Protecting Critical Infrastructure from Cyber Attack

The enemy is using cyber weapons that are hard to track and even harder to fully attribute to an adversary, companies need to act now

By Richard Staynings, Chief Security Strategist for Cylera

Escalating geopolitical tensions in Europe and Asia place a very big target on western Critical National Infrastructure Industries (CNIs). What better way to attack your enemy than to do so using cyber weapons that are hard to track and even harder to fully attribute to an adversary. Whatsmore, when attribution finally does occur, it is often years later. By that time, the world has usually forgotten and moved on, or has been stunned by an even more destructive cyberattack. Nearly all cyberattacks and cyber-attackers thus far, have gone unpunished. This makes it the perfect crime for perpetrators.

Use of criminal proxies, insider threat agents, and the manipulation of national discourse with false inflammatory narratives propagated by social media platforms, are all designed to weaken an opponent. Many of these tactics such as undermining of confidence in the western institutions of government are straight out of the 1950's KGB playbook but have found new purpose in the 2020's through the seemingly addictive mediums of Facebook, Twitter and TikTok. If late twentieth century warfare and nation state competition for power was marked by spies and threats of nuclear war, then the twenty first century appears to be marked by the development of grey warfare, societal manipulation, and cyber weapons of mass destruction.

Indeed, the offensive cyber capabilities of America's adversaries appear to out-match the nation's domestic capabilities for cyber defense. China alone is thought to employ close to 100,000 Peoples' Liberation Army (PLA) cyber warriors. The job of these special military units is to develop access to other countries' IT systems, to establish footholds on sensitive networks, and to exfiltrate vast amounts of national secrets, intellectual property, and commercial trade secrets from western businesses. This all appears part of Xi Jinping's 'Made in China 2025' plan, to boost China's state-owned industries using stolen IP, and position China as the dominant global military and economic powerhouse.

Russia too is well known for the voracity of its organized crime syndicates and mafia cyber gangs who exercise huge campaigns of cyber theft and cyber extortion against non-Russian language computer systems. This includes the 2021 Wizard Spider cyber-cartel attack against the Irish HSE (Health Services Executive) that resulted in $600m in damages, and the 2023 Lockbit ransomware attack against the Royal Mail that prevented international parcels being sent for several weeks. Combined, these types of cyber extortion attacks net billions of dollars each year in illicit earnings for the criminal Russian state. While seemingly opportunistic and motivated by the possibility of monetary gain even - if government entities refuse to pay ransoms, these attacks can also be ordered by the Kremlin for even darker purposes. In this case the Royal Mail attack occurred just after Britain had agreed to send longer range missile systems to Ukraine. Although full attribution has yet to take place, most cyber forensic investigators don't believe in coincidence.

Critical infrastructure in other countries has similarly been hit by Russian ransomware gangs. In 2021 the Colonial Pipeline which supplies gasoline and jet fuel to the US East Coast from refineries in the Gulf of Mexico was shut down for several days by DarkSide, a Russian gang. Supplying half the fuel to the US east coast as far north as New Jersey, the President was forced to declare a national emergency.

The Baku–Tbilisi–Ceyhan (BTC) pipeline transports crude oil from Baku in Azerbaijan through Georgia to the port of Ceyhan in Turkey for export to the rest of the world. In 2008 it was blown up in a huge explosion in Refahiye in eastern Turkey, possibly by Kurdish PKK separatists, or possibly by a Russian cyberattack that over-pressurized the pipeline. The explosion conveniently occurred two days before the Russian invasion of Georgia and in the middle of the Russian backed Nagorno-Karabakh, Armenia - Azerbaijan war. It deprived Baku of its oil revenue for several months and Tbilisi of needed revenue in transportation fees.

Whether or not the Kremlin was involved in these cyber-physical attacks, Russia has plainly developed some of the best cyber-kinetic offensive technologies and has been doing so since the 1990s and its wars against Chechnya, Georgia and elsewhere. The Ukraine electrical grid has been the victim of Russian cyber-attack many times since 2015 when the country failed to subvert itself to Russian hegemony following the invasion of Crimea or to put in place an east looking President following the Orange Revolution in 2014 and the un-ceremonial removal from office of Viktor Yanukovych a staunch Putin confident. Electrical power transformers have been overloaded and blown up, or the electrical grid turned off at the height of winter across parts of the country. Nor have hospitals and other CNIs been spared from the wrath of Russian hackers. Numerous hospitals have been cyberattacked, many far from the front lines where soldiers might receive treatment for wounds. The list of deliberately targeted medical facilities includes obstetrics and pediatrics hospitals and clinics – some of which have been targeted by missile attacks at the same time.

However, the Russian military establishment, through groups like 'Sandworm', part of the Russian GRU, (the Main Directorate of the General Staff of the Armed Forces of the Russian Federation) takes the prize for the singularly most costly and destructive cyberattack of all time when in 2017 'Not Petya' a viral wiperware attack was launched upon the world. It took down many global businesses and cost the world somewhere between $8 and $12bn US dollars. This Russian military supply chain cyberattack was targeted at Ukrainian tax accounting software vendor M.E. Doc and intended to cripple Ukrainian businesses, however it quickly spread beyond the borders of Ukraine to every organization that does business in the country including an alarming number of Russian companies. The cyberattack therefore also takes the prize for the largest 'home-goal' of all time, negatively impacting the Russian economy along with the rest of the world. It is unknown just how many of those involved in the Not Petya attack later fell from balconies, but by all accounts, Putin was not pleased. Russia has so far not paid compensation to those who suffered losses.

Smaller nation-states like Iran and North Korea also play a part in this game of gray warfare through attacks against CNIs including US power companies many of which were thought to have been infiltrated by Iranian attackers a decade ago. Meanwhile the DPRK has raided national banks such as the Bank of Bangladesh and launched indiscriminate ransomware attacks like WannaCry against Asian banks and healthcare providers such as the NHS.

The prospect of a small hospital system, an electrical distributor, or telco provider having to defend itself from a determined and well-resourced nation state adversary, makes absolutely no sense. These defenders will be out-gunned every time and don't stand a chance. It is perhaps no surprise then, that so many CNIs have been easily attacked and held to ransom, impacting national economies and society in general. National governments therefore not only have a duty of care to protect and defend CNIs from cyberattack but need to play an active role in the protection of their citizens from pariah state adversaries via these highly vulnerable attack vectors.

Today however, government agencies which in the US include the FBI, Secret Service, and CISA - part of Homeland Security, play only a very limited role. This mostly includes the sharing of threat intelligence via FBI and InfraGuard briefings, or assistance with forensic investigation following an attack or breach. Given the criticality of CNIs to the economy, perhaps it's time that the government did more. The trouble is that in the United States, most CNIs are privately held. As an example, outside of military DHA hospitals, the Veterans Administration, and state clinics, the vast majority of US healthcare providers are privately owned and operated. Nearly all of these suffer from chronic cybersecurity underfunding and under-staffing and have only limited capabilities to protect or defend against a regular cyberattack, let alone a state sponsored one. Other CNIs suffer from a similar predicament.

As health systems continue to modernize and adapt to the changing nature of providing critical health services to patients and communities, they become especially vulnerable to cyberattacks. A sprawling digital footprint of vast lakes of medical data, AI-based medical applications, and a growing number of unmanaged connected IoT devices, all compound historic underinvestment in security. Most providers have a hard time understanding what connects to their networks, let alone what internal vulnerabilities and risks urgently need to be addressed – even with adequate resources to do so.

The danger is that a concerted and coordinated nation-state attack against US CNIs would undoubtedly be designed in such a way as to distract and divert key resources away from the battlefield. If nine key substations are knocked out, the U.S. could suffer a crippling coast-to-coast blackout for 18 months — or longer since spare transformers are not available and are no longer being constructed. Aside from the deaths of those reliant upon electricity to power their medical devices once battery backups run out, millions more city dwellers would die within weeks of a public health crisis as lack of drinkable water or the ability to pump and treat sewage resulted pandemic diseases the United States has not witnessed since the 19th century. As a result, society would most likely quickly break down resulting in anarchy. This may prove a very attractive and convenient attack vector for an adversarial nation-state to weaken and disable the United States, without ever firing a shot and while all the time hiding behind plausible deniability.

The United States and other western nations are particularly vulnerable to such an attack, given our reliance upon critical industries. The absence of air traffic control would ground all flights, while trains and trucks would cease to transport goods to markets. Highly developed western countries are far more dependent upon CNIs than Russia and China where the majority of each population continues to grow its own food, or North Korea where electricity is highly unreliable and largely not available outside of Pyongyang. A reciprocal attack by the west would therefore have only limited impact. With few disincentives, what is to prevent an adversary from launching such an attack?

Perhaps it's time that western governments looked a lot closer at the weakness and vulnerabilities of their critical industries in the light of modern cyber weapons and recent attacks. Given a responsibility to defend and protect citizens, perhaps the US Congress should spend less time infighting and consider how best to protect the US population, US businesses and remaining US industries from those who would like to weaken and damage the country.

About the Author

Richard Staynings is a globally renowned thought leader, author, and public speaker. A thirty-year veteran of cybersecurity, he has served as a subject matter expert on government Committees of Inquiry into some of the highest profile healthcare breaches.

Richard is currently Chief Security Strategist for Cylera, a pioneer in the space of medical device security. He is author of Cyber Thoughts, teaches postgraduate courses in cybersecurity, and health informatics at the University of Denver, and is a retained advisor to a number of friendly governments and private companies.

Richard Staynings can be reached online at info@cylera.com and at our company website https://www.cylera.com/