Science & Technology

The Age of Cyberwarfare

With the Internet now a global battlefield, how serious a threat do cyberweapons pose to America’s economy and infrastructure?

By
David J. Craig
|
Summer 2019

Pete Ryan (homage to Antonio Prohías)

Jason Healey, a senior research scholar at the School of International and Public Affairs, is a leading authority on cyberattacks. *Columbia Magazine* interviewed the former intelligence officer about his work.

Can you give us an overview of your research?

I’m interested in the ways that nations are competing in cyberspace and how cyberattacks are changing the very nature of geopolitical conflict. As financial institutions, utilities, transportation systems, government agencies, and military commands all become increasingly wired, countries are putting more and more energy into identifying and exploiting vulnerabilities in their enemies’ networks. Cyberattacks are now a primary means for nations to project their power. They can involve sabotage of critical infrastructure, espionage, election tampering, and all manner of intellectual-property theft, economic disruption, and political destabilization.

Which countries are most active in this realm?

Our main adversaries in cyberspace are Russia, China, North Korea, Iran, and, to a lesser degree, terrorists. The United States is also very active. Most people are surprised to learn that we possess the most powerful offensive cybercapabilities and online espionage tools in the world and that we employ them quite aggressively. In fact, the first cyberattack to cause serious material damage was perpetrated by the United States and Israel. In the early 2000s, they developed a sophisticated computer worm called Stuxnet that infiltrated the Iranian nuclear facility at Natanz and instructed its centrifuges to spin out of control, destroying perhaps a thousand of them.

Do countries have specific strategies when it comes to cyberattacks?

Absolutely they do, based on their different geopolitical and domestic priorities. Under Putin’s regime, Russia has launched some major attacks to cause political turmoil in other countries. These attacks can blur the distinction between espionage and cybercrime. Between 2014 and 2016, Russia’s intelligence agency, the FSB, supported criminals who hacked into some five hundred million Yahoo e-mail accounts; the hackers were allowed to keep credit-card numbers they amassed in exchange for handing over the private data of journalists and politicians. Russia’s interference into the 2016 US presidential election was revolutionary, in that it combined a hacking operation — into the Democratic party’s e-mails — with a very Soviet-style disinformation and propaganda campaign.

China, by contrast, has focused on stealing the intellectual property of Western companies. This has allowed it to copy advanced weapons systems, create high-tech products like wind turbines without having to spend on research and development,

and even steal the negotiating and legal strategies of businesses bidding against Chinese companies or seeking to operate in China.

Meanwhile, North Korea, in order to raise hard currency, has been breathtakingly creative and aggressive. It almost succeeded in stealing a billion dollars from the central bank of Bangladesh and has undertaken disruptive ransomware attacks, hijacking companies' data and releasing it for a fee. The worst of these attacks, the so-called WannaCry ransomware attack of 2017, shut down hundreds of thousands of computers in 150 countries. The chaos that ensued illustrates how dependent we've become on computers: hospitals had to cancel surgeries and turn away ambulances, and factories ground to a halt.

How big a problem is cybercrime and cyberwarfare?

It's been estimated that malicious cyberactivity costs the global economy some $600 billion annually and the US economy upwards of $175 billion a year. The US is the top victim of cyberattacks in part because we are so dependent on the Internet, which makes us more vulnerable.

For years, cybersecurity experts have been warning that America's power grid is susceptible to attack. Is that a serious concern?

I have little doubt that our enemies are capable of taking down sizable portions of our power grid. We know this, in part, because we're capable of doing it to other countries and because we've detected Russian and Chinese hackers poking around inside our systems and planting malicious code. What's less clear is how large a section of our grid could be taken down and for how long. Potentially, entire regions of the US could lose power for weeks or even longer.

It's worth noting, though, that we've been worried about such a catastrophic attack for decades. The main reason it hasn't happened yet is that other countries know it's a red line they can't cross. I mean, if China were to shut off electricity across California, we'd be at war.

Terrorist groups could be more brazen. Are they capable of doing such a thing?

Not yet. But we're lowering the bar by connecting more and more of our infrastructure to the Internet. Now that our power plants, pipelines, dams, railroads,

factories, and bridges are all controlled and monitored online, we’re creating a situation where relatively unsophisticated groups have a greater chance of scoring a knockout punch.

How can we defend ourselves?

Our cyberdefenses have gotten better in recent years. For example, we’ve dramatically improved our ability to identify the perpetrators behind cyberattacks, which has a deterrent effect. The problem is that while the defenders tasked with keeping our institutions safe are getting better, the attackers are improving at an even faster pace, and staying several steps ahead. Every year, the situation gets worse. The Internet is expanding, and our electronic devices are becoming more complex, which means they contain more lines of computer code and hence more potential vulnerabilities. We’re creating unlocked digital windows into our lives, and the hackers will take advantage of that.

Jason Healey (Courtesy of SIPA / Michael DiVito)

Is there anything the US government should be doing differently?

I think the United States has been overly focused on developing and using its offensive cybercapabilities and online espionage tools at the expense of shoring up our defenses. What's more, our aggressive use of cyberweapons has had a blowback effect, inspiring enemies to plow more money into their own cyberwarfare programs and to launch attacks against us. Just look at how Iran responded to the Stuxnet sabotage of its nuclear facility. Until that time, the Iranians were focused almost exclusively on using their cybercapabilities to monitor and oppress their own citizens. But after we threw the first punch, they began harassing US financial institutions, launching attacks that flooded companies' websites in order to crash

them.

Another US cyberinitiative that's come back to haunt us is the NSA's online spying operation that was revealed by Edward Snowden's leaks in 2013. That program was massive in scale and sent a pretty loud message to the international community that the US considers routine hacking of other countries' networks acceptable behavior. We ignored other countries' complaints — saying, "It's just spying" — until those techniques were turned against us. After the Chinese stole millions of federal personnel files from the Office of Personnel Management in 2014 and 2015, we started crying about how this kind of online espionage crossed a line.

The prevailing attitude in US military and intelligence circles today is that it is imperative to dominate our enemies in cyberspace. Now, I don't think that's self-evident. In fact, one of the questions I ask in my research is: What are the unintended consequences of treating the Internet like one big battlefield?

What's the downside of doing that?

You have to consider that the Internet is the most extraordinary human invention since the printing press. It's been a force for remarkable progress, freedom, and prosperity. Shouldn't we treat it as a precious resource and try to sustain it for future generations? Yet the US government is actively involved in militarizing the Internet. Everyone is peeing in the pool, and I think that we may come to regret this. Our whole economy depends on having a free, open, and safe Internet, after all. I say aim for prosperity and defense first.

Given your background, you're certainly uniquely qualified to talk about the militarization of the Internet.

Yes, in the late 1990s I was an intelligence officer in the US Air Force, and I helped to establish the military's first-ever cyberwar-fighting command. Our mission was to defend the Department of Defense against cyberattacks and, later, coordinate offensive attacks. I then served as director of cyberinfrastructure protection at the White House from 2003 to 2005, coordinating the federal government's efforts to secure US cyberspace and critical infrastructure in both the public and private sectors.

How should the US shore up its cyberdefenses?

The government should be doing more to enable and encourage big tech companies like Google, Microsoft, and Apple to come up with industry-wide solutions, because they have the expertise to fix things at scale. I recently coauthored a report on the major cybersecurity improvements made in the US private sector over the past few years, and we found that the vast majority aimed to address vulnerabilities at the level of individual computers or companies. These measures provide some protection but typically end up being bypassed by savvy attackers. What we need instead is for companies that can work at scale to secure billions of computers at a time. If necessary, we may even have to consider government regulations to require them to take such steps.

What can ordinary people do to protect themselves from cybercrime?

First, keep your computer and phone fully updated. Vendors are pretty good about sending security patches, so don't leave yourself open by putting off these updates. Also, definitely use a password manager. I use LastPass, which generates long, complex passwords for all of my online accounts and remembers them for me. You'll only have to log into one app to access them all. That might not strike some people as a good idea, but it's what we pros rely on.

Also, save your data in the cloud. The big technology companies that offer cloud services are much better at security than you'll ever be. I never worry about the data on my computer because there's almost literally nothing saved there.

How are you preparing students for jobs in cybersecurity?

At SIPA, we've expanded our curriculum in recent years, creating new courses in subjects like cyberrisk in business and cyberthreat intelligence analysis. We offer a half dozen cyber-related courses, and they're always full. My favorite class is one that I teach with professors from Columbia Law School and the Department of Computer Science. We take eight students from each area and put them together into teams so that everyone can learn from the unique perspectives of the other disciplines. Overall, our focus at SIPA is giving students the practical skills they'll need to develop policies that help government agencies, corporations, or other employers protect themselves against cyberattacks. Our graduates are well-versed in the technical aspects of the threats but also understand the international forces driving attacks. When new threats are looming, they're able to write crisp and intelligible policy recommendations that non-specialists can understand. It's a

popular area for students now because it’s intellectually challenging, and we help connect them to the many good jobs in the field.

What are you working on right now?

Currently, I’m studying a new US military strategy that calls for our spies to mirror the movements of enemy hackers, even if that entails following them into the computer networks of our allies. What results is a sort of digital cat-and-mouse game, where our spies and those of our enemies are constantly looking for signs of one another while trying to remain hidden, sort of like two gangsters hunting for each other in a dark warehouse. The Pentagon officials behind the program say that it will enable them to detect and scuttle impending cyberattacks before they occur. I’m watching to see if it works. I think it’s possible that it will. But the strategy comes with serious risks, because whenever you engage an adversary, there’s a chance that one side will misread the other’s activities as being more threatening than they really are, which can escalate tension.

What do our allies think of this program?

They don’t like it, because we’re doing it without their permission! The whole thing raises profound questions about how we define sovereignty in cyberspace, questions that we’re likely to be grappling with for the next hundred years.

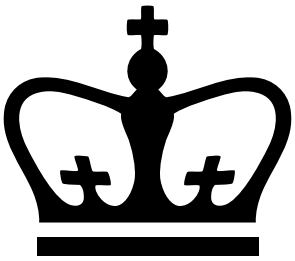
Is there any momentum to limit the use of cyberweapons?

There have been some fledgling attempts by the UN, but the proposals haven’t gained much traction. The US has generally hindered these efforts, because we don’t want any restrictions on how we act in cyberspace.

When it comes to cyberattacks, what frightens you the most?

It’s not a major attack on our physical infrastructure. I worry more about another attack like Russia’s theft of the Democratic National Committee’s e-mails in 2016. Imagine this scenario: the US economy is in crisis and Federal Reserve officials are holding private discussions to figure out how to prevent a crash. Imagine if someone hacked into the Fed’s servers and released the e-mails. Now there’s widespread panic and we’re in a recession that would not have occurred otherwise. Something like that is bound to happen sooner or later.

Read more from
David J. Craig



Guide to school abbreviations

All categories >

Read more from

David J. Craig