Cybersurveillance and the New Frontier of Deterrence

SUSAN LANDAU

From Paul Revere's legendary ride in 1775 to warn the American colonists in Massachusetts after he spotted the approach of British troops, to the success of codebreakers in cracking the German Enigma codes during World War II, which enabled Allied convoys to reach Britain, the value of intelligence in warfare cannot be overstated. As the Chinese general and strategist Sun Tzu wrote over two millennia ago, "Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge."

But if intelligence and surveillance win wars, they also help prevent them. During the Cold War, for example, US surveillance satellites disclosed what armaments the other side possessed. By eliminating guesswork, the information helped serve as a deterrent to war. In 1967, President Lyndon Johnson noted, "We've spent between thirty-five and forty billion dollars on space . . . but if nothing else had come from that program except the knowledge that we get from our satellite photography, it would be worth ten times to us what the whole program has cost. Because tonight I know how many missiles the enemy has and . . . our guesses were way off. And we were doing things that we didn't need to do. We were building things that we didn't need to build. We were harboring fears that we didn't need to have."

Recently, much has been written about cyberexploits—the theft of electronic data through computer networks. Such thefts typically involve copying data to a site of the hacker's choice while usually leaving the original data at its initial site. (Tampering with the original data is a cyberattack, not a cyberexploit.) This includes China's cyberexploits from US systems, which have been characterized as the greatest theft of intellectual property in human history, as well as successful efforts by Russian and Eastern European criminal groups to steal customer data. It also includes the vast surveillance capabilities of the so-called Five Eyes—the United States and four of its closest allies: Britain, Canada, Australia, and New Zealand. Here I would like to focus on a different consequence of US surveillance: its effectiveness in deterring cyberexploits and cyberattacks.

As we all know, the Internet can be a dangerous tool. The announcement by US officials in December 2014 that North Korea was responsible for a cyberattack on Sony Pictures Entertainment made it a little bit safer. The episode warrants a closer look for its lessons on deterrence in the cyber age.

Sony had produced a movie, *The Interview*, mocking North Korean leader Kim Jong-un—it was a comedy about an assassination plot against him—and planned to release it over the Christmas holidays. North Korea fumed and blustered, but to little effect. Then the situation turned serious, with less talk and more action. Hackers threatened to delete data on Sony servers and publicly release confidential information, including emails and personnel records, that they had lifted from those servers. When there was no response from the company, the hackers carried out their threats. Warned of possible violence in theaters if the movie was released, Sony halted distribution. Then the company was convinced to go ahead with releasing the film after all—but despite the publicity, it was not a critical success.

What was intriguing was the US government's response. The White House characterized the cyberattack and theft of information as a "serious national security matter." Given that Sony is a media company that produces music and movies, calling it a "serious national security matter" was somewhat over the top. But hidden behind that characterization are two very interesting questions. How did US officials know for certain that North Korea was behind the attack? And why did the government openly say so?

SUSAN LANDAU *is a professor of social science and policy studies at Worcester Polytechnic Institute.*

At the time of the attack, many experts did not believe that the White House had evidence to back its accusation. There is a common perception that the Internet makes it easy for users to preserve their anonymity—or as a famous *New Yorker* cartoon, showing a dog sitting at a computer, put it two decades ago, "On the Internet, nobody knows you're a dog."

But in fact, if you do not work hard to hide your identity online, attribution is typically easy—even if the only personal information explicitly revealed on a Web connection is an Internet Protocol address, the number assigned to each device on the network. Internet advertisers have certainly figured this out. They are able to determine not only that you are a dog but whether you are a poodle or a pug, where your owner lives, and how often she takes you to the park.

DARK CORNERS

In other situations, however, attribution can be extremely challenging. Sometimes users deliberately seek to hide their identity. There are legitimate reasons for this—for example, evading censorship, or conducting journalistic or business investigations—and illegitimate ones, including cyberexploits.

US surveillance of the Internet is a deterrent to cyberattacks by nation-states.

When data is stolen, whether by cybercriminals lifting credit card numbers and other personal information, or by government spies, the thieves typically hide their tracks by downloading stolen files into a "cascade" of computers. They accomplish this by corrupting the machines. The problem starts when machine A infiltrates compromised machine B using an unpatched vulnerability. Then machine B does the same to unpatched machine C, machine C to unpatched machine D, and so on. Eventually machine G infiltrates and steals data from a target, then sends the stolen data to machine F, which forwards it to E. The data eventually gets back to A. Two issues are key to the data thief's anonymity. Stolen data may reside only briefly on intermediate machines. And if the jurisdiction in which machine F—or machine E or D—does not immediately open an investigation to track the stolen data, determining who really took the files becomes extremely difficult.

There are many dark corners of the globe where such investigations are either slow to begin or don't occur at all. Criminals and nation-states launder their cyberexploits through these venues, complicating the task of identifying them.

North Korea is one such dark corner. That's why many computer experts initially distrusted the Federal Bureau of Investigation's announcement fingering North Korea in the Sony cyberattack. In fact, there was evidence to support the claim. Ironically, it was in Edward Snowden's disclosures about the global scope of Internet surveillance by the US National Security Agency (NSA). Leaked NSA memos revealed that US intelligence operatives had gained access to North Korean computer networks, which enabled US authorities to conclusively determine that North Korea was behind the Sony infiltration and attack. That revelation, in January 2015, convinced the doubters.

Of course, attacking a media company hardly constitutes a national security threat. The United States issued largely symbolic sanctions against North Korea. It appears that, rhetoric aside, Washington agrees that the Sony attack was not a national security threat. So why did US officials reveal that they knew North Korea was behind the attack? It was an exercise in misdirection worthy of a John le Carré novel.

NAMING NAMES

Isolated, with few networks, North Korea has not shown strong capability to wreak electronic havoc on the United States. Although North Korea has repeatedly attacked South Korean firms and infrastructure, it has not attacked US infrastructure, or US companies supporting critical infrastructure (such as banks). Yet the United States was nonetheless peering deeply into North Korea's computer networks. The purpose behind publicly blaming North Korea for the Sony attacks was not to send a signal to North Korea. The United States wanted to send an unmistakable message to other nations: Do something bad on the Internet and you won't be able to hide from the US government.

In much the same way that US satellites and high-altitude surveillance flights have been a force for deterrence, so is US surveillance of the Internet a deterrent to cyberattacks by nation-states. The announcement about North Korea's involvement

is likely to resonate more loudly than the recent US indictments of hackers believed to be working for the Chinese military. We knew, of course, that US intelligence agencies are always watching China. The Sony incident sent the message that they are always watching everywhere they can. The fast response to the North Korean hacks showed that some cyberattacks on the United States will be quickly tracked. That undoubtedly was the rationale for going public about the source of the attack.

The NSA can't watch everywhere—there is too much data. The agency has to be selective in what it collects and what it looks at. North Korea is important because of its nuclear weapons program; that effort is a major target of NSA surveillance. North Korea's nuclear program, however, is largely unconnected to the Internet. Despite that, the NSA was watching. The Sony episode showed that the NSA was watching in places we hadn't necessarily expected.

US cybersurveillance will not prevent Internet crime or cyberexploits against the government or corporations. But cybersurveillance, combined with the government's willingness to disclose its capabilities, has changed the equation for nations seeking to conduct cyberattacks against US interests. With the Sony incident, the US government put the world on notice: Anonymous attackers are unlikely to remain anonymous.

Identification—the capability to know "whodunnit"—is merely a first step to deterrence. Much more remains to be done in order to secure US cyber infrastructure. However, putting perpetrators of bad actions on notice that they won't remain hidden is essential.

In emphasizing the importance of the deterrence that US cybersurveillance provides, I am in no way seeking to diminish the infringements of privacy and civil liberties that such surveillance entails. While US laws and regulations in large part protect American persons (citizens, residents, and US corporations), citizens of other nations are typically not afforded similar protections, either by their own governments or by the United States. We must find ways to protect their fundamental human rights.

Nonetheless, the fact that NSA cybersurveillance has been excessive, irresponsible, or of questionable legality—or some combination of all three—should not cause us to ignore the fact that it has increased our ability to deter cyberattacks. And that is a good thing for security and privacy, both domestically and abroad. ■