A CISO'S GUIDE TO GEOPOLITICS AND CYBERSECURITY

Understanding the Cyberwarfare Strategies of Russia, China, and Iran

EXTRAHOP®

Table of Contents

GEOPOLITICAL STRAIN HAS ESCALATED INTO CYBERWARFARE

> **“Geopolitical conflict is increasingly playing out in cyberspace, amplifying risks to U.S. and allied critical infrastructure.”**
>
> — 2024 Report on the Cybersecurity Posture of the United States, Office of the National Cyber Director and Executive Office of the President[1]

Geopolitical tension has arguably reached fever pitch around the world, the result of wars and conflicts, regional instability, military posturing, tariffs and trade restrictions, border skirmishes, high stakes elections, and countless other critical issues. Strained relations between major powers have escalated into a new domain of warfare, where cyberattacks serve as both a tool for espionage and a weapon of disruption. Such attacks threaten national security, the economy and commercial interests, while having profound implications for critical infrastructure worldwide.

In addition to targeting critical infrastructure operators and government agencies at the highest levels, adversaries are increasingly causing disruptions at public and private businesses worldwide. And while these nation-state sponsored attacks can cost organizations financially, the impacts can be much more devastating and far-reaching:

- **Military disruption** - Cyber operations and tactics are now critical elements of many countries’ military strategy, and they take center stage when foreign actors are considering how to influence global affairs.
- **Emotional and psychological warfare** - Cyberattacks can create population behavior effects, inspiring feelings of terror, paranoia, and uncertainty. Additionally, distribution of false information through mis- and disinformation campaigns can cause confusion and divisive behavior.
- **Information theft** - Nation-state sponsored cyberattacks have long been used to gather intellectual property (IP) and other information that can be used strategically and destructively, now or in the future.
- **Financial fallout** - Attacks could have a wide-reaching impact on financial markets and local and global economies, creating a destructive domino effect.
- **Critical infrastructure disruption** - Nation-states are targeting infrastructure that deliver critical services to citizens, including power grids, water supply networks, and transportation systems.

Experts advise organizations to prepare for an uptick in nation-state-backed cyberattacks, particularly those from Russia, China, and Iran. What specifically should cybersecurity leaders expect from these nation-states this year and beyond? To anticipate these threats, it helps to understand each country’s cyber strategy and objectives.

1 2024 Report on the Cybersecurity Posture of the United States Office of the National Cyber Director Executive Office of the President. *WH.GOV*, May 2024. https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

RUSSIA

Information strategy

Russia views the information space in geopolitical terms, defining it more broadly than the West to include not only hardware, software, and infrastructure, but also social media, Open Source Intelligence (OSINT), and psychological layers. The country exploits democratic freedoms and Western "openness" to gain information superiority, and then uses those democratic freedoms against its targets to destabilize foreign entities.

Objectives

Russia has two goals for its cyber operations against the U.S. and other countries, says Dr. Bilyana Lilly, CISSP, Chair of the Resilience Track for the Warsaw Security Forum, and author of the book "Russian Information Warfare: Assault on Democracies in the Cyber Wild West." First, Russia seeks to damage the technology and digital infrastructure of its adversaries. Second, Russia aims to erode and manipulate the decision-making power of its adversaries as well as affect the minds and behavior of U.S. and other citizens. This is a psychological objective that encompasses everything from mis- and disinformation campaigns to assassinations and coups d'état.[3]

While Russia has been distracted with domestic issues and crises, Lior Div, world-renowned expert in offensive and defensive cybersecurity, believes Russia has reemerged as a formidable cyberthreat to U.S. organizations.[4]

> **"Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology (OT) networks; and disrupt critical industrial control systems (ICS)/ OT functions by deploying destructive malware."**
>
> — Cybersecurity & Infrastructure Security Agency (CISA)[2]

Russian state-sponsored actors

Russia's special services, including the Main Directorate of the General Staff of the Armed Forces (GRU), Federal Security Service (FSB), and Foreign Intelligence Service (SVR), are involved in running cyberwarfare operations and managing groups of threat actors like APT28, CyberBerkut, and SandWorm. Russian threat actors operate under the mission to secure the Russian regime, engage in competitive intelligence, and decentralize direct action. Russia also relies on cyber proxies like oligarchs, businesses, non-profits, the Russian Orthodox church, media, civilians, gangs, and criminals to reduce direct conflict and maintain plausible deniability.

2 CISA. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 9 May 2022, www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

3 Cleveland, Sarah. "The Impact of Geopolitics on Cybersecurity in 2024 and Beyond." *ExtraHop*, 15 May 2024, www.extrahop.com/blog/geopolitics-and-cybersecurity-risk-in-2024-and-beyond

4 Cleveland, Sarah. "The Impact of Geopolitics on Cybersecurity in 2024 and Beyond." *ExtraHop*, 15 May 2024, www.extrahop.com/blog/geopolitics-and-cybersecurity-risk-in-2024-and-beyond

Notable attacks

German wind turbines

Launching a malicious software update, Russian nation-state sponsored cyber attackers exploited a fault in the satellite connection between IT systems and German wind turbines. The attack took 5,800 turbines offline simultaneously, disabling operators' ability to monitor the critical infrastructure remotely.

Colonial Pipeline

Acting as a proxy for the Russian government and in its interests, a Russian ransomware group launched a multi-stage cyberattack on Colonial Pipeline, bringing the major gas line to a standstill. The attackers gained access through compromised end-user VPN and network credentials, stole over 100Gb data, and then infected the network–all within a two-hour window. Colonial Pipeline paid a $4.4 million ransom, but the effects of the attack were widespread, impacting the airline industry due to a jet fuel shortage, causing panic-buying and long lines at gas stations, and significantly increasing average gas prices.[5]

SolarWinds

Dubbed by some as "the most audacious cyberattack in history," Russian threat actors used malware to sabotage code within SolarWinds' IT monitoring and management software, which was made possible because it had not been updated. The attackers gained unfettered access to the networks, systems, and data of thousands of SolarWinds customers for over nine months, including U.S. federal government agencies like the U.S. Department of Homeland Security, Justice Department, State Department, the National Nuclear Security Administration, and the Department of Energy. The fallout cost to SolarWinds was at least $18 million.[6]

> **"We know that malicious cyber activity is part of the Russian playbook, which is why every organization–large and small–should take action to protect themselves during this heightened threat environment."**
>
> — Jen Easterly, Director, Cybersecurity & Infrastructure Security Agency (CISA)

5 Kerner, Sean. "Colonial Pipeline Hack Explained: Everything You Need to Know." *TechTarget*, 26 Apr. 2022, www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

6 Satter, Raphael. "SolarWinds Says Dealing with Hack Fallout Cost at Least $18 Million." Reuters, 13 Apr. 2021, www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/

THE PEOPLE'S REPUBLIC OF CHINA (PRC)

Information strategy

China's overall information strategy is driven by its goal to become a "cyber superpower."

Like Russia, China defines cyber broadly to include not just hardware, software, infrastructure, and data, but also social networks, news outlets, etc. However, unlike Russia, China takes a long-game approach to cyberattacks, launching malware on networks and waiting to attack and disrupt western critical infrastructure when it's most advantageous, often during times of crisis or conflict.

Chinese advanced persistent threats (APTs) are unique in that they do extensive research and field work on their intended targets. They infiltrate existing infrastructure years in advance of an exploit with custom-built malware and persistent advanced social engineering. China takes pride in its cyber capabilities, launching cyberattacks as a way to showcase their prowess.

> **"China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks. If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."**
>
> — The Office of the Director of National Intelligence's 2024 Annual Threat Assessment[7]

7 People's Republic of China Cyber Threat | CISA. *Cybersecurity and Infrastructure Security Agency CISA*, 2024, www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

8 Fox-Sowell, Sophia. "'We Know They're on the Network,' CISA Official Says of Nation-State Actors Infiltrating U.S. Critical Infrastructure." *StateScoop*, 19 Mar. 2024, statescoop.com/nation-state-actors-us-critical-infrastructure-cisa-2024/

Objectives

China's objective is to establish cyber supremacy and independence from the West. However, Div says China's overall cyber and information strategy is simpler and more transparent. China launched "Made in China 2025" in 2015, a 10-year strategic plan to develop its dominance in 10 industries, including information technology and telecommunications, advanced robotics and artificial intelligence, aerospace engineering, alternative energy vehicles, biomedicine, and medical devices. With Made in China 2025 in mind, the motivation for China's hacking campaigns becomes clear: cyber espionage and intellectual property theft.[8]

Chinese threat actors operate under the mission to secure the Chinese regime, engage in competitive intelligence, and decentralize direct action. Therefore, its approach to cyberwarfare rarely uses ransomware as a weapon, instead opting to use malware to maintain a presence on organizations' networks for as long as possible to collect as much information as they can. Andrew Scott, associate director for China operations at the Cybersecurity and Infrastructure Security Agency (CISA), disclosed that "…our incident response effort has confirmed that [People's Republic of China] cyber actors have been on our critical infrastructure networks for in some cases up to the last five years." Div believes that China has collected more information than it can currently use, including encrypted data. But he surmises that when quantum computers become available, the government will be able to decrypt and use this data.

Chinese state-sponsored actors

China has two main cyber units that run cyber warfare operations and manage groups of threat actors:

- **The Ministry of State Security (MSS)** is the principal civilian intelligence, security, and secret police agency in China, and the most advanced and prolific cyberwarfare organization in the country.
- **The Strategic Support Force (SSF)** was formed in 2015 and has joint information warfare command with the People's Liberation Army. The unit operates with a broad mandate covering electronic warfare, strategic military cyber operations, and political warfare.

Using cyber proxies is an especially strategic practice because China is run in a "whole of country" approach, fusing national defense and the private sector. The country leverages skills from individuals, universities, and the public/private sectors to support its cyberwarfare efforts. Recently, proxy groups have been encouraged to take a more overt approach to employing disruptive tactics, focusing on disruption to supply chains, biotech, semiconductors, quantum research, and renewable energy industries.

> **"They're not focused just on political and military targets. We can see from where they position themselves across civilian infrastructure, that low blows aren't just a possibility in the event of conflict, low blows against civilians are part of China's plan."**
>
> — Christopher Wray, Director of the FBI

Notable attacks

APT40 attacks on the U.S. and Australia

In July 2024, a joint advisory from Australia, the U.S., the U.K., Canada, New Zealand, Germany, the Republic of Korea, and Japan issued an unprecedented multinational security warning that APT40, a hacker group linked to China's Ministry of State Security (MSS), carried out sophisticated cyberattack operations against Australian and U.S. networks. The group is known to exploit vulnerable, public-facing infrastructure vs. using techniques that rely on user interaction such as phishing campaigns."[9]

Microsoft Exchange server breach

In March 2021, Microsoft detected multiple zero-day exploits being used to attack on-premises versions of Microsoft Exchange Server. Within days, an estimated 250,000 servers were attacked, including servers belonging to around 30,000 organizations in the U.S. Hackers used several Exchange vulnerabilities to gain access to email accounts and install webshell malware, a technique that required very little technical skill. This approach gave the cybercriminals ongoing administrative access to the victims' servers and potential conduits to other organizations they were connected to.[10]

11-year access of targeted data theft

Two Chinese hackers working with the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS) ran an 11-year intellectual property theft operation, stealing terabytes of data, which posed a sophisticated and prolific threat to U.S. networks. Targeting the technology manufacturing, healthcare, energy, defense, and gaming industries, the hackers gained access to the victims' networks by exploiting publicly known software vulnerabilities in popular web server software, web application development suites, and software collaboration programs.[11]

Volt Typhoon (malware)

In April 2024, FBI Director Christopher Wray warned that China is developing the "ability to physically wreak havoc" on U.S. critical infrastructure, warning that the attackers are waiting "for just the right moment to deal a devastating blow.[12] He was referring to the ongoing Chinese hacking campaign called Volt Typhoon in which the hackers install malware on network routers and internet connected devices. While it is unknown how widespread the attacks are, hackers have already gained access to several American companies in the telecommunications, energy, water, and other critical sectors, with 23 pipeline operators targeted. "Its plan is to land low blows against civilian infrastructure to try to induce panic," says Wray.[13]

2023 phishing campaign

Beginning in 2023, China launched a widespread phishing campaign targeting Uzbekistan, South Korea, the Philippines, and Japan. Hackers gained access to the victims' systems, inserted spyware, and established command and control and the ability to spy on their targets' activity.

9 Woollacott, Emma. "Eight Nations Issue Warning about Speed of Chinese Hackers' Operations." *Forbes*, 9 July 2024, www.forbes.com/sites/emmawoollacott/2024/07/09/eight-nations-issue-warning-about-speed-of-chinese-hackers-operations/

10 Carlson, Brian. "The Microsoft Exchange Server Hack: A Timeline." *CSO Online*, 6 May 2021, www.csoonline.com/article/570653/the-microsoft-exchange-server-hack-a-timeline.html

11 "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research." *U.S. Department of Justice*, 21 July 2020, www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

12 Bing, Christopher. "FBI Says Chinese Hackers Preparing to Attack US Infrastructure." *Reuters*, 18 Apr. 2024. https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/

13 Bing, Christopher. "FBI Says Chinese Hackers Preparing to Attack US Infrastructure." *Reuters*, 18 Apr. 2024. https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/

IRAN

Information strategy

Iran's information strategy is focused on destruction, disruption, espionage, political interference, coercion, and confrontation. Attacks on the U.S. have historically been "retaliatory," intended "to make the point that the United States is not invulnerable but without going too far."[15] The Office of the Director of National Intelligence warns that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."[16]

Iran was among the first to formulate a national cyber strategy, and it has steadily improved its cyber capabilities over the past 15 years in response to the Stuxnet cyberattack on Iranian nuclear facilities in 2010, foreign cyber espionage, the need to control its own population, and years of engagement with Israel and Saudi Arabia.[17, 18] Iran dedicates a massive and growing budget to cyber according to the Institute for National Security Studies (INSS). By 2016 Iran was spending over $1 billion annually on its cyber capabilities compared with the $2 billion by the United Kingdom, one of the world's leading cyber powers. Iran's cyber budget increased twelvefold between 2013 and 2021.[19]

> **"The number of Iran's cyber operations and their degree of sophistication have grown, and Iran has demonstrated the ability to disrupt, destroy, distort, sabotage, or undermine critical national infrastructure, commercial interests, military capabilities, domestic politics, societal resilience, and international diplomacy. Iran's capabilities will likely continue to improve, both due to its own indigenous capabilities as well as Russian and Chinese assistance."**
>
> — The Institute of National Security Studies[14]

14 Freilich, Chuck. "The Iranian Cyber Threat: The Institutions and Praxis of Iran's Cyber Strategy." *The Institute for National Security Studies | INSS*, Jan. 2024. https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf

15 Lewis, James. "Iran and Cyber Power." Center for Strategic & International Studies | CSIS, 25 June 2019, www.csis.org/analysis/iran-and-cyber-power

16 "2023 Annual Threat Assessment of the U.S. Intelligence Community." Office of Director of National Intelligence, 8 Mar. 2023, www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3676-2023-annual-threat-assessment-of-the-u-s-intelligence-community

17 Lewis, James. "Iran and Cyber Power." *Center for Strategic & International Studies | CSIS*, 25 June 2019, www.csis.org/analysis/iran-and-cyber-power

18 Freilich, Chuck. "The Iranian Cyber Threat: The Institutions and Praxis of Iran's Cyber Strategy." *The Institute for National Security Studies | INSS*, Jan. 2024. https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf

19 Freilich, Chuck. "The Iranian Cyber Threat: The Institutions and Praxis of Iran's Cyber Strategy." *The Institute for National Security Studies | INSS*, Jan. 2024. https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf

Objectives

The mission behind Iran's cyberwarfare efforts is to deepen political divisions among adversaries, undermine electoral processes, cause business and social disruption, and conduct espionage. The Director of U.S. National Intelligence warns that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S, and allied networks and data." Iran has a number of state-sponsored units that run cyberwarfare operations and manage groups of threat actors, including:

- **The Iranian Revolutionary Guard Corps (IRGC)** targets U.S. interests, Israeli critical infrastructure, Saudi Arabia, and other Gulf states. The unit also provides operational direction and support for the cyber operations of Iranian proxies.
- **Basij** is a civilian paramilitary organization composed of 120,000 cyber warfare volunteers and controlled by the IRGC. The unit leverages connections to universities and religious schools to recruit a proxy hacker force, and it also outsources cyberattacks to sympathetic hacktivist groups.
- **Other units** include the:
  - Passive Defense Organization (NPDO)
  - Ministry of Intelligence and Security (MOIS)
  - Intelligence Group 13

Iran also leverages proxies to support and mask its efforts including Hezbollah, Hamas, and several hacktivist groups.

Notable attacks

"Abadil" DDoS attacks on major American banks

In September 2012, Iranian hackers linked to the Islamic Revolutionary Guard Corps conducted a coordinated denial of service cyberattack on the websites of Bank of America, JPMorganChase, Wells Fargo, and 43 other U.S. financial institutions, resulting in simultaneous outages. Attackers flooded bank servers with junk traffic, which prevented customers from accessing online banking services. It is believed that the attack was in response to U.S. imposed economic sanctions to counter Iran's nuclear program.[20]

"Shamoon" attack on Saudi Arabia's national oil company

In 2012, Saudi Aramco, one of the world's largest oil companies, suffered an enormous cyberattack by suspected Iranian state-sponsored hackers in response to Aramco's support of the Al Saud royal family's authoritarian regime. Initially gaining access to the company's infrastructure via a single phishing email, the attackers used Shamoon malware to wipe out or partially destroy 35,000 computers within just a few hours. Aramco was relegated to managing supplies, shipping, and contracts with governments and business partners using faxes and typewriters. After weeks, the organization temporarily ceased selling oil to domestic gas tank trucks and began giving away free oil to keep it flowing within Saudi Arabia.[21]

20 "Connect the Dots on State-Sponsored Cyber Incidents - Denial of Service Attacks against U.S. Banks in 2012–2013." *Council on Foreign Relations*, Sept. 2012, www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

21 Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." *The New York Times*, 23 Oct. 2012, www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Notable attacks, continued

Attack on New York City's Bowman Avenue Dam

In 2015, an Iranian hacktivist group claimed responsibility for a 2013 cyberattack on a New York city dam. The hackers gained access to the control system for the Bowman Avenue Dam in the suburbs of New York city, accessing and reading files that included usernames and passwords. The hackers claimed they didn't come forward sooner because of "a 'state-level' warning not to go public with it 'for the greater good.'" Experts believe the hackers gained access through a system that was either misconfigured or outdated.[22]

Destructive cyberattack on the Sands Casino

In 2015, Iranian state-sponsored hackers used malware to infiltrate servers owned by the Sands' Casino in Las Vegas. The hackers targeted the Casino for its CEO's support for Israel and condemnation of the Iranian regime. The attackers wiped out more than $40 million in equipment and data and stole private employee information including names, titles, Social Security numbers, and e-mail addresses.[23]

Dustman malware attacks on Bahrain government agencies and critical infrastructure

In 2019, Iranian-sponsored hackers used Dustman malware to attack several of Bahrain's government departments and critical infrastructure, including Bahrain's National Security Agency, the Ministry of Interior, the First Deputy Prime Minister's Office, the Electricity and Water Authority, and Aluminum Bahrain, one of the world's biggest smelters. Because Bahrain is the regional home for the U.S. Navy's Fifth Fleet and Central Command, experts believe the attacks were likely a message for the U.S. Developed by Iran, this was the country's first attack using the Dustman data wiping program. The Bahrainis did eventually detect and stop the malware, but not before it caused significant damage.[24]

Dustman malware attacks on U.S. websites in response to Suleimani's assassination

In 2020, two Iranian hackers infected 51 websites in the United States with Dustman malware in response to the U.S. assassination of General Suleimani–Iran's most powerful security and intelligence commander and longtime head of the Islamic Revolutionary Guards Corps' Quds Force. The hacked websites were used as tools of protest, showing pictures of General Suleimani against an Iranian flag and displaying anti-American messages.

Attacks focused on disrupting U.S. elections

To undermine the 2020 U.S. elections, two Iranian hackers sent threatening and false messages to thousands of people after breaking into voter registration systems and a media company. Targeting both democrats and republicans, the messages used dis- and misinformation to evoke and spread feelings of fear, chaos, paranoia, and hate across Americans. Investigations linked the hackers' efforts to Tehran's government ministries.

22 Connor, Tracy, et al. "Iranian Hackers Claim Cyber Attack on New York Dam." *NBC News*, 23 Dec. 2015, www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611

23 Elgin , Ben, and Michael Riley. "Now at the Sands Casino: An Iranian Hacker in Every Server." *Bloomberg*, 12 Dec. 2014, www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas

24 Hope, Bradley, et al. "High-Level Cyber Intrusions Hit Bahrain amid Tensions with Iran." *The Wall Street Journal*, 7 Aug. 2019, www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488

THE POWER OF NETWORK VISIBILITY IN DETECTING NATION-STATE ATTACKS

With the ExtraHop RevealX NDR Platform, IT and security teams can triage more efficiently, mitigate issues quickly, and keep operations running smoothly, resulting in a

193% ROI.[25]

Residential proxies, protocol tunneling, communication via encrypted channels, application layer protocols, non-application layer protocols, non-standard ports. These are all highly sophisticated, network-based techniques that nation-state actors use to gain access to systems, hide in network traffic, evade endpoint- and log-based detection and response solutions, and appear less suspicious to security teams.

The ExtraHop RevealX network detection and response platform detects all of those techniques–and more–by monitoring, analyzing, and decrypting encrypted North-South and East-West network traffic to identify suspicious behavior on the network in real time, without impacting performance. ExtraHop leverages the industry-standard MITRE ATT&CK Matrix for Enterprise to operationalize RevealX workflows. Providing coverage for 92% of attack techniques deemed network-addressable by MITRE ATT&CK, RevealX fills visibility gaps and provides investigative coverage right out of the box for 126 techniques across 12 of the 14 MITRE ATT&CK framework tactics.[26]

RevealX was designed to maximize its coverage of network-addressable threats and attacks even beyond what's defined by the MITRE ATT&CK framework. Providing complete visibility into your network, RevealX helps to expose every step an intruder takes, giving you the opportunity to quickly investigate and stop them as they attempt to maneuver through your network infrastructure.

In the current geopolitical climate, cybersecurity is national security. ExtraHop is here to help. To learn more about how the ReveaX NDR platform can help you detect and respond to nation-state sponsored threats, watch a demo.

25 https://hop.extrahop.com/resources/papers/forrester-tei-study-2023/

26 "MITRE ATT&CK - Network Detection & Response with RevealX." ExtraHop, 2024, www.extrahop.com/resources/papers/revealx-mitre-framework. Accessed 25 July 2024

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com