foreignaffairs.com

Why the U.S. Should Switch from Cyber-Deterrence to Playing Cyber-Offense

By Michael Sulmeyer

9-12 minutes

The United States has been the victim of repeated cyberattacks by foreign powers, and it seems to have little power to stop them. During the 2016 U.S. presidential campaign, Russian hackers broke into the Democratic National Committee's e-mail servers and made more general efforts to influence the election's outcome, as detailed in Special Counsel Robert Mueller's indictment of 13 Russians and three Russian entities. In February, U.S. intelligence and law enforcement officials warned that the Russian government would again try to use cyber-operations to interfere with midterm elections in November. That same month, the White House publicly blamed Russia for "the most destructive and costly cyberattack in history," the 2017 NotPetya malware campaign, which crippled the government of Ukraine before spreading to multinational corporations such as FedEx and Maersk, causing billions in damage.

The Russians are not the only ones hacking at the United States' expense. Chinese hacking groups have stolen U.S. intellectual property from industrial manufacturers and military contractors. In 2015, China weaponized its "Great Firewall" and conducted distributed denial of service attacks against U.S. websites, including GitHub, which Beijing wished to punish for hosting content that the Chinese leadership found undesirable. In 2014, North Korean hackers attacked the U.S. film studio Sony Pictures to block the release of a movie, *The Interview,* that depicted the attempted assassination of North Korean leader Kim Jong Un. The attack erased the content of thousands of computers, released embarrassing internal e-mails, and intimidated Sony into canceling the movie's theatrical release. Iran too has lashed out in cyberspace, attacking U.S. financial institutions and a dam in New York.

These threats have led to renewed calls for cyber-deterrence measures that would impose greater costs on would-be hackers while denying them benefits. The administration of President Donald Trump, for instance, has elevated U.S. Cyber Command to a unified combatant command, which it believes will signal greater capability and resolve. Deterrence is also likely behind the Trump administration's broad declaratory policy in its Nuclear Posture Review, which contemplates the use of nuclear weapons to deter non-nuclear threats. Former President Barack Obama prioritized cyber-deterrence as well, including in his administration's 2015 Department of Defense Cyber Strategy and in his Justice

Department's efforts to indict Chinese and Iranian hackers. In cyberwarfare, Washington should recognize that the best defense is a good offense.

This focus on cyber-deterrence is understandable but misplaced. Deterrence aims to change the calculations of adversaries by persuading them that the risks of an attack outweigh the rewards or that they will be denied the benefits they seek. But in seeking merely to deter enemies, the United States finds itself constantly on the back foot. Instead, the United States should be pursuing a more active cyberpolicy, one aimed not at deterring enemies but at disrupting their capabilities. In cyberwarfare, Washington should recognize that the best defense is a good offense.

THE PROBLEMS WITH DETERRENCE

There are three main problems with U.S. efforts at cyber-deterrence. The first is that Washington is trying to use a cold war strategy to address a twenty-first-century problem. History teaches that deterrence kept the Cold War cold: the United States and the Soviet Union were each vulnerable to the other's thousands of nuclear weapons. When it comes to cyberspace, however, the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security. But although the societies and infrastructure of Washington's adversaries are less connected and vulnerable than those of the United States, their methods of hacking can still be disrupted.

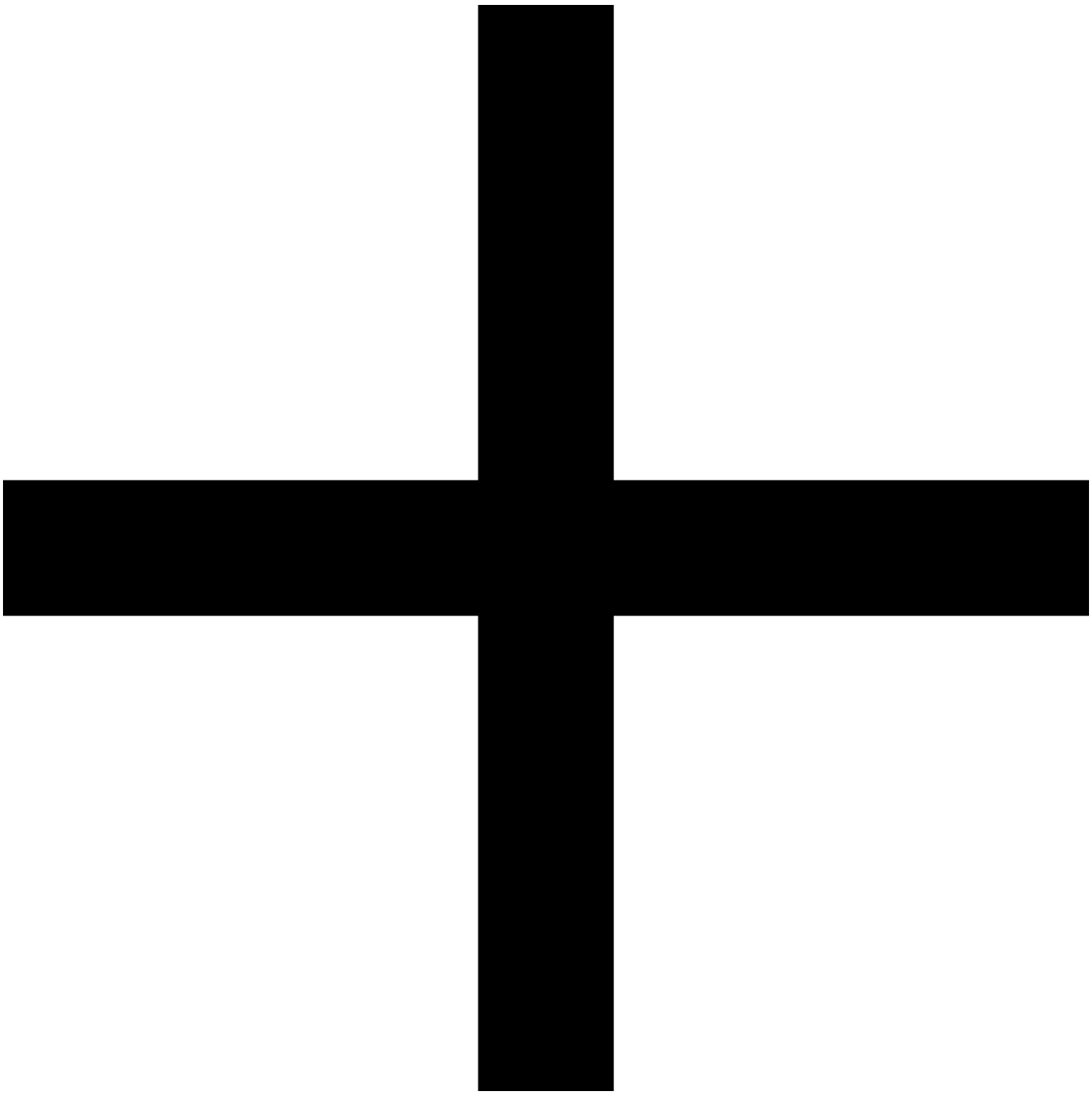
Second, it is difficult to convince foreign leaders (and foreign hackers) that the costs of hacking really do outweigh the benefits. Deterrence is all about perception: does an actor believe that the threat of punishment is real enough to prevent him from acting? This is as much a question of psychology as one of national security strategy. Many U.S. adversaries are less vulnerable in cyberspace than the United States is, so meaningful punishment would require discerning their priorities (for instance, money or public reputation) and threatening concerted action against them. Yet gaining clarity about foreign leaders' priorities—and credibly threatening them—is easier said than done: during the Cold War, Soviet leaders often misunderstood signals from their U.S. counterparts, as when they interpreted the NATO military exercise Able Archer 83 as a prelude to war. Not much has changed—National Security Agency Director Admiral Michael Rogers acknowledged during a recent hearing that the Russians "haven't paid a price . . . that's sufficient to get them to change their behavior."

Third, it is virtually impossible to know if deterrence is working. The goal is to prevent attacks. But if no attacks occur, it is hard to determine why—perhaps the would-be attacker was deterred by the threat of punishment; perhaps the attack failed for some other reason. Washington should not base its national cyberpolicy on a strategy whose success, almost by definition, cannot be evaluated, especially if there are good alternatives available.

Today's fight in cyberspace occurs in the gray zone between war and peace. If the United States hopes to win, it should spend less time trying to persuade its competitors that it is not worth hacking and more time preempting them and degrading their ability to do so. It is time to target capabilities, not calculations.

Yuri Gripas / Reuters

A Department of Justice staffer stands near a wanted poster of a Russian hacker in Washington, D.C., March 2017.



HACK THE HACKER

How could the United States begin degrading its opponents' ability to hack? Washington's actions need not always be aggressive or destructive. In countries where technology companies are willing to cooperate with the U.S. government (or with requests from their own government), a phone call to the right cloud provider or Internet service provider (ISP) could result in getting bad actors kicked off the Internet. This is not a permanent solution, but it will force adversaries to rebuild,

which often prompts unforced errors, making them more vulnerable to U.S. surveillance and disruption.

If subtle measures prove insufficient, the United States should be ready to take more offensive action. In situations where the defense of the nation is on the line, U.S. hackers could pursue a campaign of erasing computers at scale, disabling accounts and credentials used by hackers to attack, and cutting off access to services so it is harder to compromise innocent systems to conduct their attacks. Such a campaign would aim to make every aspect of hacking much harder: because hackers often reuse computers, accounts, and infrastructure, targeting these would sabotage their capabilities or render them otherwise useless.

Such actions need not send a message that hacking the United States doesn't pay. Instead, they should support a more limited but more achievable objective: stop adversaries from hacking the United States. Whether or not foreign leaders perceive that cyberattacks on the United States are worth conducting, Washington can prevent them from doing so in the first place.

Offensive cyber-operations should not be undertaken lightly—the United States must bear in mind its commitments under international law and its relationships with its allies. But excessive caution cannot prevent Washington from defending itself: with the United States' enemies already attacking it online, the country will need to be more proactive than it has

been thus far.

The U.S. government has already undertaken a few asymmetric, or non-cyber, approaches to degrading its adversaries' abilities to hack targets in the United States. It has sanctioned foreign individuals and companies to limit their access to capital and resources. It has also indicted some hackers from China, Iran, and Russia in the hope that public exposure will make it more difficult for them to hack. These are efforts worth pursuing, but not because they deter. Rather, like offensive cyber-operations, they can degrade attackers' capabilities, although only in indirect ways because they rely on the cooperation of foreign governments. Today's fight in cyberspace occurs in the gray zone between war and peace.

DEFENSE AT SCALE

Even as it seeks to upgrade its offensive cyber-capabilities, the United States should also be improving its defense. Best practices for cybersecurity, such as more secure methods to authenticate users, are increasingly well-known and easy to implement. The issue today is how to improve cyberdefenses at scale. The only way to do so is for the government to work with large technology companies to implement security enhancements for everyday Internet use. Examples include rolling out secure connections to websites, known as "https" (as opposed to the unencrypted "http"), for everyone and increasing the use of physical security tokens to improve the security of user credentials. Companies that offer these

services need not force every customer to use them, but making greater security the default and allowing users to opt out rather than opt in would go a long way toward increasing protection.