with third parties to influence political advertising during the 2016 presidential election, Facebook rapidly lost more than $42 billion in its market value.[31] While recovering from this scandal, Facebook admitted later in 2018 to another hack that exposed more than 30 million users to the loss of personal information including names, phone numbers, and birth dates: precisely the type of sensitive data a malign actor could use to penetrate financial accounts.[32] The breach of John Kelly's cell phone raises the specter of a cyberattacker using what appears to be a valid social media account from a supposedly secure personal electronic device to induce market chaos.

Recent history offers several examples of what social media screeds from prominent American political leaders can do to financial markets. The world saw two instances of this in December 2018 alone. Early in the month, President Donald Trump's tweet about being a "Tariff Man" raised uncertainty about a trade deal that the United States and China had just reached; the stock indexes most likely to be affected by that deal lost between 3–4 percent of their value almost immediately.[33] Only a few weeks later, another tweet from the president criticizing the chairman of the Federal Reserve was rapidly followed by 2–3 percent losses across stocks on Wall Street.[34] Stock markets have always been vulnerable to the volatility of emotion and perception, and an attacker able to access the private media accounts of prominent political leaders would likely seek to exploit that in a widespread cyberstrike.

The evidence above details some of the second-order economic damage a hacker using data gleaned from the OPM database could inflict. Yet, there are third-order effects apart from these that would act as amplifying feedback loops, spreading the chaos and disorder beyond the immediate confines of vulnerable federal employees. OPM victims would merely become vectors for market instabilities that could affect any American invested in the stock of large corporations. And again, history has already provided ample evidence of these companies' susceptibility to cyberwar. The Yahoo breach of 2013–14 knocked $350 million off the company's value when it was put up for sale; the hack Target experienced in 2013 caused the resignation of the business's chief information officer and chief executive officer, along with a loss of $162 million; and the Uber breach of 2016 cost the company a staggering $20 billion loss in

market valuation.[35] In 2018, when Bloomberg News reported that China had potentially inserted compromised microchips into both Apple and Amazon devices, each company rapidly lost 5 percent of its market value despite vehement denials of any such intrusions.[36]

Moreover, while the author discussed the potential diplomatic impact of faked videos used to drive a wedge between the United States and key allies, an attacker could tailor a fiscal component to their fakery as well. Commercial advertisers would not run the risk of their ads popping up next to videos showing sexual violence by American servicemembers against local civilians. Companies would likely pull their digital advertisements, precisely as several major corporations pulled marketing dollars from YouTube in 2017 after learning their ads ran next to several violent extremist videos in a boycott that cost Google millions.[37] Taken together, these historical trends paint a disturbing picture of what might happen following a broad-based cyberattack targeting victims of the OPM breach. The financial instability following such a breach would rapidly extend beyond the immediate victims and their families. Simultaneous market losses hitting America's largest corporations—Amazon, Google, Apple, Facebook, and others—would crush the investment portfolios of virtually every American citizen. DOD personnel might be grappling with the mental and moral fallout of a targeted strike that stretched beyond the economic realm, but the American population as a whole would suddenly find itself caring far more deeply about the turmoil within its borders than the actions of an adversary overseas.

The Fallout

Cyber penetrations are rarely permanent; over time, experts usually find them and can often trace them with confidence to a particular group or country. Investigators would doubtless discover the truth eventually; but the point of such an attack, when combined with myriad other cyberstrikes, is to sow enough mistrust and discord that the organization's focus turns inward to deal with its own internal friction. A widespread, coordinated, and deep cyberbreach leveraged against American servicemembers could undermine individual and organizational morale to the point that the entire Department of Defense would be obligated to take an operational pause to sort out fact from fiction and let servicemembers get their lives back in order. This pause also would be in addition to the broader national disorders and delays caused by such a massive destabilization of financial markets. In the past, when facing a sufficiently severe problem, defense leaders have implemented wide-reaching pauses.[38] Individual commands also often execute stand-downs to address critical nonoperational problems, such as sexual assault or substance abuse.[39] Even if DOD leaders did not execute a formal operational pause, the functional effect would be the same:

individuals and units would turn their focus inward to deal with the myriad crises caused by simultaneous widespread cyberattacks.

China could potentially exploit the formal pause and overall national distraction to flood the South China Sea with conventional forces and pursue long-held national goals, be that securing economic supremacy across southeast Asia's waterways or isolating Taiwan. A surprise cyberattack targeting the personal lives of American servicemembers would enjoy the dual benefit of not requiring detectable physical preparations and making moot the question of how effective China's antiaccess/area denial and antistealth capabilities really are in combat.[40] Even just a few days of confusion would be enough for conventional Chinese forces to radically alter the balance of power in the South Pacific.

It is not impossible for organizations to recover from severe cyberattacks. Facebook took only two months for its market value to recover the $134 billion lost in the Cambridge Analytica data scandal; Marriott International offered customers identity monitoring and passport replacement costs following the years-long breach of its reservation database.[41] And one can always buy a new smartphone. Cohesion, morale, and fighting spirit, on the other hand, have no monitoring software, product replacement plan, or easily recoverable market value. A pervasive surprise cyberstrike, targeting those things closest to home for servicemembers, could—without firing a single bullet—have a devastating impact on the American military's ability to rapidly deploy, and it would generate lingering fear and mistrust even after counter-cyber efforts revealed the truth. Even if U.S. warfighters prove unexpectedly resilient, a market recovery two months after the fact does not offset the chaos caused by a rapid, short-term market destabilization that would paralyze an immediate American response to sudden Chinese military aggression.

Not Just a Hypothetical

There are historical precedents for a widespread cyberattack used either to significantly disrupt an adversary's government as a goal in itself or as a prelude to military action. Russia preceded its invasions of Georgia, Crimea, and Ukraine with a variety of cyberoperations.[42] Aside from OPM, adversarial hackers have breached other American government agencies, such as the National Security Agency and the U.S. Department of State.[43] And the National Health Service attack in Britain demonstrated how hostile organizations can exploit personal information—in this case, medical records. The aforementioned hypotheticals differ only in degree from capabilities attackers already have. And the Chinese government, with its purloined OPM data, enjoys an access key that other entities, such as Russia, did not.

This author used the OPM hack as a starting point, but Russia's activities in the 2016 election provided a practical template for how a potential Chinese

attack might play out. That attack targeted trust and other intangibles, such as faith in the U.S. political system. Russian operatives directed their attack against a few target sets—social media channels, a political party's computer systems—and executed it with comparatively modest resources.[44]

Yet, Russia's trust attack did not fully exploit this method's potential. As noted in the official intelligence community assessment, Russia spread confusion and mistrust as apparent ends in themselves: "Russia's goals were to undermine public faith in the US democratic process . . . [to] apply lessons learned . . . to future influence efforts worldwide, including against US allies and their election processes."[45] Russia seemed satisfied with spreading confusion and mistrust where it could get easy access, such as social media and badly protected private networks. Russian hackers did not penetrate more hardened networks in the financial or defense sectors, possibly because they did not see the need, but more likely because they did not have an exploitable access point. Moreover, Russia did not capitalize on the confusion achieved in the United States as an opportunity to pursue national objectives requiring a direct confrontation with America.

China, on the other hand, has both the opportunity and need for a maximized trust attack. The opportunity lies in possessing exploitable information that Russia lacked: the OPM database. Its need stems from the fact that any robust pursuit of national objectives in the South China Sea and against Taiwan would put it in direct conflict with American interests.[46] While China has generally eschewed direct confrontation in recent years, the United States should not dismiss the possibility that China's leaders might think they could come out ahead in a direct confrontation in their virtual backyard, especially in the wake of a debilitating trust attack against the American military and national economy.

Conclusion

As Mark F. Cancian noted in the final CSIS report, the United States is particularly vulnerable to the surprise attack today because many of its discussions about conflict display a disturbing hubris. "Senior officials," Cancian notes, "have repeatedly made claims that the U.S. military is not just the best in the world but the best the world has ever known. As with Greek heroes of legend and literature, hubris can lead to downfall."[47] The American military might enjoy an unmatched level of funding and equipment, but it could all be rendered moot by a cyberattack that bypassed the military's physical superiority to disrupt its moral capacity to fight. Moreover, as the historical data in this article has shown, American companies remain susceptible to costly data breaches, and America's financial markets regularly suffer in the aftermath. And it seems any assumption by the public that the federal government, at least, has learned some

lessons from the OPM hack is misplaced: as of the end of 2018, OPM still has not implemented many key recommendations from the Government Accountability Office on securing its data, including the continued use of passwords that hackers compromised in the original 2015 breach.[48]

This inactivity implies that, despite lip service and congressional hearings to the contrary, America's senior politicians, bureaucrats, and military leaders remain insouciant about the threat posed to the United States by a catastrophic cyberattack capable of incapacitating its military and paralyzing the economic lifeblood of the country.[49] This author believes that, to the contrary, the many real-life events described above suggest that a competent adversary armed with the right information could indeed aim such an attack against the United States and its armed forces. China has shown itself to be a competent and shrewd competitor in many arenas, but particularly in its theft of the treasure trove of OPM data. Such data is precisely the type of key a competent adversary could use to devastating effect, if it so chose. This author believes that the fact China has, to date, chosen not to use the data suggests it is waiting for a moment when it will maximize the advantages it can gain from it. The American government needs to heed the hard lessons it has already endured in disruptive practice runs such as the OPM hack and 2016 election; those may be the last warnings it gets before an opponent initiates an attack sufficiently catastrophic that it truly alters the balance of power in a region critical to America's interests.

Notes

1. Ian T. Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare* (Quantico, VA: Marine Corps University Press, 2018), 229.
2. Scott Brown, "*WarGames*: A Look Back at the Film that Turned Geeks and Phreaks into Stars," *Wired*, 21 July 2008.
3. *Live Free or Die Hard*, directed by Len Wiseman (Los Angeles, CA: Twentieth Century Fox Film Corporation, 2007), digital; and P. W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War* (New York: Houghton Mifflin Harcourt, 2015).
4. Kim Sengupta, "ISIS-Linked Hackers Attack NHS Websites to Show Gruesome Syrian Civil War Images," *Independent*, 7 February 2017; James Titcomb, "Every Wi-Fi Network at Risk of Unprecedented 'Krack' Hacking Attack," *Telegraph*, 16 October 2017; Andrea Mitchell and Ken Dilanian, "Experts: North Korea Targeted U.S. Electric Power Companies," NBC News, 10 October 2017; Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," *Time*, 24 March 2016; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014; and Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, 20 June 2017.
5. Determining the quantifiable impact of Russia's interference in the 2016 election is a very difficult—perhaps impossible—exercise. However, many sources have amply documented the stark fact that Russia was injecting its own desired information into the news and social media cycles of that election; for example, see Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (New York: HarperCollins, 2018); "Russia Spent $1.25M per Month on Ads, Acted Like an Ad Agency: Mueller," *AdAge*, 16 February 2018; *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D (Washington, DC: Office of the Director of National Intelligence, 2017); Jonathan Masters, "Rus-

sia, Trump, and the 2016 U.S. Election," Council on Foreign Relations, 26 February 2018; and Mary Louise Kelly and Emma Bowman, "CIA Concludes Russian Interference Aimed to Elect Trump," NPR, 10 December 2016.

6. To read the final study, see Mark F. Cancian, *Coping with Surprise in Great Power Conflicts* (Washington, DC: Center for Strategic and International Studies, 2018).
7. Ian Brown, "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust?," *War on the Rocks*, 22 May 2018. For the original article focusing on the detailed nature and history of "trust attacks," see Neal A. Pollard et al., "Trust War: Dangerous Trends in Cyber Conflict," *War on the Rocks*, 16 January 2018.
8. Pollard et al., "Trust War."
9. Cancian, *Coping with Surprise in Great Power Conflicts*, 109–11.
10. Brendan I. Koerner, "Inside the Cyberattack that Shocked the U.S. Government," *Wired*, 23 October 2016.
11. Taylor Armerding, "The 18 Biggest Data Breaches of the 21st Century," *CSO Online*, 20 December 2018.
12. Chris Strohm, "Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says," *Bloomberg*, 28 September 2017.
13. Iain Thomson, "Hackers Nick $60m from Taiwanese Bank in Tailored SWIFT Attack," *Register*, 11 October 2017.
14. Barack Obama, interview by Mary Louise Kelly and Audie Cornish, "ISIS Uses Cyber Capabilities to Attack the U.S. Online" (transcript), NPR, 25 April 2016; Emma Graham-Harrison, "Could ISIS's 'Cyber Caliphate' Unleash a Deadly Attack on Key Targets?," *Guardian*, 12 April 2015; and Raphael Satter, "Russians Posed as ISIS Hackers, Threatened US Military Wives," Military.com, 8 May 2018.
15. Alexa Liautaud, "Explicit Photos of Female Service Members Are Being Shared in a Dropbox Folder Called 'Hoes Hoin'," *Vice News*, 9 March 2018.
16. Jessica Lerner, "North Branford Man Admits Hacking iCloud Accounts of 250 People, Celebrities," *New Haven (CT) Register*, 12 April 2018.
17. Dan Bilefsky, "Britain Says North Korea Was Behind Cyberattack on Health Service," *New York Times*, 27 October 2017.
18. "Healthcare Under Attack: What Happens to Stolen Medical Records?," *Trend Micro*, 30 June 2016.
19. Lily Hay Newman, "The Worst-Case Scenario for John Kelly's Hacked Phone," *Wired*, 6 October 2017.
20. Shawn Snow, "Seven Marines Court-Martialed in Wake of Marines United Scandal," *Marine Corps Times*, 1 March 2018; Mark D. Faram, "Officer Accused of Patronizing Prostitutes Worked in Sex Assault Prevention Office while Awaiting Court-Martial," *Navy Times*, 9 March 2018; and Mark D. Faram, "7th Fleet Amphib Squadron Leadership Fired," *Navy Times*, 26 February 2018.
21. Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *Diplomat*, 1 April 2017.
22. "Okinawa Rape and Murder: U.S. Military Base Worker Shinzato Jailed in Japan," *BBC*, 1 December 2017; Andrew Pollack, "One Pleads Guilty to Okinawa Rape; 2 Others Admit Role," *New York Times*, 8 November 1995; "U.S. Sailors Admit Okinawa Rape," *BBC*, 26 February 2013; "U.S. Military Chopper Bursts into Flames on Landing in Okinawa," *Kyodo (Tokyo) News*, 11 October 2017; and Anna Fifield, "U.S. Military Imposes Alcohol Ban across Japan after Fatal Okinawa Crash," *Washington Post*, 19 November 2017.
23. The term *generative adversarial network* (GAN) refers to a type of artificial intelligence machine learning technique made up of two nets that are in competition with one another in a zero-sum game framework. GANs typically run unsupervised, teaching itself how to mimic any given distribution of data. James Tapsfield, "Could Robots Pretend to Be YOU?: Cyber Security Experts Warn that AI Could Mimic Writing Styles and Habits of Millions of Users to Launch Devastating Scams," *Daily Mail*, 27 February 2018; Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," *New York Times*, 18 February 2018; Brian Wang, "AI Voice Clon-

ing from a Few Seconds of Voice Sampling Is Real and Rapidly Improving," *Next Big Future*, 27 February 2018; Amy Zegart, "Even Cybersecurity Is Bigger in Texas," *Horns of a Dilemma* (podcast), 30 March 2018; and Jonathan Aberman, "Fake Video: What Do We Do When Seeing Is Not Believing?," *Washington Post*, 29 January 2018.

24. Drew Harwell, "Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: 'Everybody Is a Potential Target'," *Washington Post*, 30 December 2018.
25. Chris Townsend, "OPM Breach Costs Could Exceed $1 Billion," *Symantec Thought Leadership* (blog), 23 March 2017.
26. Derek Hawkins, "The Cybersecurity 202: 'A Wake Up Call.' OPM Data Stolen Years Ago Surfacing Now in Financial Fraud Case," *Washington Post*, 20 June 2018.
27. Armerding, "The 18 Biggest Data Breaches of the 21st Century."
28. Carly Page, "WannaCry Attack Cost Cash-Strapped NHS an Estimated £92m," *Inquirer*, 15 October 2018.
29. Suzanne Barlyn, "Global Cyber Attack Could Spur $53 Billion in Losses: Lloyd's of London," *Reuters*, 16 July 2017.
30. Barlyn, "Global Cyber Attack Could Spur $53 Billion in Losses."
31. "Facebook Stock Loses $42 Billion Amid Data Hacking Scandal," Nine.com, 19 March 2018.
32. Troy Wolverton, "Hackers Stole Millions of Facebook Users' Personal Data—Here's Why You Should Be Worried," *Business Insider*, 12 October 2018.
33. "Stock Markets Plunge after Trump's 'Tariff Man' Tweet," *New York Post*, 4 December 2018.
34. Alex Veiga, "Trump Once Boasted of Market Gains, Now Tweets Cause Drops," *Washington Times*, 25 December 2018.
35. Armerding, "The 18 Biggest Data Breaches of the 21st Century."
36. Mike Murphy, "Homeland Security Says It Has No Reason to Doubt Spy-Chip Denials by Apple, Amazon," *MarketWatch*, 7 October 2018.
37. Olivia Solon, "Google's Bad Week: YouTube Loses Millions as Advertising Row Reaches U.S.," *Guardian*, 25 March 2017.
38. "Navy Orders Complete Standdown," *CBSNews*, 15 September 2000; and Megan Eckstein, "Marine Corps Orders 24-Hour Operational Pause for All Aviation Units within Next 2 Weeks," *USNI News*, 11 August 2017.
39. SrA Katrina Heikkinen (USAF), "SAPR Stand-Down Day: Deter, Ensure, Rebuild," Air Force Global Strike Command, 13 May 2014; David San Miguel, "ACC Stand Down Raises Sexual Assault Awareness," U.S. Army, 13 June 2013; and Dustin Perry, "Camp Zama Hosts Safety Stand-Down Day, Effects of Alcohol Training Event," U.S. Army, 8 January 2012.
40. Stephen Chen, "China Powers Up New Radar Tech to Unmask Stealth Fighters," *South China Morning Post* (Hong Kong), 27 September 2017.
41. Anthony Mirhaydari, "Facebook Stock Recovers All $134B Lost after Cambridge Analytica Data Scandal," *CBS News*, 10 May 2018; and Kari Paul, "Exclusive: After Massive Hack, Marriott Pledges to Pay for New Passports if Fraud Has Taken Place," *MarketWatch*, 4 December 2018.
42. Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, U.S. Army, 2011); Michael Holloway, "How Russia Weaponized Social Media in Crimea," RealClear Defense, 10 May 2017; and Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," Jamestown Foundation, 24 May 2017.
43. Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *Wall Street Journal*, 5 October 2017; Evan Perez and Shimon Prokupecz, "Sources: State Dept. Hack the 'Worst Ever'," CNN, 10 March 2015; Ellen Nakashima, "New Details Emerge about 2014 Russian Hack of the State Department: It Was 'Hand to Hand Combat'," *Washington Post*, 3 April 2017; and Susan Crabtree, "Obama Admin Did Not Publicly Disclose Iran Cyber-Attack During 'Side-Deal' Nuclear Negotiations," *Washington Free Beacon*, 7 June 2017.
44. "Russia Spent $1.25M Per Month on Ads."

45. *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ii–iii.
46. For analyses of China's strategic perspective, see LtCol Scott Cuomo et al., "Not Yet Openly at War, But Still Mostly at Peace," *Marine Corps Gazette* (February 2019); Brahma Chellaney, "China Expands Its Control in South China Sea," *(Tokyo) Japan Times*, 17 September 2018; and Toshi Yoshihara and James R. Holmes, *Red Star Over the Pacific: China's Rise and the Challenge to U.S. Maritime Strategy*, 2d ed. (Annapolis: Naval Institute Press, 2018).
47. Cancian, *Coping with Surprise in Great Power Conflicts*, vii–viii.
48. Lee Matthews, "Office of Personnel Management Still Vulnerable 3 Years After Massive Hack," *Forbes*, 15 November 2018.
49. Tarah Wheeler, "In Cyberware, There Are No Rules," *Foreign Policy*, 12 September 2018; and Sydney J. Freedberg Jr., "U.S. 'Gets Its Ass Handed to It' in Wargames: Here's a $24 Billion Fix," *Breaking Defense*, 7 March 2019.