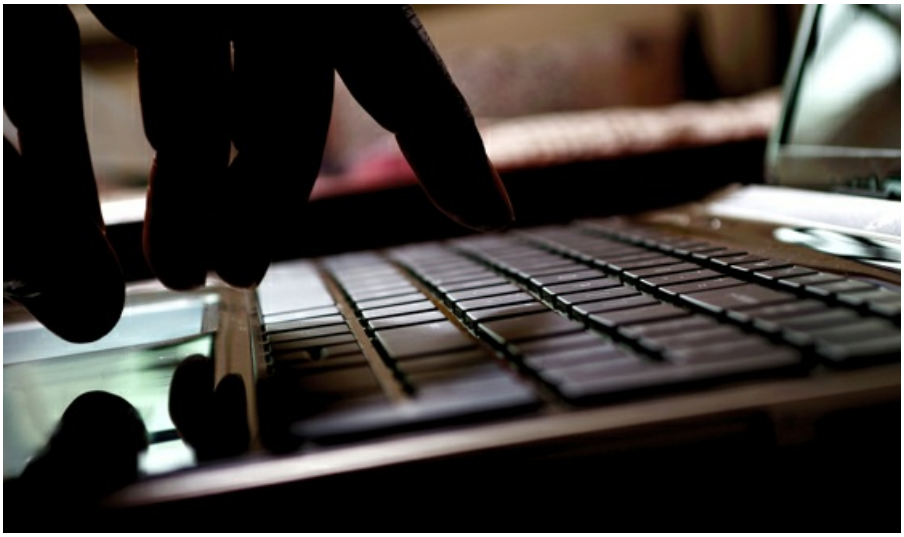
deTrompet



ISTOCK.COM/JAMINWELL

Cyberwarfare Is Worse Than Ever

- Richard Palmer
- 09-02-2018

America is vulnerable to cyberattacks. You're probably not surprised by that. But you may be surprised by just *how* vulnerable. In 2017, nearly twice the number of cybercrimes in America were reported compared to the year before. From 2015 to 2016, the number of ransomware attacks (in which hackers hold a victim's data to ransom) increased not by 100 percent, 200 percent or 300 percent—but by 16,700 percent, according to one estimate.

This may be termed "cybercrime," but it is often not only shady criminals behind these attacks but foreign governments.

Defense expert Peter W. Singer reviewed this growing threat in an article titled "The 2018 State of the Digital Union: The Seven Deadly Sins of Cyber Security We Must Face ," published January 30 on War on the Rocks. The danger of cyberattacks has become dramatically worse over the last few years. It's a story that too few are familiar with.

Here's a summary of some of his most important points:

An Explosion of Attacks

Last year was the most expensive year ever for cyberattacks. FedEx is just one the most well-known of many companies to lose hundreds of millions of dollars. And it is not just the number of attacks that has increased, it is also the danger. Singer wrote that there has been an explosion in numbers of "mega-breaches"—cyberattacks where at least 10 million identities are exposed. In 2012, there was just one of these breaches. Now they are so common we pay them little attention.

"For example, many recall the Target breach of five years ago that affected 41 million Americans," wrote Singer. "But few even noticed the 2017 loss of nearly 200 million Americans' voter data (names, date of birth, address, phone numbers, voter registration details) by Deep Root Analytics, a marketing firm that works for the Republican National Committee."

With more and more of this data in the open, hostile individuals or governments can combine the leaked data and build a huge store of knowledge about millions of Americans.

'The Collapse of Deterrence'

America has come under repeated attack from foreign nations. Russia has targeted both the Democratic and Republican national committees. Foreign nations have also targeted government institutions and crucial private networks, such as those in the finance industry. America's response?

Nothing.

"The failure to clearly respond has taught not just Russia, but any other would-be attacker, that such operations are relatively no pain on the cost side, and all gain on the benefits side," wrote Singer. "Until this calculus is altered, the United States should expect to see not just Russia continue to target its citizens and institutions … but also other nations and non-state groups looking for similar gains."

The Ukrainian Testing Ground

Ukraine has seen some of the worst cyberattacks in recent years. On Dec. 23, 2015, hackers shut down power to 80,000 homes for six hours. The next year they struck again, with a far more sophisticated attack. Singer explained that these attacks should be of great concern far beyond Ukraine:

Russia has treated Ukraine as a kind of battle lab for all sorts of new cyberthreats and tactics. Think of it as a digitized version of how the Spanish civil war in 1930s was used by the Germans not just to hone the technology of the Blitzkrieg, but to learn just what the world would let them get away with. Most worrisome has been a series of Russian attacks on civilian power grids , the type of attacks that have long been the nightmare scenario of cybersecurity, but here again with no consequence. This has been accompanied by probing attacks on previously off-limits areas in critical infrastructure, such as into nuclear plants in both the United States and Europe.

The leader of a team investigating the attacks against Ukraine said that when the perpetrator of those hacks "finally nails Western critical infrastructure, and folks react like this was a huge surprise, I'm gonna lose it."

The 'Internet of Things'

Cyberattacks could be about to get worse because more "stuff" keeps going online. An estimated 9 billion devices are online now, and this could double, triple or more over the next five years. New smart cars, televisions, thermostats, power plants and other real-world objects are being manufactured with Internet connectivity, which means there are more and more things to attack. The security of these devices is often terrible. *Most* of these Internet-enabled devices have known security flaws.

This new connectedness could mean hackers can start causing more *physical* damage with *cyber*attacks. These kind of attacks "will cost not just future money, but lives," wrote Singer.

Reliance on Foreigners

For all these smart devices, whether in the home, in a power station or in the military, America relies on foreign nations to make the key components. "Never before has a nation been in geostrategic competition with another nation that manufactures substantial parts of both its business and military technology," wrote Singer. "This is the predicament for the United States, which finds itself beholden to China, all the way down to the microchip level. It creates not just a type of dependence never before seen, but also one that can be exploited through the potential of 'hardware hacks ,' where vulnerabilities might be baked into systems in a manner that might not be made evident for years if not decades. The chips that you buy today, could cost you a war tomorrow ."

America's Achilles' Heel

"America is the greatest superpower this world has ever known," wrote editor in chief Gerald Flurry in "America's Achilles' Heel" in the January 1995 *Trumpet* issue. "But we have a very vulnerable point in our military—our own Achilles' heel. It is so dangerous that I am amazed it hasn't received more publicity."

He quoted defense analyst Joseph de Courcy, who wrote, "Computer dependence is the Western world's Achilles' heel, and within a few years this weakness could be tested to the full."

If anything, that weakness is even worse today. And still it receives little publicity.

Mr. Flurry wrote that de Courcy's warning immediately reminded him of Ezekiel 7:14: "They have blown the trumpet, even to make all ready; but none goeth to the battle: for my wrath is upon all the multitude thereof."

"It seems everybody is expecting our people to go into battle, but the greatest tragedy imaginable occurs!" Mr. Flurry wrote. "Nobody goes to battle—even though the trumpet is blown! Will it be because of a computer terrorist?"

In his article, Mr. Flurry drew special attention to Germany. In April last year, Germany launched a massive new Cyber and Information Space Command . When it reaches its full strength of 13,500, it will include nearly as many personnel as the German Navy. And it's working on conducting offensive cyberattacks.

The picture painted by Mr. Flurry in his 1995 article is now more plausible than ever.

America's cybervulnerabilities exist for an important reason. Mr. Flurry wrote:

One of the main reasons we won World Warii was because the British broke the German radio code. We knew about most of their war plans in advance! Quite a gigantic advantage.

I believe the code breaking was a miracle from God to help us win the war. But we arrogantly refuse to give God credit for the many miracles that saved us in World War ii.

God had a hand in Britain's and America's history, and He has a hand in the events today. "The overall reason this crisis occurred was because God's 'wrath is upon all the multitude thereof,'" wrote Mr. Flurry. "Will one of God's curses come upon us in the form of computer terrorism? We are not receiving God's blessings. We are being cursed (Leviticus 26; Deuteronomy 28)."

In Ezekiel 7:9 God says He is behind these curses so "ye shall know that I am the Lord that smiteth."

There will be terrible consequences because of this terrible weakness. But it is all part of God's plan to have Israel and the world get to know Him.

For more on this vulnerability, read our Trends article "Why the *Trumpet* Watches America's Cybervulnerabilities." ▪