FOREIGN AFFAIRS
Published by the Council on Foreign Relations

Monday, April 17, 2017 - 12:00am

Hack Job

How America Invented Cyberwar

Emily Parker

EMILY PARKER is a Future Tense Fellow at New America and the author of *Now I Know Who My Comrades Are: Voices From the Internet Underground*. [1]

Today's cyberbattles could almost make one nostalgic for the Cold War [2]. The nuclear arms race created a sense of existential threat, but at least it was clear who had the weapons. In contrast, a cyberattack could be the work of almost anyone. After hackers broke into [3] the U.S. Democratic National Committee's servers in 2016 and released e-mails embarrassing to the DNC's leadership, the Republican presidential candidate Donald Trump said the attacker [4] could be China, Russia, or "somebody sitting on their bed that weighs 400 pounds."

U.S. intelligence officials have said [5] that the attack did indeed come from Russia [6], which Trump later acknowledged [7]. But Trump's comment underscored a larger problem with cyberwarfare: uncertainty. How does a government respond to an invisible attacker, especially without clear rules of engagement? How can officials convince other governments and the public that they have fingered the right suspects? How can a state prevent cyberattacks when without attribution, the logic of deterrence—if you hit me, I'll hit you back—no longer applies? Two recent books delve into these questions. *Dark Territory*, by Fred Kaplan, and *The Hacked World Order*, by Adam Segal, lay out the history of cybersecurity in the United States and explain the dangers that future digital conflicts might pose. Both authors also make clear that although Americans and U.S. institutions increasingly feel themselves to be in the cross hairs of hackers and other cybercriminals, the United States is itself a powerful aggressor in cyberspace.

In the future, the United States must use its cyberpower judiciously. Every conflict poses the risk that one party will make a mistake or overreact, causing things to veer out of control. When it comes to cyberwar, however, the stakes are particularly high for the United States, as the country's technological sophistication makes it uniquely vulnerable to attack.

CYBER-SUPERPOWER

The dramatic headlines surrounding Russia's alleged hacking of the DNC and attempts to spread misinformation online during the U.S. election may have reinforced the perception among Americans that the United States is primarily a victim of cyber-intrusions. It's not. In *Dark Territory*, Kaplan details the United States' long history of aggression in cyberspace. It's not easy to write an engaging book on cyberwar, and Kaplan, a national security columnist at *Slate*, has done an admirable job. He presents a clear account of the United States' evolution into a formidable cyberpower, guiding the reader through a thicket of technical details and government acronyms.

It turns out that the U.S. government has been an aggressor for over a quarter century. Kaplan

describes “counter command-control warfare”—attempts to disrupt an enemy’s ability to control its forces—that goes back to the Gulf War [8] in 1990–91. At a time when U.S. President George H. W. Bush [9] had never used a computer, the National Security Agency (NSA) was employing a secret satellite to monitor the conversations of Iraqi President Saddam Hussein and his generals, which sometimes revealed the positions of Iraqi soldiers.

The United States flexed its digital muscles again in the late 1990s, when Serbs in Bosnia and Herzegovina were protesting the presence of NATO soldiers enforcing the 1995 Dayton peace agreement, which had ended the Bosnian war. U.S. officials learned that local newscasters were telling protesters when and where to gather and even instructing them to throw rocks at NATO soldiers. It turned out that 85 percent of Serbs got their television broadcasts from just five transmission towers. U.S. officials, working with the NATO-led stabilization force, or SFOR, installed devices on those five transmitters that allowed SFOR engineers to turn them on and off remotely. Whenever a newscaster began urging people to protest, the engineers shut off the transmitters.

American officials also enlisted the help of Hollywood producers, persuading them to supply programming to a U.S.-aligned Serbian station. During major anti-NATO protests, Serbians would turn on the television to find the channel playing episodes of *Baywatch*. Kaplan asserts, “Many Serbs, who might otherwise have hit the streets to make trouble, stayed in to watch young women cavorting in bikinis.”

Around a decade later, the United States set up what Kaplan calls a “mini-NSA” in Iraq. Kaplan describes how NSA teams in the Middle East intercepted insurgents’ e-mails and shut down many of their servers with malware. In other cases, they sent insurgents deceptive e-mails directing them to places where U.S. Special Forces would be waiting to kill them. “In 2007 alone, these sorts of operations . . . killed nearly four thousand Iraqi insurgents,” Kaplan writes.

The United States’ most ambitious cyberattack began in 2006, when it teamed up with Israel to sabotage the Iranian nuclear program. The collaboration, dubbed Operation Olympic Games, targeted Iran’s Natanz reactor, which relied on remote computer controls. Malware designed by American programmers took over the reactor’s valve pumps, allowing NSA operatives to remotely increase the flow of uranium gas into the centrifuges, which eventually burst. By early 2010, the operation had destroyed almost a quarter of Iran’s 8,700 centrifuges.

For years, the Iranians failed to detect the intrusion and must have wondered if the malfunctions were their own fault. In that sense, Kaplan writes, “Operation Olympic Games was a classic campaign of information warfare: the target wasn’t just the Iranians’ nuclear program but also the Iranians’ confidence—in their sensors, their equipment, and themselves.” The Iranians and the wider public might never have learned about the virus, now widely known as Stuxnet, if it had not accidentally spread from the computers in Natanz to machines in other parts of the world, where private-sector security researchers ultimately discovered it.

With Olympic Games, the United States “crossed the Rubicon,” in the words of the former CIA director Michael Hayden. Stuxnet was the first major piece of malware to do more than harm other computers and actually cause physical destruction. The irony was rich, as Kaplan notes: “For more than a decade, dozens of panels and commissions had warned that America’s critical infrastructure was vulnerable to a cyber attack—and now *America* was launching the first cyber attack on *another* nation’s critical infrastructure.”

Of course, cyberattackers have often targeted the United States. In 2014 alone, Kaplan reports, the country suffered more than 80,000 cybersecurity breaches, more than 2,000 of which led to data losses. He also points out that until recently, U.S. policymakers worried less about Russia than China, which was "engaging not just in espionage and battlefield preparation, but also in the theft of trade secrets, intellectual property, and cash."

China and Russia are not the only players. Iran and North Korea have also attacked the United States. In 2014, the businessman Sheldon Adelson criticized Iran, which responded by hacking into the servers of Adelson's Las Vegas Sands Corporation, doing $40 million worth of damage. That same year, hackers calling themselves the Guardians of Peace broke into Sony's network. They destroyed thousands of computers and hundreds of servers, exposed tens of thousands of Social Security numbers, and released embarrassing personal e-mails pilfered from the accounts of Sony executives. U.S. government officials blamed the North Korean government for the attack. Sony Pictures was about to release *The Interview*, a silly comedy about a plot to assassinate the North Korean ruler Kim Jong Un. As opening day neared, the hackers threatened theaters with retaliation if they screened the movie. When Sony canceled the release, the threats stopped.

EVERYBODY HACKS

The Hacked World Order covers some of the same ground as *Dark Territory*, although with a slightly wider lens. In addition to discussing cyberattacks and surveillance, Segal, a fellow at the Council on Foreign Relations, details how the United States and other countries use social media for political ends. Russia, for example, tries to shape online discourse by spreading false news and deploying trolls to post offensive or distracting comments. The Russian government has reportedly hired English speakers to praise President Vladimir Putin on the websites of foreign news outlets. The goal is not necessarily to endear Americans to Putin, Segal explains. Rather, it sows confusion online to "make reasonable, rational conversation impossible." Chinese Internet commenters also try to muddy the waters of online discussion. Segal claims that the Chinese government pays an estimated 250,000–300,000 people to support the official Communist Party agenda online.

Segal suggests that the United States will likely not win social media wars against countries such as China or Russia. U.S. State Department officials identify themselves on Facebook and Twitter, react slowly to news, and offer factual, rule-based commentary. Unfortunately, as Segal notes, "content that is shocking, conspiratorial, or false often crowds out the reasonable, rational, and measured."

Social media battles also play out in the Middle East. In 2012, the Israel Defense Forces and Hamas fought a war for public opinion using Facebook, Twitter, Google, Pinterest, and Tumblr at the same time as the two were exchanging physical fire. The Islamic State (also known as ISIS) has launched digital campaigns that incorporate, in Segal's words, "brutality and barbarism, packaged with sophisticated production techniques." The United States has tried to fight back by sharing negative stories about ISIS and, in 2014, even created a video, using footage released by the group, that featured severed heads and crucifixions. The video went viral, but analysts inside and outside the U.S. government criticized it for embracing extremist tactics similar to ISIS' own. Moreover, as Segal notes, it seems to have failed to deter ISIS' supporters.

Part of what makes the cyber-era so challenging for governments is that conflict isn't limited to states. Many actors, including individuals and small groups, can carry out attacks. In 2011, for example, the hacker collective Anonymous took down Sony's PlayStation Network, costing the company $171 million in repairs. Individuals can also disrupt traditional diplomacy, as when

WikiLeaks released thousands of State Department cables in 2010, revealing U.S. diplomats' candid and sometimes embarrassing assessments of their foreign counterparts.

Segal is at his best in his discussion of China's cyberstrategy, on which he has considerable expertise. Americans tend to see themselves as a target of Chinese hackers—and indeed they are. The problem is that China also sees itself as a victim and the United States as hypocritical. In June 2013, U.S. President Barack Obama warned Chinese President Xi Jinping that Chinese hacking could damage the U.S.-Chinese relationship. Later that month, journalists published documents provided by Edward Snowden, an NSA contractor, showing that the NSA had hacked Chinese universities and telecommunications companies. It didn't take long for Chinese state media to brand the United States as "the real hacking empire."

The U.S.-Chinese relationship also suffers from a more fundamental disagreement. U.S. policymakers seem to believe that it's acceptable to spy for political and military purposes but that China's theft of intellectual property crosses a line. The United States might spy on companies and trade negotiators all over the world, but it does so to protect its national interests, not to benefit specific U.S. companies. The Chinese don't see this distinction. As Segal explains:

The intense secrecy surrounding cyberwarfare makes deciding what kinds of hacking are acceptable and what behavior crosses the line even harder. The Snowden revelations may have alerted Americans to the extent of U.S. government surveillance, but the public still remains largely in the dark about digital conflict. Yet Americans have a lot at stake. The United States may be the world's strongest cyberpower, but it is also the most vulnerable. Segal writes:

FOREWARNED IS FOREARMED

Neither Kaplan nor Segal offers easy solutions to these challenges. Kaplan argues that the cyber-era is much murkier than the era of the Cold War. Officials find it difficult to trace attackers quickly and reliably, increasing the chances that the targeted country will make an error. The U.S. government and U.S. firms face cyberattacks every day, and there is no clear line between those that are merely a nuisance and those that pose a serious threat. The public also understands cyberthreats far less well than it does the threat of nuclear weapons. Much of the information is classified, inhibiting public discussion, Kaplan notes. He concludes that "we are all wandering in dark territory."

Segal's conclusions are somewhat more prescriptive. The United States must support research and technological innovation, for example, and not just by providing more federal funding. Segal recommends that the United States replace its federal research plan with a public-private partnership to bring in academic and commercial expertise. Government and private companies need to share more information, and companies need to talk more openly with one another about digital threats. The United States should also "develop a code of conduct that draws a clear line between its friends and allies and its potential adversaries." This would include limiting cyberattacks to military actions and narrowly targeted covert operations, following international law, rarely spying on friends, and working to strengthen international norms against economic espionage. If the United States is attacked, it should not necessarily launch a counterattack, Segal argues; rather, it should explore using sanctions or other tools. This was apparently the path that Obama took after the attack on the DNC, when the United States punished Moscow by imposing fresh sanctions and expelling 35 suspected Russian spies.

It's likely only a matter of time before the Trump administration faces a major cyberattack. When that happens, the government will need to react calmly, without jumping to conclusions. Failure to do so could have dire consequences. "The United States, Russia, and China are unlikely to

launch destructive attacks against each other unless they are already engaged in military conflict or perceive core interests as being threatened," Segal writes. "The greatest risks are misperception, miscalculation, and escalation."

Those risks now seem greater than ever. Some experts have argued that Obama's response to the Russian cyberattacks in 2016 did not do enough to deter future attackers. But if Obama underreacted, the United States may now face the opposite problem. Trump has proved willing to make bold, sometimes unsubstantiated accusations. This behavior is dangerous in any conflict, but in the fog of cyberwar, it could spell catastrophe.

Is there anything the American public can do to prevent this? All over the country, people have been trying to check Trump's worst impulses by protesting, appealing to members of Congress, or simply demanding more information. Policy about cyberspace generally doesn't draw the same level of public engagement, in part due to a lack of knowledge. Cyberbattles can seem confusing, technical, and shrouded in secrecy, perhaps better left to the experts. But cybersecurity is everyone's problem now. The American public should inform itself, and these two books are a good place to start. If Washington inadvertently led the United States into a major cyberwar, Americans would have the most to lose.

Links
[1] https://www.amazon.com/Now-Know-Who-Comrades-Are/dp/0374535515
[2] https://www.foreignaffairs.com/search?qs=Cold+War
[3] https://www.foreignaffairs.com/articles/russian-federation/2016-10-20/russias-october-surprise
[4] http://www.cnn.com/videos/politics/2016/09/26/mobile-clinton-trump-debate-400-pound-man-cyber-security-hofstra-sot-05.cnn
[5] https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf
[6] https://www.foreignaffairs.com/articles/russian-federation/2016-07-31/cyber-showdown
[7] http://www.cnn.com/2017/01/11/politics/donald-trump-press-conference-highlights/
[8] https://www.foreignaffairs.com/reviews/capsule-review/1992-12-01/after-storm-lessons-gulf-war
[9] https://www.foreignaffairs.com/topics/ghw-bush-administration