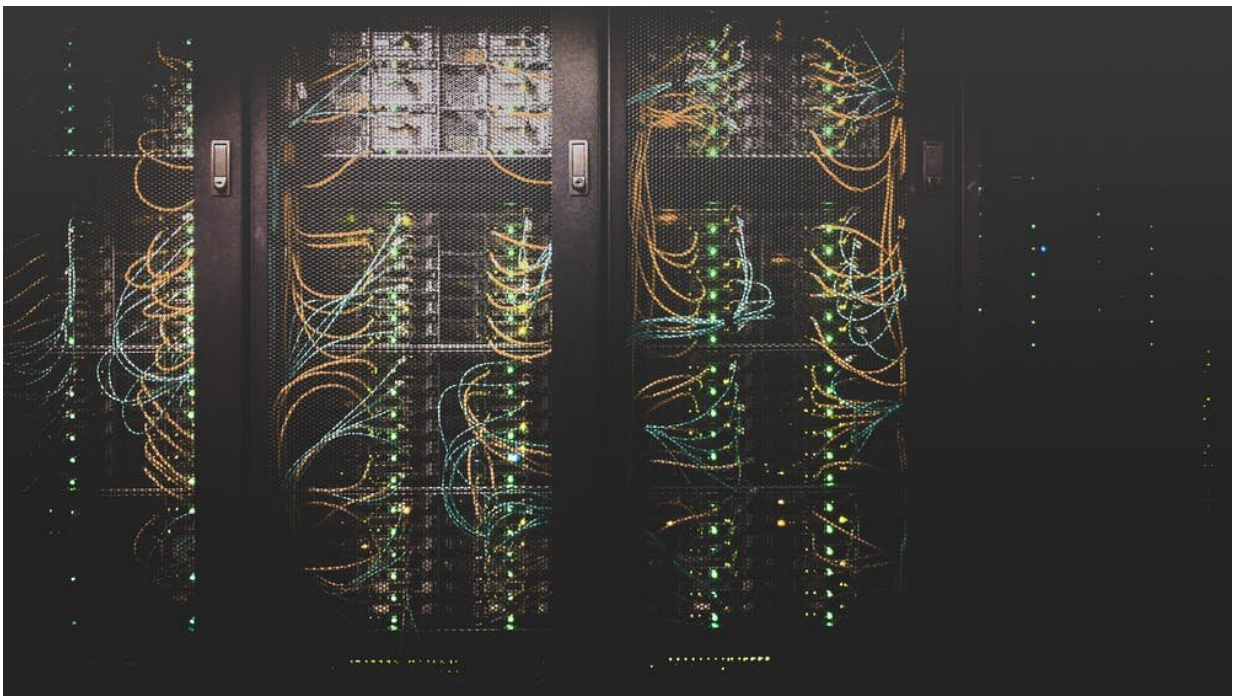
Cyberspace is the next front in Iran-US conflict – and private companies may bear the brunt

January 13 2020, by Bryan Cunningham



Front lines in an Iran-U.S. cyberwar are spread out all over the country. Credit: Taylor Vick/Unsplash, CC BY

Iran and other nations have waged a stealth cyberwar against the United States for at least the past decade, largely targeting not the government itself but, rather, critical infrastructure companies. This threat to the

private sector will get much worse before it gets better and businesses need to be prepared to deal with it.

As in the days of pirates and privateers, much of our nation's critical infrastucture is controlled by private companies and enemy nations and their proxies are targeting them aggressively.

The U.S.-Iran cyberconflict has simmered for years, but the current crisis boiled over with Iranian attacks on U.S. interests in Iraq that led to the Jan. 3 U.S. drone strike that killed a senior Iranian general and terrorist leader. Iran's supreme leader threatened "harsh revenge," but said Iran would limit those efforts to military targets.

But even before Iranian missiles struck U.S. military bases in Iraq on Jan. 7, pro-Iranian hackers reportedly attacked at least one U.S. government-related website, along with a number of private company sites. Of greater concern, a new report details significant recent efforts by Iran to compromise the U.S. electric, oil and gas utilities.

Iran, which has reportedly attacked Saudi Arabian energy production, is also capable, according to U.S. officials, of conducting "attacks against thousands of electric grids, water plants, and health and technology companies" in the U.S. and Western Europe. Disrupting those systems could cause significant damage to homes and businesses and, in the worst case, injuries and death.

Much of our targeted critical infrastructure is under the control of private companies. Without government protection—and in the absence of any agreed-upon rules of cyber warfare—businesses are at high risk, and strict American criminal laws prohibit many forms of cyber self-defense by private companies. But there are straightforward measures companies can take both to protect themselves and to enhance our collective national cybersecurity.

What will Iran do?

Though it's impossible to predict with certainty the behavior of the Iranian regime and their many proxies, their cyberattacks likely will continue to go well beyond governmental systems, which are reasonably well defended. Iran and its supporters likely will focus on easier targets operated by private companies.

A recent U.S. Department of Homeland Security alert highlights Iran's capabity and willingness to engage in multiple types of destructive cyberattacks over the last decade. According to indictments filed by the U.S. Department of Justice, as cited in the DHS alert:

- Beginning as far back as 2011, Iran has conducted numerous Distributed Denial of Service (DDoS) attacks, sending massive amounts of internet traffic to knock websites offline. Iran's DDoS attacks have targeted, among others, financial institutions, for whom the resulting downtime reportedly cost millions of dollars.
- In 2013, one or more Iranians working for the country's Revolutionary Guard illegally accessed the control system of a New York dam, although no direct damage apparently was done.
- In 2014, Iran conducted an attack on the Sands Las Vegas Corporation, stealing customer credit card, Social Security and driver's license numbers and wiping all data from Sands' computer systems.
- Between 2013 and 2017, hackers working on behalf of Iran's Revolutionary Guard conducted a "massive" cyber theft operation targeting academic and intellectual property data, along with email information, from hundreds of universities, more than 45 companies, at least two federal agencies, at least two state governments and the United Nations.

It is possible that new efforts along these lines could be planned and timed to affect upcoming American elections. In addition, other countries could launch attacks and try to blame them on Iran, or vice versa.

No clear cyber rules of engagement

For conventional and even nuclear warfare, nations have, over the centuries, agreed to rules of armed conflict. They've developed ways to signal their intentions to escalate or deescalate a conflict. The U.S. and Iran have, for now, deescalated their public military conflict, thanks to Iran warning of its missile attack and not killing or injuring anyone and the U.S. not taking any further military action.

But cyberspace remains the wild west, with few, if any, agreed-on rules of engagement or well-understood signaling mechanisms. This makes any ongoing cyberconflict between Iran and its enemies all the more dangerous, with critical infrastructure companies at risk of being caught in the crossfire.

Without government assistance, those companies are largely on their own in defending against Iranian or other foreign government attacks. Strict criminal laws severely restrict companies' defensive options, prohibiting, for example, technologies to trace and destroy stolen data.

Collective cyberdefense

All of that said, there are steps companies can take to protect themselves, not only from Iranian or other governmental attacks but against hacking by data thieves, ransomware gangs, corporate rivals, disgruntled employees or anyone else.

Vigilance and communication is key. Companies, particularly in critical infrastructure sectors such as energy, financial, telecommunications and health care, should stay in closer-than-usual touch with appropriate governmental bodies, including the Department of Homeland Security, the FBI and the appropriate cyber Information Sharing & Analysis Centers. ISACs can help companies quickly get threat intelligence from the government and report attacks that may have implications beyond a single company.

Businesses also should carefully check their systems for malware previously inserted maliciously to enable future attacks. They should, of course, scan their systems on an ongoing basis for viruses and other malicious code that could let hackers have unauthorized access to systems or data. Companies should also securely back up their data, closely monitor data traffic on their networks, require workers to use multi-factor authentication when logging into IT resources, and provide cybersecuritiy training and awareness to employees.

Protecting our national and economic security from attack is in the hands of private citizens and companies in a way that hasn't been true perhaps since British boat owners rescued their nation's army from annihilation at Dunkirk in 1940. By taking reasonable cybersecurity measures, companies, and all of us individually, can not only help protect ourselves and our nation but, perhaps, even help to prevent a war.

Provided by The Conversation

https://techxplore.com/news/2020-01-cyberspace-front-iran-us-conflict-private.html