ORION FORUM

A Need for Informed Policy Against Critical Cyberattacks: The ROCCA Project

JULY 13, 2026

According to data from the Orion Policy Institute's newly launched Records of Critical Cyber Attacks (ROCCA) Project, China and Russia account for 458 originated cyberattacks, or 48% of the 954 incidents recorded between 2005 and 2025. The United States is the most targeted country, and these attacks have increased sharply since 2017. ROCCA data also show that phishing and social engineering, ransomware, and cyberespionage (e.g., credential attacks) are the three most frequent attack types that state and non-state actors have engaged in during the same period.

As cyberattacks become more sophisticated and widespread, with social, political, economic, and psychological implications, the need for informed policy decisions grows more urgent. To respond effectively to the evolving challenges posed by state and non-state APT actors, data-driven policies are essential. The ROCCA project is designed to help fill this gap. ***ROCCA*** is a structured, open-source database that systematically records critical cyber incidents conducted by state and non-state actors.

Critical cyber-attacks are no longer a matter of preference or immediate operational necessity; rather, they have become an embedded state operation, like any other traditional, conventional, or non-conventional political, military, economic, and strategic operation. As part of long-term cyberwarfare, or simultaneously with kinetic warfare, critical cyberattacks enable nation-states and non-state actors to advance and achieve political, economic, and military objectives. State-linked Advanced Persistent Threat (APT) actors, state-sponsored groups, crime-as-a-service organized cybercriminal groups, and politically motivated non-state actors

pose one of the most serious national security risks to nation-states, public and private entities, and society at large.

Among many others, China-based APT41, Salt Typhoon, Volt Typhoon, and Flax Typhoon; Iran-affiliated and Iranian-sponsored APTs such as CyberAv3ngers, APT34, and Handala (a.k.a. Void Manticore); Russian Foreign Intelligence Service (SVR) APT29 (also known as the Dukes, and CozyBear); Russian FSB APTs like SEABORGIUM; Russian General Staff Main Intelligence Directorate (GRU); and Russia-sponsored APT 28 are examples of major state-linked and state-sponsored groups actively targeting the United States and its allies. These groups engage in cyberespionage, disruptive and destructive cyberattacks, hacking, doxing, disinformation and misinformation campaigns, and digital transnational repression. Their operations often involve long-term intrusions into critical infrastructure, intelligence collection, and the theft of intellectual property. However, the objectives of today's APTs go beyond these activities, often prioritizing surveillance, infiltration, and the exploitation of information to advance the malign actor's national interests.

During the US-Israel and Iran war, the hacker group Handala, linked to the Islamic Republic of Iran's Ministry of Intelligence and Security (MOIS), claimed responsibility for a cyberattack on March 11, 2026, targeting a Michigan-based medical device maker, Stryker Corp. The incident disrupted the company's order processing, manufacturing, and shipping services. Widely described as the first destructive wiper attack claimed against a US Fortune 500 company, the incident materially affected Stryker's first-quarter earnings, and the FBI subsequently seized Handala's leak-site domains. While the Iranian regime's cyberwarfare capabilities are limited compared to those of other state actors, including China, Russia, and North Korea, the Stryker attack demonstrates the adversary's reach through cyberattacks. These nation-state actors, however, have engaged in more advanced and sophisticated critical cyberattacks, ranging from utilizing "traditional cyberattacks to living-off-the-land [a type of attacks that "blend seamlessly with normal administrative operations], making detection almost impossible without sophisticated behavioral analysis." In recent years, China-based APT actors, such as Volt Typhoon, have engaged in living-off-the-land type of attacks – a technique in which the cybercriminal uses legitimate tools within the victim's system- to target the US critical

infrastructure "to find information on the system, discover additional devices on the network, and exfiltrate data." Similarly, Russia-linked groups have carried out several sophisticated cyber operations, including targeting critical infrastructure, political parties, elections, and politicians; engaging in misinformation and disinformation campaigns; and conducting cyberespionage in the US and European countries. North Korea's cyber operations mainly focus on revenue-generating cyberattacks, including global supply chain attacks, cryptocurrency theft, "launching of ransomware campaigns against Healthcare and Public Health Sector (HPH)" organizations, and other critical infrastructure in the US.

Given the complexity of the actors and targets involved, the sophistication of the tactics used, the pace of technological evolution, and the complexity of response options, informed policy frameworks are now essential. Attribution is one of the most challenging aspects of data collection on critical cyber-attacks because, while nation-states engage in such attacks, they more often rely on non-state proxies, such as organized cybercriminals. Even if government employees are involved, it is complex to link them to a particular attack.

To help policymakers and practitioners navigate this complex environment, the ROCCA project aims to provide a timely track of critical cyber-attacks and inform a wide range of actors, including policy makers, the national security and intelligence community, cybersecurity professionals, critical infrastructure operators from public and private sectors, researchers and scholars from universities, think tanks, and research centers, as well as the media and society at large. Unlike general cyber incident datasets, ROCCA focuses exclusively on incidents planned to produce significant societal, political, or economic impact. These include strategic cyberattacks and operations, disruptive and destructive attacks targeting critical infrastructure, and cyber operations linked to geopolitical competition, conflict, or financially or politically motivated non-state actors. The dataset covers incidents from 2005 onward and is continuously updated. It is designed to support quantitative and qualitative policy analysis, attribution research, and geopolitical risk modeling.

It is especially important to provide policymakers with up-to-date data on cyberattack patterns, systematic briefs on APT actor profiles, and refined, feasible policy analysis. ROCCA will also be beneficial for national security professionals and the intelligence community. While they have

greater access to such information, the ROCCA project will serve as an additional open-source database, helping them track critical cyber incidents, APT actors, and patterns in targets and tactics, and analyze the malign activities and strategic objectives of state and non-state actors.

Cybersecurity professionals and critical infrastructure operators from the public and private sectors would also use the ROCCA project outcomes to analyze and compare cyberattack patterns, understand sector-specific threats, and make informed decisions about risk mitigation, incident response, and long-term planning.

Last but not least, the ROCCA project will help researchers and scholars access open-source data and analysis for their own research. Moreover, the media and the broader public will have a better understanding of the critical cyberattacks. In doing so, ROCCA will also support broader efforts to raise public awareness about these attacks.

In a period when critical cyberattacks have become integral to the strategic and tactical arsenals of state and non-state actors, evidence-based policy is even more pressing. ROCCA aims to help fill the gap by providing robust analysis through an open-source database that systematically records critical cyber incidents carried out by state and non-state actors and supports informed policy responses.
