KnowBe4

Cyber Attacks on Infrastructure

The New Geopolitical Weapon

CYBER ATTACKS ON INFRASTRUCTURE:

THE NEW GEOPOLITICAL WEAPON

Critical infrastructure, the systems and physical assets that keep a society functioning, includes a vast system of power grids, communication systems, transportation networks, ports, and more. Take any one sector down, and you can cripple entire segments of a society. A collapse of the transportation networks, for example, could mean that air traffic controllers suddenly can't communicate to planes in the air. Freezing the ports and shipping lines will slow to a crawl, hampering the delivery of food and other goods and creating economic havoc. Bring down the power grid in the middle of winter and millions of homes could be plunged into darkness, with communications cut, no access to bank accounts, and closed hospitals. Virtually any of these scenarios set the stage for widespread social unrest.

Large scale outages can disrupt critical services including healthcare and emergency services, and government agencies on a global scale. Numerous hospitals may have issues accessing data, and appointments and surgeries can be delayed. Cybercriminals swiftly try to exploit the situation, registering phishing domains and impersonating support staff.

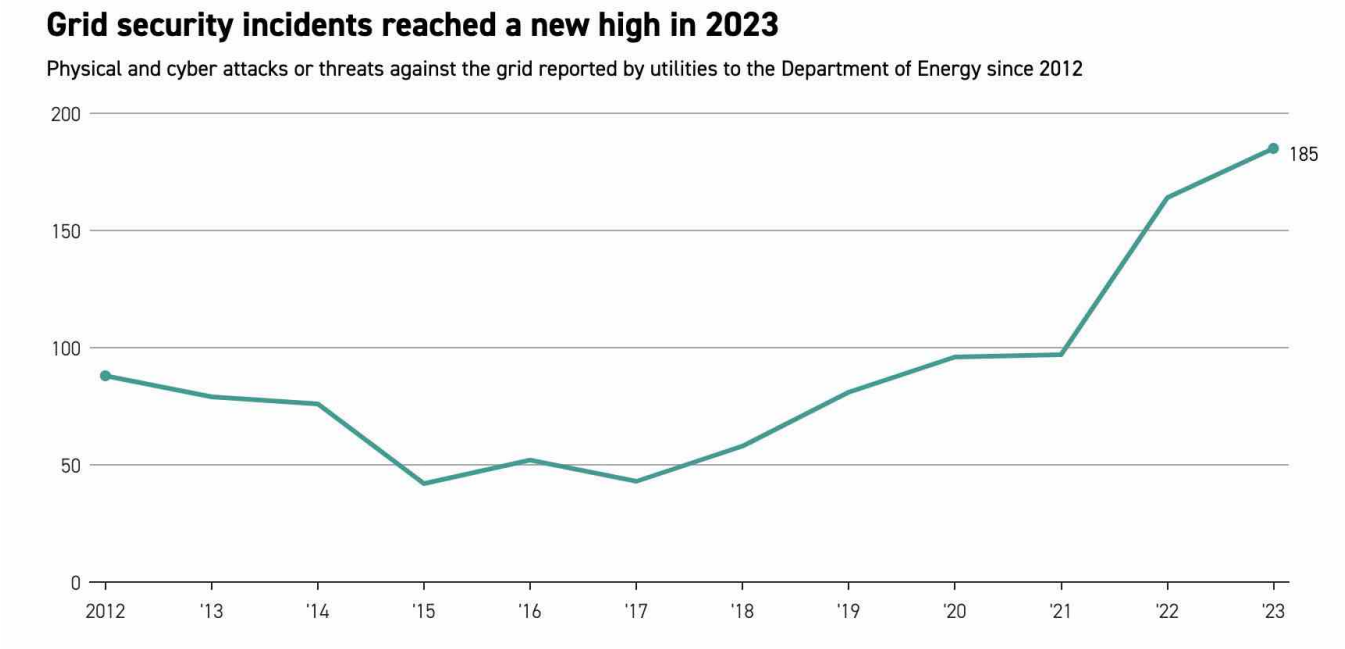
As the infrastructure sectors in developed nations have become increasingly interconnected to digital technologies, advancements have increased their capacities and efficiency; but they have also opened new vulnerabilities to cyberattacks. Energy, transportation, and telecommunications have all become primary targets. And knowing that the consequences of an attack on any of these targets are potentially severe, geopolitical adversaries have been moving into position to exploit the sector's vulnerabilities, making cyberattacks on infrastructure a powerful new addition to the arsenal of digital weapons.

One of the most frightening events would be an attack on the energy sector, which includes power generation, water treatment, electricity production, and other interconnected platforms. Any attack on this sector could throw communities into chaos; for example, in time of war, a sudden power shutdown could severely hamper the operations of hospitals, first responders, and military bases. This is not as far-fetched a scenario as we would like to think.

In November 2023, a report from the Paris-based International Energy Agency (IEA) found that globally, the average number of cyberattacks against utilities each week more than doubled between 2020 and 2022 worldwide. In 2023 they doubled again.

On April 4, 2024, the North American Electric Reliability Corporation (NERC) reported that the number of points in the US power grids that are vulnerable to cyberattacks is increasing at a rate of approximately 60 per day. In 2022 the number of susceptible points grew from 21,000 to 22,000. Now it is between 23-24,000.[1]

1 Kierney, Laila, "US electric grid growing more vulnerable to cyberattacks, regulator says," Reuters, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04



[2]

Europe's power grid is under a "cyberattack deluge," inundated by thousands of attacks since Russia's invasion of Ukraine. Leonard Birnbaum, chief executive of E.ON, one of Europe's largest utilities, said last November that "the crooks are becoming better by the day," adding "I am worried now and I will be even more worried in the future." [3]

In May of last year Denmark's energy infrastructure was compromised in a coordinated attack, with the attackers gaining access to some of the companies' industrial control systems. "The attackers," the organization said, "knew in advance who they were going to target and got it right every time."

Polish Deputy Energy Minister Ireneusz Zyska, speaking to *Politico* last November, recalled a recent visit to Poland's grid operations hub, buried three stories underground to protect it from nuclear attacks. "I was… observing thousands of attacks on our energy grid taking place live. It is clear that these attacks come

2 Morehouse, Catherine, "Tensions at home and abroad pose growing threat to US grid," E&E News, April 8, 2024 https://www.eenews.net/articles/tensions-at-home-and-abroad-pose-growing-threat-to-us-grid/

3 Jack, Victor, "Europe's grid is under a cyberattack deluge, industry warns," Politico, November 23, 2023 https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/

from the East: the Russian Federation and non-democratic countries," he said, adding that these places "have created special teams of people working on attacking the democratic states of the European Union cybernetically to cause havoc."

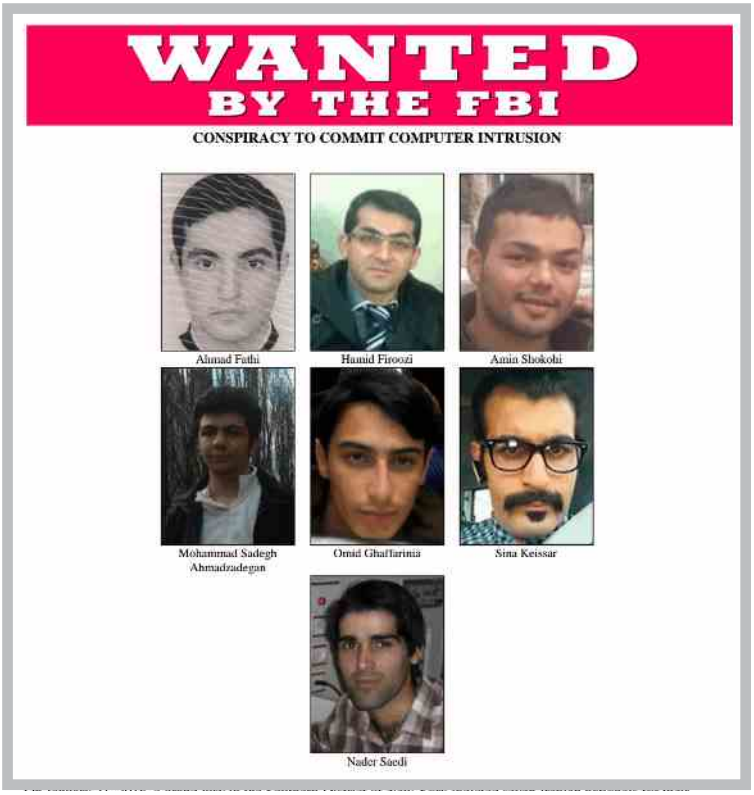
In September 2023, *The Record* reported that the national power grid of an "unspecified Asian country" had been attacked, with signs pointing to ShadowPad malware, which is used by hacking group APT41, a hacking group connected to China's Ministry of State Security and the People's Liberation Army.[4] The infiltration went undetected for six months, during which the hackers expanded their access to storage devices, gathering system credentials, and covering their tracks.

According to research from Recorded Future, ShadowPad had also been used over the course of the year in 2020, to target a large portion of India's power sector, as China and India were involved in border disputes near eastern Ladakh and Tibet. Ten distinct power sectors were infiltrated, including four of the country's Regional Load Dispatch Centers, which balance electricity supply and demand. The attackers are also believed to have targeted a high-voltage transmission substation, a coal-fired thermal power plant, and two seaports. Research has pointed to at least five Chinese state-sponsored groups using ShadowPad for espionage purposes.[5]

THE RISING TARGET

Cyberattacks on critical infrastructure are not seeking information; they are most frequently seeking access to control systems for the purposes of disruption, whether for foreign or domestic terrorism, or access to secrets for the purpose of espionage. And while such attacks are on the rise globally, they are not new.

In 2013, Iranian hackers breached the command and control center of the Bowman Avenue Dam in Rye Brook, New York, and gained control of the floodgates. In 2016 the US Justice Department unsealed an indictment that indicated this was only one part of a plan. Between 2011 and 2013 seven Iranian nationals, members of Iran's Islamic Revolutionary Guard Corps, had launched cyberattacks on 46 US companies and institutions. According to the indictment, Hamid Firoozi, the man who infiltrated the Bowman Avenue Dam, had accessed its supervisory control and acquisition data (SCADA) system via a cellular modem that connected the dam to the Internet.



A Department of Justice poster of seven indicted Iranian hackers, March 24, 2016 in Washington, DC.(FBI.gov)

4 Greig, Jonathan, "Power grid of Asian nation shows signs of intrusion by espionage group," The Record.media, September 12. 2023, https://therecord.media/power-grid-asian-nation-cyber-espionage-redfly-shadowpad

5 Janofsky, Adam, "China-linked Hackers Target India's Power Grid Amid Border Clashes," The Record, February 28, 2024 https://therecord.media/china-linked-hackers-target-indias-power-grid-amid-border-clashes

Firoozi gained remote access to information on "the status and operation of the dam, including information about the water levels and temperature, and the status of the sluice gate, which is responsible for controlling water levels and flow rates." Manhattan US Attorney Preet Bahara said in a statement at the time that the infiltration of the dam represented a "frightening new frontier in cybercrime. We now live in a world where devastating attacks on…our infrastructure and our way of life can be launched from anywhere in the world, with a click of a mouse."

In 2017, one of the most potentially dangerous cyberattacks on industrial infrastructure, the Triton Malware Attack, nearly caused a massive explosion at a Saudi petrochemical plan, when Russian hackers were able to take over the plant's safety system and operate the system remotely. The Australian security consultant called to the scene said that what he found "made his blood run cold."

The hackers appear to have been inside the organization's network since 2014, moving from the corporate IT network to the plant's own network, then into an engineering workstation, possibly by intercepting an employee's login credentials. Luckily, a flaw in the malware's code gave the hackers away before they could execute their plan, which was apparently to overload the plant's safety checks, leading to the release of toxic hydrogen sulfide gas or to cause massive explosions, each of which would have resulted in substantial loss of life. According to the *MIT Technology Review*, it was the first time the cybersecurity world had seen code deliberately designed to put lives at risk.[6]

It was later discovered that the attack was state-sponsored by a Russian federal institute. Theories have differed on whether the attack was the result of a successful misconfiguration attack, or the result of spear phishing.

In 2020, during the peak of Covid-19 and in the midst of a heatwave, hackers tried to take over the industrial control systems (ICS) of five Israeli Water Authority facilities in two rural locations, trying to compromise the systems for pumping stations, wastewater plants, and agricultural pumps; their plan was to spike the level of chlorine and other chemicals to harmful levels in the nation's water supply. The attack was detected before damage could be done. Had they been successful they would have severely disrupted the region's water supply in a critical period, overloaded hospitals, devastated crops as farmers unwittingly poisoned their crops, and more. The perpetrators have not been identified.

In 2021, the Colonial Oil pipeline, the largest pipeline in the US, was hit with a massive targeted ransomware attack. The pipeline supplies more than 45% of the gas, diesel, and jet fuel for the American East Coast. The pipeline was forced to shut down and was offline for 11 days after paying $5 million in ransom. The attack, which left 11,000 gas stations out of gas, caused states of emergency to be declared in four states, and spiked the cost of fuel to its highest in six years, was perpetrated by the Russian hacker group DarkSide.

6 Giles, Martin, "Triton is the world's most murderous malware, and it's spreading," MIT Technology Review, March 5, 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

While these have been the most talked about and press worthy attacks on critical infrastructure, they don't begin to give the full picture. The sheer numbers of attacks are accelerating every year. Between January 2023 and January 2024, the world's critical infrastructure has been attacked more than 420 million times with attacks ranging in magnitudes, according to Forescout Research – Vedere Labs.This is 13 attacks per second, a 30% increase from 2022.

The attacks have impacted 163 countries. The United States has been the primary target, followed by the United Kingdom, Germany, India, and Japan. China accounts for the highest concentration of threat actors targeting critical infrastructure, followed by Russia, and Iran.[7]

THE LARGER CYBER WAR

Other developments threatening the vulnerabilities of critical infrastructure may make a group of Russian or Iranian hackers, even when state sponsored, look like child's play.

In May 2023, about the time the US was shooting down a spy balloon launched by China, inspectors found something while investigating intrusion activity that had impacted a US port. As they traced the intrusion, they found other networks that had been hit, "including some in the telecommunications sector in Guam," home to a vast military base that would be a central point of any US response to a Chinese invasion of Taiwan. The code had been installed by a government hacking group in China.

7 "2023 Global Threat Roundup," Forescout-Vendere Research, January 24, 2024, https://www.forescout.com/resources/research-report_2023-threat-roundup

US Air Force B-52H Stratofortress bomber

According to the *New York Times*, "The operation was conducted with great stealth, sometimes flowing through home routers and other common internet-connected consumer devices, to make the intrusion harder to track." It used a web shell, a malicious script that allows remote access to a server. The National Security Agency in the US, with their counterparts in Australia, Britain, New Zealand and Canada, published a 24-page advisory about the finding, saying that the state-sponsored Chinese effort was aimed not only at critical infrastructure including communications, electric and gas utilities, but also maritime operations and transportation. American officials said that the intrusion was part of a "vast Chinese intelligence collection effort that spans cyberspace, outer space and, as Americans discovered with the balloon incident, the lower atmosphere." [8]

James A. Lewis, Director and Pritzger Chair of the Center for Strategic and International Studies (CSIS) says we shouldn't act surprised, that probing the critical infrastructure of potential adversaries to identify targets and prepare them for possible cyberattack is "the kind of reconnaissance any capable nation would engage in."

What is unusual about the Guam attack, Lewis says, is that the attacks were not aimed at Guam's infrastructure. The primary targets, both in Guam and the United States, were those that would support US forces in any engagement over Taiwan.

There is no evidence that China has used these intrusions in an offensive capacity. But should a conflict over Taiwan broaden, Lewis says, China "may decide that cyber actions against civilian infrastructure in the United States could usefully disrupt communications and the flow of material needed for military operations."[9]

If such a decision was made, the first target would most likely be electrical power facilities. The second would be the pipelines and railroads in the continental United States. Third would be the logistics and communications networks, including those that support supply chains for manufacturing munitions and military aircraft. Other primary targets would include telecommunications systems in cities and regions where naval and air bases are located, such as California, Hawaii, and Washington State.

The cost, of course, would be the risk of full-on military engagement with the United States. With that in mind, China could also decide not to bring about a wide-scale cyber disruption, and instead reserve its cyber activities for espionage purposes.

---

8 Sanger, David E., "Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?" New York Times, May 24, 2023, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

9 Lewis, James A., "Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario," Center for Strategic and International Studies, August, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230811_Lewis_Cyberattack_Taiwan.pdf

OUR ROLE

Cyberattacks on critical infrastructure by global adversaries is a clear illustration of the evolution and changing nature of conflict in the 21st century. Just as aerial bombing and military occupation disrupted civilian lives in World War II, the citizenry of countries suffering such attacks could be the group most heavily impacted by the conflicts.

While it still has not happened to a catastrophic level, individuals and the entire business community have a role to play in protecting their lives and operations. While government agencies and diplomats work with other leaders to mitigate the potential effects of the next attack, one of the strongest protections against intrusion in our lives by foreign adversaries is a shared culture of security.

More than one of the attacks noted above used home routers to infiltrate the systems controlling safety checks and water safety. Having a router in your living room that is not configured securely with a secure password could potentially leave the door open for an adversary. Buying a router from eBay when you don't know its origin could be similarly dangerous.

An IT manager for an organization producing a small part of their country's infrastructure could likewise, through lax security, leave the door open for adversaries to enter their nation's infrastructure.

These small "holes" are what allow threat actors to enter larger systems, sometimes staying there for years while they travel the system, gathering information and planting malicious software. Even when the intrusion goes unnoticed at the time, it can have staggering effects on large swaths of people down the road.

All hackers, including those sponsored by their state, love and use phishing and social engineering to steal credentials or gather other information that allows them to enter systems. A lack of cybersecurity awareness, in communities or organizations, leaves a wide attack surface open for intrusion.

All hackers, including those sponsored by their state, love and use phishing and social engineering to steal credentials or gather other information that allows them to enter systems. A lack of cybersecurity awareness, in communities or organizations, leaves a wide attack surface open for intrusion.

The creation of a strong security culture requires more than discussions, reports, and papers, and it cannot be the job of only governments and large corporations. The susceptibility of individual users, whether at home or at work, is an important place to start.

Each year, KnowBe4 analyzes the online behavior of users to determine a baseline of how many individuals, without security awareness training, are susceptible to clicking on fraudulent links in phishing emails. For its 2024 Phishing by Industry Benchmarking report, KnowBe4 analyzed the behavior of 11 million users across various industries and sizes. The baseline statistics indicate a "Phish-prone PercentageTM" (PPP) of 34% of users; in other words, more than one out of three computer users tested were likely to click on a bad link in a phishing email, creating a liability not just for their personal affairs, but for their organizations while at work, and for their communities.

The good news is that consistent and comprehensive cybersecurity awareness training works. According to the study, 90 days into an integrated approach of educational content and simulated phishing tests changed the outcomes noticeably, with the Phish-prone Percentage across industries dropped to 18.4%. After one year or more of ongoing training, the percentage of users who will fall for a phishing email falls to 4.5% across industries.

Strengthening Your Organization's Defense

The continuing and escalating number of cyberattacks on critical infrastructure poses a global threat, potentially causing widespread social and economic disruption. Organizations must adopt a multi-layered defense strategy involving technology, processes, and people to reduce the risk of a successful cyber breach.

Organizations can ensure a more resilient cybersecurity program by implementing the following steps:

- Foster a strong security culture through ongoing training and assessments
- Implement asset inventory management
- Enforce multi-factor authentication (MFA) for access to all critical systems
- Develop and regularly update incident response playbooks
- Conduct periodic tabletop exercises and simulations
- Establish secure backup systems, testing, and recovery procedures
- Collaborate with industry partners and government agencies to share threat intelligence
- Continually assess and update security measures to address emerging threats

By integrating these practices, critical infrastructure organizations can significantly improve their resilience against evolving cyber threats. As the threat landscape changes, cybersecurity strategies should adapt to continue to protect the critical systems society depends on daily.

INCIDENT RESPONSE PLAYBOOKS

Organizations must be prepared for potential incidents and disasters. Incident response playbooks, developed by IT and cybersecurity teams, outline procedures for known attacks to minimize risk and downtime. While it's impossible to anticipate every catastrophe, disaster recovery programs should have the infrastructure to restore normal operations swiftly.

These plans are compiled in a "playbook," containing recovery procedures, communication chains, and crucial information like Bitlocker codes or admin passwords. It is advisable to have secure hard copies stored in multiple locations to avoid a single point of failure.

Regular drills and tabletop exercises involving IT, OT, and business teams help ensure staff readiness during incidents. By incorporating basic cybersecurity practices such as asset inventory management, MFA implementation, and fostering a strong security culture, organizations, especially those in critical infrastructure, can significantly boost their resilience against evolving cyber threats.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Training Preview
See our full library of security awareness content; browse, search by title, category, language or content

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E08K01