

Melding of State and Criminal Threat Actor Motivation: The Nebulous Normal

TLP:WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.





Key Judgements

- Nation-state threat actors have been observed empowering local cybercriminal outfits to further geopolitical objectives.
- A shadow industry of offensive cyber tooling research and development companies has emerged, widening the R&D capabilities for state-sponsored cyber espionage groups.
- Relationships between intelligence agencies and ransomware actors may be present, increasing the sophistication of financially driven cybercrime gangs.
- Criminal elements offer plausible deniability to state-sponsored groups and may be used as proxies to launch nation-state attacks.
- Forward-facing intelligence consumption is essential to the success of organizations trying to navigate the opaque threat landscape.

Introduction

As the fusion of espionage, hacktivism, and financially-motivated crimes continue to meld together, there are a number of reasons for this trajectory, and many are dependent on the society in which the cybercrime originates.

From the perspective of the state, having a large roster of cyber specialists to call upon, but not to have to pay to maintain this resource when not involved in directed action to benefit the state, is a money-saving bonus - especially when the state might be facing Western sanctions and moving money into the country is harder than it once was.

The state can hire criminal operators on a case-by-case basis, or perhaps instead purchase the malicious software they produce, or co-opt their capabilities for a promise to look the other way as they conduct nefarious online activity. The state also retains a level of deniability if attacks are attributed to its agents.

In the case of hacktivism, states can create fake groups or sponsor authentic hacktivist groups to launch attacks under the guise of empowered civilians. In the case of creating fake groups, this tactic has been called fakativism and it seeks to accomplish two major objectives. First as a psychological tool. By creating a fake movement, legitimate hacktivists and non-technical civilians may become inspired to join a cause sympathetic to the country that created the group. Second as a proxy for nation-state attacks. The created group will have access to more advanced tooling, being able to launch more impactful and sophisticated attacks while maintaining plausible deniability.¹

1. <https://www.ibm.com/think/topics/quantum-computing>



Groups have also been known to migrate between categories: The Killnet group started out a band of Russian hacktivists offering DDoS for hire services, before making the switch to becoming a ransomware gang.²

Russia

Russian Ransomware Gangs

When it comes to cybercrime, Russia is a world leader and is home to many ransomware gangs. The gangs are organized groups of cybercriminals that launch attacks against victims, where sensitive data is encrypted and only the payment of a ransom, usually in the form of cryptocurrency, will lead to decryption of the data. In recent years, this technique has extended to extorting victim organizations to pay, or face the public dumping of stolen data. Unfortunately, this particular type of cybercrime can be quite lucrative, drawing in significant amounts of money into the Russian economy. It is moderately likely that Russian decision-makers turn a blind eye to this behavior in exchange for ransomware gangs following certain rules of engagement due to the money it brings in.

In a 2024 threat intelligence report on the Russian-speaking ransomware gang QiLin, a recruitment ad to join the group specified that the gang was not allowed to target organizations in Commonwealth of Independent States (CIS) countries. The CIS is a group of countries in Eurasia that are geopolitically aligned with Russia, and were typically part of the former Soviet Union.³

In order to gain a level of protection, gangs adhere to a set of tacit expectations to stay in the Kremlin's good graces: Do not work against the Russian national interest or take from local businesses, but stealing from geopolitical rivals is encouraged.

According to the news outlet Associated Press, a conversation taking place on a Russian-speaking dark web forum had alleged ransomware gang members admonishing a peer that had just suffered from Western authorities seizing infrastructure, as the servers could have been moved inside Russia to stay beyond the reach of American and European authorities.

"Mother Russia will help," a forum member wrote. "Love your country and nothing will happen to you."⁴

There is significant evidence to suggest that this is the case. In 2021, the US Treasury released a sanctions package against Russia targeting Russian malicious cyber actors. In the package, the US Treasury discussed how Russian intelligence agencies – the Federal Security Service (FSB), Russia's Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR) – use malicious cyber activity to disrupt and support strategic objectives.

2. <https://intel471.com/blog/pro-russian-hackivism-shifting-alliances-new-groups-and-risks>

3. https://blackpointcyber.com/wp-content/uploads/2024/08/Qilin-Ransomware-Threat-Profile_Adversary-Pursuit-Group-Blackpoint-Cyber_2024Q3.pdf

4. https://apnews.com/article/business-technology-general-news-government-and-politics_c9dab7eb3841be45dff2d93ed3102999



Furthermore, the sanction announcement included the cooperation and bolstering of criminal elements to further offensive intelligence operations. Specifically, this activity was attributed to the FSB, where it was reported that they actively “cultivate and co-opt criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns.”⁵

Russian APT44

Moscow has used ransomware gang software to support its offensive kinetic objectives, as shown by Russian military intelligence-linked APT44 (also named Sandworm) using malware from cybercriminal organisations upon Russia's invasion of Ukraine.⁶ Google has said it believes Russian cyber espionage groups made the switch to using free or publicly available tooling due to resource constraints, seeking to hamper any efforts to attribute the attacks to the Russian state, and in the case that a campaign is discovered, it is the cybercrime gang's malware and access that is burned, not malware and access developed by the state.

"The group has used criminally sourced tools and infrastructure as a source of disposable capabilities that can be operationalised on short notice without immediate links to its past operations," Google wrote.

More recently, Mart Noorma, director of the NATO Cooperative Cyber Defense Center of Excellence located in Tallinn, Estonia said as well as attempting to sow chaos, that Russian hackers were also interested in money.⁷

"By supporting hacker groups, the state can more easily create confusion. Then the state is not directly connected. Creating chaos has been a constant for Russia – their goal is to achieve geopolitical and cognitive effects so that people in democratic countries begin to doubt their values and governments," Noorma said.

"Quite often, Russian hackers also have financial motives – the proceeds are divided among state agencies."

North Korea

Taken to its most extreme example, North Korea directly funds its economy with cybercrime, hence its focus on cryptocurrencies and the infrastructure to support them. This is largely due to the absence of legitimate revenue streams and international trade partners. As a result, many state-sponsored cyber operations are financially motivated, which deviates significantly from the cyber espionage operations conducted to further the geopolitical agendas of China, Russia and Iran.

5. <https://home.treasury.gov/news/press-releases/jy0127>

6. <https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat>

7. <https://news.err.ee/1609687160/russian-hackers-are-interested-in-chaos-and-money-says-nato-ccdcoe-director>





In an example of digital asset theft in 2022, the cryptocurrency gaming platform Axie Infinity was attacked by North Korean nation-state threat actors, resulting in the theft of nearly \$620 million after the threat actors gained access to the company's network through spearphishing. The FBI was able to attribute the attack to the North Korean nation-state activity cluster referred to as the Lazarus Group or APT38.⁸

There is certainly something to be said for ignoring piecemeal and sporadic returns from ransomware that might have multiple millions of dollars in a single payment on a good day, when instead, a hack of a crypto exchange can add an extra set of zeroes and be measured in the billions.⁹ Three years after its Axie Infinity theft, Lazarus Group managed to make off with \$1.5 billion from crypto exchange ByBit, and was able to convert \$300 million of its cryptocurrency haul into cash within two weeks.

This was far from the first time the DPRK attempted to complete a hack that could be measured in billions, with the nation's hackers behind the 2015-2016 attack on the SWIFT banking network that saw North Korea gain \$100 million.

In a twist on the overlapping motivations of espionage and financial gain, North Korean actor Kimsuky, also known as APT43, focuses on collecting intelligence, but also dabbles in cryptocurrency theft in order to fund itself and purchase operational infrastructure.¹¹

In the later parts of 2024 and persisting into 2025, a campaign mass-targeting remote worker positions in the US and EU has been identified. This campaign, determined to be originating in North Korea, is using a sophisticated network of fraudsters and fabricated identities to obtain employment in organizations based in the US and EU. These operators then attempt to extort their employer for money, or send the vast majority of their salary to fund North Korean weapons development programs. DPRK operators involved in these scams often work in laptop farms or other centralized locations that force them to work long grueling hours with little compensation.

The compensation structure adds an additional motivation to operators in the network of fake IT workers, the well-being of them and their families. In North Korea, average citizens are subject to extreme poverty with extremely low wages for the work they perform. These criminal schemes that fund the nuclear weapons programs of North Korea are often the only way these espionage operators can feed themselves and their families.¹²

8. <https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/>

9. <https://www.bbc.com/news/articles/c2kgndwwd7lo>

10. <https://www.bbc.com/news/stories-57520169>

11. <https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat>

12. <https://www.dtexsystems.com/exposing-dprk/>



Iran

Iran is notable for its targeting of critical infrastructure systems through nation-state activities and by sponsoring hacktivist groups, making attribution difficult for threat intelligence analysts.

An example of this dynamic is the Iranian hacktivist group CyberAv3ngers, which is suspected to be associated with the Iranian military. The group has a reputation for targeting critical infrastructure. In a particularly severe attack at the end of 2023, the group targeted the programmable logic controllers (PLCs) inside US water treatment facilities because they were manufactured by Unitronics, an Israeli technology company.¹³

During the recent Israel-Iran conflagration, over 100 different hacktivist groups rushed to Iran's side with cyber attacks on Israel or declarations of support. After the United States entered the conflict, it too became a target.¹⁴

The pattern for this activity followed the typical hacktivist cycle: An initial explosion of activity, a brief plateau, a secondary surge lower than the initial burst, and rapid decline.¹⁵

Typically these attacks have been unsophisticated and consisted predominantly of DDoS attacks, website defacements, and claiming data breaches against government and military organisations.¹⁶

However, recent reporting has said that Iranian nation-state actors have been providing tooling, techniques, and resources to hacktivist groups. It is something that Tehran does to avoid what would be termed a conventional cyber war.¹⁷

"This is very Russian in nature," Alexander Leslie, a threat intelligence analyst at Recorded Future, told Axios. "Using proxies for plausible deniability is essentially the essence of how they can scale these operations and remain resilient to any kind of disruption."

For the cybercrime aspect, particularly in nations less rich than the Anglosphere – namely the United States, Canada, Australia, New Zealand, and the United Kingdom – moonlighting to conduct cybercrime operations is a way to supplement operator income, as well as lower costs for the nation state.¹⁸

The best example of this arrangement is the Iranian-based threat actor known as hidehacker, who in 2020, worked as part of APT34 by day, and a cybercriminal at night, because Tehran did not give him a good enough salary. To address his fiscal complaints, hidehacker sold information from government-linked work, and most of the information was from targets of Iran.¹⁹

13. <https://www.sentinelone.com/blog/iran-backed-cyber-av3ngers-escalates-campaigns-against-u-s-critical-infrastructure/>

14. <https://cyberknow.substack.com/p/iran-israel-war-cyber-tracker>

15. <https://www.group-ib.com/blog/middle-east-cyber-escalation/>

16. <https://www.cloudsek.com/blog/part-1-the-iran-israel-cyber-standoff—the-hacktivist-front>

17. <https://www.axios.com/2025/07/01/iran-hacktivist-israeli-us-strikes>

18. <https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat>

19. <https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat>



China

When the United States gets a new administration, espionage from Beijing typically spikes, and it is reported that Chinese government actors have currently doubled the number of attacks since 2023.²⁰

“The US is absolutely facing the most serious Chinese hacking ever,” SentinelOne China expert Dakota Cary told The Washington Post.

“We are in China’s golden age of hacking.”

Traditionally, Chinese state actors selected and broke into targets themselves, however private industry has recently been emboldened to hack Western companies and sell initial access back to Beijing. This has resulted in the number of Western companies impacted by Chinese state-adjacent hacking ballooning, even if they are of no interest to China. In particular, Beijing is interested in hacking software and security vendors to access many victims at once.

The Washington Post reported that Chinese actors have perfected the ability to move through networks of compromised US devices, so that the final leg to a target appears as domestic US traffic, forging the ability of the NSA to look into the communications.

In China, private industries are all required to help pursue state objectives. This means that the services of various institutions can be called upon to conduct or support espionage activities. China enacted its National Intelligence Law²¹ in 2017, and requires organizations and citizens in the Middle Kingdom to help with national intelligence efforts and protect any national intelligence work secrets they may be aware of. It effectively compels Chinese commercial entities or citizens to provide assistance to national intelligence operations when called upon. As a result, there is a large private industrial base that supports Chinese intelligence activities in the form of contract work.

While this dynamic was known to Western security researchers, the true scope of involvement of private industries was brought to light when internal documents leaked from a Shanghai-based offensive cyber operations contractor I-Soon in 2024. The documents revealed the firm was working with national intelligence agencies like the Ministry for State Security, and the Ministry of Public Security. Furthermore, the leak highlighted the size of the private market for cyber espionage contractors.

I-Soon and similar contractors are likely supporting cyber espionage in a major way, highlighting the intersection between state entities and private contractors. In that same vein, there was evidence in the leak that linked I-Soon command and control (C2) infrastructure and tooling to known Chinese nation-state activity group clusters.²²

20. <https://www.washingtonpost.com/technology/2025/07/16/china-hacking-us-targets/>

21. <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>

22. <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/>



A particular speciality of China that involves a level of crossover between state interests and cybercrime activity has been intellectual property theft, an activity that is often directed by the state.

In 2020, the US Department of Justice indicted two Chinese nationals on charges that included intellectual property theft on eight targets, and additionally looking to extort cryptocurrency out of a victim by threatening to release the stolen source code.

"China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals being 'on call' to work for the benefit of the state," then-US Assistant Attorney General for National Security John C. Demers said at the time.²³

"Cybercrimes directed by the Chinese government's intelligence services not only threaten the United States but also every other country that supports fair play, international norms, and the rule of law, and it also seriously undermines China's desire to become a respected leader in world affairs."

Instead of utilising cybercrime tooling for nation-state activity, Chinese actor APT41 goes in the other direction and has been observed using espionage tooling and non-public malware in its cybercrime operations.²⁴

It is speculated that the group's targeting of the video game industry -- where its techniques have included supply chain compromises to software updates, bootkits, and compromised digital certificates -- have helped it develop tools and techniques that are later used in its espionage operations.

Taken at a high level, while Western and other nations with strong adherence to the rule of law may choose to delineate between cyber activities that benefit the state or benefit the individual, the nations opposed certainly do not.

Key Societal Drivers

In its May 2025 takedown of DanaBot infrastructure, the US Department of Justice (DoJ) said the group behind the malware offered one variant for cybercrime, and another with its own infrastructure for espionage that would send data back to Russia.²⁵

Security firm Intel471 said at the time of the takedown that Russia allows professional cybercriminals to operate on the proviso that actors focus their activities on targets outside of Russia and the former Soviet republics, and that they will help Russian intelligence when asked.

23. <https://www.justice.gov/archives/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>

24. <https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>

25. <https://www.justice.gov/usao-cdca/media/1401356/dl?inline>





"The foundation for these relationships is institutionalised corruption," Intel471 said.²⁶

"Where the state – which has the power to conduct raids, audits, and other forms of harassment – can coerce cybercriminal actors into paying protection money, participating in state-directed cyber operations such as espionage or data theft, and supporting state narratives through hacktivist or misinformation campaigns."

Whether it is obfuscation of activities, seeking to confuse anyone trying to attribute a campaign, letting the operators have a little fun and boost their income after hours, or even directly funding the state and its agencies, it is clear that the cyber adversaries of the West choose not to make the same separation between individual and state activities.

At the core of nation-state cooperation with non-state elements lies the idea that expanding the pool of available resources to partake in offensive cyber operations is likely viewed as a force multiplier for existing geopolitical objectives.

Pertaining to cybercrime, enabling criminal activity may be considered a force multiplier when attempting to destabilize adversarial nations and sow chaos. This tactic is observed in Russian ransomware safe harboring, Iranian fakativism, and tool sharing between state and non-state actors to increase non-state capabilities. In the case of North Korea, full-scale funding of criminal activity using state-sponsored teams to launch financially motivated attacks to fund weapons programs represents a key driver for Kim Jong Un's regime.

Outside of criminal activity, the mission to expand the resource pool can lead to a thriving offensive cyber operations industrial base comprising of private contractors. In places like China and Russia, there exist thriving markets of private-sector offensive security contractors. These organizations create tools and provide specialized knowledge when needed, allowing nation-state elements to expand their capabilities through outsourcing. In China, the company I-Soon created custom malware and C2 infrastructure for use by the Chinese government in an offensive capacity. Similarly, the Russian company Pasit provides research and development (R&D) to create new technologies that directly bolster the cyber operations of the SVR. In both instances, there are entire shadow industries built around cyber-espionage contracting.

It is also clear that adversarial states have benefitted, and continue to benefit from the lack of differentiation between state and criminal activities, otherwise they would not have continued doing it for decades without changing it up.

For defenders against these actors, the writing is on the wall. A common trope in cyber defence is that nation-state actors will not target me because I do not have information that state actors are interested in. However, that may simply mean you are not targeted during work hours, and could be ripe for the picking by an after-hours moonlight operator.

Just because you are not interested in defending against state actors does not mean that state actors are not interested in you.

²⁶. <https://intel471.com/blog/danabot-malware-disrupted-threat-actors-named>



Mitigations

When it comes to defense strategies, hacktivism may be the most straightforward. In a report released by Forescout analyzing hacktivist attacks in 2024, it was found that nearly 89% of attacks launched by these groups were distributed denial of service (DDoS) attacks designed to overload servers with large amounts of traffic.²⁷ These attacks can be mitigated by installing web traffic filters aimed at thwarting large numbers of requests. To learn more about this attack, please read the Health-ISAC DDoS White Paper [here](#).

In general, taking a set of foundational defensive steps can go some way to improving cyber posture. These actions include ensuring that all devices – be it servers, laptops, firewalls, routers, IoT devices, VPN appliances – are promptly patched when updates are released; enabling multifactor authentication, preferably using time-based or one-time codes, wherever possible; and using a password manager to provide unique, complex passwords for each service.

With each group and country tending to have different tactics, techniques, and procedures (TTPs), participating in information-sharing channels is vital to staying abreast of the latest trends and attack vectors.

Additionally those responsible for organisational cybersecurity, such as chief information security officers, should ensure that foundational strategic controls are also in place. This includes having a proper backup regime in place and ensuring the restoration process is regularly tested, having an incident response and business continuity plan in place should a threat actor be detected on the organisation's network, having a full asset inventory to allow patching and detection to cover all endpoints, and conducting regular risk assessments to record where gaps exist and if progress is being made.

As an organisation's cyber posture matures, it can adopt further strategies to reduce attack surfaces. These include application allowlisting; blocking Microsoft Office macros and internet advertising; introducing network segmentation; and ensuring users have the lowest level of privilege required to perform their duties. With controls such as these in place, should an intrusion occur, the impact of the event and the reduction in lateral movement will go some way to preventing catastrophic consequences.

27. <https://www.forescout.com/resources/the-rise-of-state-sponsored-hacktivism/>



Conclusion

Nation-state, hacktivists, and cybercriminals used to have three distinct types of attacks and motivations. However, as the world transitions to a new normal of asymmetric hybrid warfare in which hacktivist groups and cybercriminals can benefit the nations that are supposed to prosecute them, attacks become much harder to predict. This can make threat modeling an arduous task for defenders and cybersecurity teams.

Therefore, consuming forward-facing intelligence and participating in information-sharing communities can help organizations keep abreast of the emerging security threats. Proactive security measures are especially important now as threat actor characteristics continue to meld together and create an opaque threat environment.

By joining and actively participating in your information-sharing communities, you gain:

- **Foresight:** Early warnings about emerging threats and proven mitigation strategies from your peers.
- **Expertise:** Crowdsourced knowledge from industry veterans to strengthen your defenses and elevate your team's skills.
- **Resilience:** Collaborative trust to navigate evolving threats with confidence and maintain a secure, reliable network.
- **Innovation:** Shared insights that fuel cutting-edge cybersecurity solutions for a safer future of healthcare.

