SWP Comment
NO. 30 JUNE 2025

Hand and Glove: How Authoritarian Cyber Operations Leverage Non-state Capabilities

An Integrated Understanding of Both Is Required to Recalibrate Political and Legal Responses

Jakob Bund

Authoritarian states are increasingly leveraging non-state cyber capabilities to expand their operational reach, thereby challenging conventional distinctions between state and non-state activity. This practice complicates attribution and presents obstacles for coordinated international responses. Moreover, as cyber threats become more complex and entangled, effective countermeasures necessitate enhanced information sharing, trusted partnerships and the development of response tools that function independently of political attribution.

Historically, Western assessments of cyber threats have concentrated on state adversaries. More than 600 state-backed groups are tracked globally. Yet, for more than a decade, Western analyses and discussions of cyber threat concerns have focused mainly on four states: China, Iran, Russia and North Korea. Based on open-source reporting evaluated by the European Repository of Cyber Incidents (EuRepoC), these countries account for more than 70 per cent of the state-backed threats that Europe and its partners have faced since 2000.

The focus on a subset of states is due to high activity levels and national security implications related to intellectual property protection, state secrets and the resilience of critical services. However, state-nexus operations account for just 29 per cent of the operations recorded by EuRepoC. That figure highlights concerns about a "fetishisation" of state-sponsored groups (advanced persistent threats or APTs), whereby the practice among criminal groups and hacktivists of pursuing similar targets for the purpose of extortion or disruption is overlooked.

Critically, in the current climate of heightened geopolitical tension, the operational divide between state and non-state actors shows signs of collapsing, as states seek to assert control over cyber capabilities both inside and outside their borders. A closer examination of EuRepoC data underscores the need for a more integrated understanding in the analysis of state and

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

non-state actor threats. These trend lines are particularly pronounced in the case of the authoritarian states that have been dominating Western threat perceptions, drawing attention to the reinforcement that long-standing nation state threats derive from non-state capabilities. Russia, China and North Korea have developed their own distinct approaches. While Russia has provided sanctuary for criminal groups, China's state programmes have served to accelerate the emergence of a domestic hacking industry. Charting its own path, North Korea has sought to create bridgeheads extraterritorially for its operators.

Not least, it is effective state responses to the threats enabled by this co-optation of capabilities that are predicated on an integrated understanding of the role non-state assets play in these models. To ensure that the toolkit of responses developed by the EU and its partners remains fit for purpose, an expanded threat assessment is needed. The key components are a differentiated assessment of i) the favourable conditions created by authoritarian actors to draw non-state capabilities into their sphere of influence and ii) the measures taken to bring those capabilities under state control.

Russia: The safe haven blueprint

Russian cyber criminals make up nearly half of the most wanted list published by Germany's Federal Criminal Police Office (BKA). That list typically includes individuals accused of high-profile crimes, such as members of the far-left terrorist organisation RAF, those who collaborated in the 9/11 attacks and individuals such as Jan Marsalek, the former chief operating officer of the now bankrupt payment processor Wirecard. The BKA list has had a notable success rate. Close to 70 per cent of suspects included on it since 1999 were arrested. However, in the case of the twenty-six people included on the list because of suspected links to the Russian criminal underground, there is little expectation of any breakthrough, despite German law enforcement and its international partners having collected a wealth of information on those individuals.

The reason for this is the nature of the relationship that Russia's security agencies have fostered with local cybercrime groups, which can best be understood as a social contract. Criminal groups are allowed to operate unencumbered from Russian law enforcement and are also shielded from prosecution or extradition. In exchange, they refrain from pursuing Russian targets and occasionally take on tasks assigned to them by the state authorities, while otherwise steering clear of Russian strategic interests.

In effect, this laissez-faire arrangement gives criminals free rein — as long as they remain within these boundaries. As a result, Russia has turned into a safe haven for a wide range of malicious cyber activities. And this has had a positive side effect from the perspective of the Kremlin: making foreign targets the focus of cyber threats has the potential to generate costs for, and put pressure on, states that Moscow regards as adversaries.

A comparison of EuRepoC data illustrates these dynamics. Of the cyber incidents attributed to Russia as country of origin, only a marginal 3.6 per cent were against targets within Russia itself. For operations launched from China, that share doubles. But in the case of incidents tracked to Western states, the percentage of victims in the country of origin is significantly higher: for the US, it is more than eight times that of Russia and for EU member states it is nearly 14 times (see Figure 1).

Carve-outs for Russian targets can also be observed at the technical level. Malware — such as the Ryuk ransomware, operated by the Trickbot group, which is included on BKA's most wanted list — often scans for language settings and is programmed to delete itself if it believes that it is running on a Russian system.

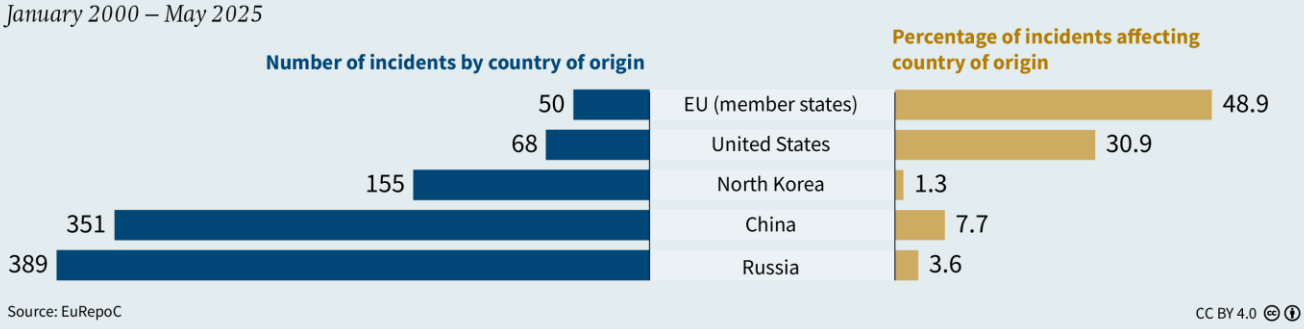
Probing the safe-haven promise

International law enforcement efforts have repeatedly pursued criminals operating from

Figure 1

Total attributed cyber incidents and share affecting country of origin

January 2000 – May 2025



Source: EuRepoC

the perceived safety of Russian territory. In what appeared to be an auspicious case of collaboration with the Russian Federal Security Service (FSB), agents from the FBI and the US Secret Service went to Moscow in 2009 to witness the planned arrest of Roman Seleznev, who had been behind the large-scale online theft of credit card information. Because of his connections, Seleznev was a test case for the safe haven assurances of the Russian authorities: by his own admission, he had secured protection from the cybercrime division of the FSB. After being tipped off by his FSB contacts, Seleznev escaped arrest in 2009; but at the request of the US, he was ultimately apprehended in 2014 while vacationing in the Maldives. He was subsequently sentenced by a US court to twenty-seven years in prison. Having strayed beyond Russia's protection, Seleznev was one of a handful of Russian hackers serving a sentence abroad until his release as part of a prisoner exchange in August 2024.

Since Seleznev's arrest and sentencing, law enforcement actions have evolved to take into account the low likelihood that such successes can be repeated. Operation Endgame, the largest international law-enforcement crackdown on cybercrime to date, has expanded beyond arrest warrants to the dismantling of the tools and attack infrastructure of criminal groups as impact vector. In the second phase of the crackdown, German law enforcement working together with international partners recently issued arrest warrants for twenty actors, mainly Russia-based, who are unlikely to leave their safe haven. Although BKA communications about Operation Endgame prominently cite these arrest warrants, there are different success indicators for taking down criminal infrastructure. Disruptive objectives are measured in metrics such as the number of servers seized and domains shut down during Operation Endgame — 300 and 650, respectively — these being the means with which criminals control intrusion tools and compromise victim systems.

The fact that, in parallel, the US unsealed overlapping indictments against seventeen actors underscores the low probability of the supporting US warrants resulting in arrests. Typically, such charges are kept secret to allow for unsuspecting offenders to be detained — for example, during trips to cooperating jurisdictions, as in the case of Seleznev. The indictments in May 2025 were filed back in 2022 and had not led to any arrests in the interim.

From laissez-faire to state capture

The laissez-faire perspective on safe havens puts the emphasis on the advantages gained by criminal actors. For their part, Russian intelligence services have sought to lean on capabilities and actors operating under their umbrella — either by coercion, through symbiosis or as paying customer.

Criminal groups proclaiming support for the Kremlin following Russia's full-scale invasion of Ukraine has further focused attention on what intelligence services receive in

return for providing sanctuary. Shortly after Trickbot had pledged allegiance in February 2022, leaked internal chats of the group revealed that, at least since the spring of 2021, it had been communicating with the FSB about targeting regime critics. Since then, the war on Ukraine has put significant pressure on the resources of Russia's offensive cyber units, which, in turn, has boosted the relevance of the criminal underground as a comparatively cheap source of assets.

However, reports about FSB efforts to make use of cybercriminals long precede the war. In 2017, the United States indicted Aleksey Belan, a hacker of Latvian and Russian nationality, and his two FSB handlers. The charges brought against these individuals officially documented for the first time the Russian authorities' practice of using cybercriminals.

In early 2014, the FSB approached Belan to break into the system of the technology company Yahoo and obtain credentials for at least 500 million email accounts, including those of journalists and government officials. At the time, Belan had already been on the radar of European law enforcement and had even spent time in custody. Indicted twice (in 2012 and 2013), he was detained in Greece in 2013 on a US arrest warrant. After being released on bail, he managed to flee to Russia. Just two months before he was approached by the FSB in January 2014, Belan had been added to the "Cyber's Most Wanted" list of the FBI. From the perspective of his FSB handlers, neither the criminal charges brought against Belan nor his run-ins with law enforcement posed an obstacle for clandestine operations. On the contrary, Belan's criminal notoriety provided deep cover for the intelligence agents steering the operations.

The responsibilities of the FSB Centre for Information Security — also known as Centre 18 and by its military unit number 64829 — are emblematic of a structural design that facilitates the interlacing of state objectives and criminal activities. Officially, Centre 18 serves as the FSB's cybercrime unit; but the information it collects is also used to identify criminal hackers (such as Aleksey Belan) as possible recruits for agency projects. At the same time, Centre 18 oversees a cyber espionage programme of its own. State-led groups under its direction include Star Blizzard, which, since at least 2019, has been tasked with gathering intelligence on civil society organisations and defence and government targets in NATO countries. Further, it is thought that Centre 18 coordinates the activities of Gamaredon, a cluster of FSB officers in Crimea that have been conducting operations against the authorities and critical infrastructure of Ukraine in support of Russia's occupation of the peninsula.

Appropriation of tools

FSB efforts to co-opt criminal actors, as in the case of Aleksey Belan, are complemented by attempts across the Russian intelligence services to adopt and adapt criminal tools. The bid to blend into the criminal landscape became most evident during the destructive wave of the NotPetya cyberattack in June 2017. Attributed to Unit 74455 of Russia's military intelligence service (GRU), NotPetya leveraged the encryption framework of an existing ransomware tool, while making modifications for uncontrolled propagation with no technical possibility of decryption in order to increase the capacity for causing permanent damage.

A lower-profile attempt at criminal camouflage observed in 2024 for a separate GRU unit relies on access data sourced from underground markets. Tracked as "Void Blizzard", the hacking department of Unit 26165 specialises in the purchase of stolen credentials to infiltrate high-value targets across NATO and EU member states, including foreign and defence ministries, defence companies, technology firms with government clients, political parties and journalists. In the assessment of the Dutch intelligence services AIVD and MIVD, the group's use of criminal resources makes it difficult to distinguish its activities from those of other known Russian actors.

Such tactics have economic ramifications. The state's interest in acquiring or

licencing capabilities, rather than engineering them, generates new market demand. Criminal developers cater directly to this demand with tailored offerings. For example, the Russia-based network behind DanaBot, which is used to steal information and load additional malware onto infected devices, created two versions of its tool. One version, targeted at criminal affiliates, enables the deployment of ransomware or initial access for fraudulent purposes. The other version, designed for espionage, was made available to unidentified threat actors (possibly state actors) who used it to steal confidential communications extracted from military, diplomatic, government and non-government targets. As an additional precaution to preserve exfiltrated information in the event of discovery, data channelled through the espionage pipeline was stored exclusively in Russia.

An expendable and expandable resource

The integration of non-state actors and tools into the offensive cyber programme of the Russian intelligence services stands out as a concerning development against the background of the reported use of "disposable agents" to assist with physical sabotage attempts across Europe. Western security officials in late 2024 revealed that a network of proxies had been recruited by the GRU to carry out the final stages of a plot to plant explosive packages on cargo planes headed for North America. Enlisting such proxies is part of a concerted effort to minimise the loss of intelligence service assets and limit the diplomatic fallout in the event of detection.

Moreover, diversification away from state assets is in keeping with tactics to reduce the risk of detection in the first place. From an operational security perspective, the goal has been to turn a weakness into a strategic advantage. On-demand recruitment and the decentralised organisation of proxies allow for the compartmentalisation of tasks, which means that discovery of one node does not imperil other parts of the network.

Just as the deployment of proxy networks for physical operations aims to offset the travel restrictions in Europe faced by Russian operatives, so the use of criminal assets in cyber operations seeks to overcome limitations by covering digital footprints. Rotating in previously undocumented actors or deploying capabilities associated with non-state groups are part of a concerted attempt to blur the lines of continuity in state-sanctioned activity.

The cyber operations units of Russia's intelligence services have become among the most extensively tracked threat actors since a number of their members and leaders were named in criminal indictments. Because of the close scrutiny to which they are now subject, these groups risk early discovery, which may necessitate the costly redesigning of plans and a slower operational tempo. The use of proxies deliberately expands the landscape of threat actors in order to misdirect investigative efforts. Putting analytic resources under additional strain may delay the uncovering of malicious activities and their strategic objectives.

To ensure situational awareness and the ability to impose costs on malicious actors, the response tools need to be recalibrated to the strategic switch points in the coordination of state and non-state capabilities.

China: Command, control, deny

Unlike Russia, the People's Republic of China (PRC) seeks to seize non-state cyber capabilities through the targeted development of a commercial ecosystem. This approach is part of the three-fold aim to establish command, control and deniability within the PRC cyber portfolio. As regards the first goal, command efforts are designed to secure unconditional authority over high-risk operations entrusted to the military.

Meanwhile, initiatives to strengthen control have centralised the coordination of cyber espionage objectives within the Ministry of State Security (MSS). This arrangement is supported by the legally mandated reporting of vulnerabilities and a network of hack-

ing competitions that channel the findings of vulnerability research into offensive programmes. The MSS 13th Bureau's management of the Chinese National Vulnerability Database ensures near-seamless integration into this vulnerability discovery system.

By outsourcing the processing of high volumes of vulnerability information and the development of exploits, the MSS has helped promote the emergence of a web of competing private companies. In a bid to shore up deniability and frustrate endeavours to establish political and legal responsibility, these contractors are not only tasked with identifying vulnerabilities and developing attack tools but have also become involved in the execution of espionage operations.

Escalation control

The PRC leadership reasserted command over the cyber capabilities of the People's Liberation Army (PLA) as part of two wider restructurings of the armed forces. After an initial reorganisation launched in December 2015 had pooled most cyber capabilities within the Strategic Support Force, a subsequent reform in April 2024 further consolidated technical reconnaissance capabilities across PLA services. Under this revised structure, cyber components have been elevated to a dedicated Cyberspace Force but placed under the direct supervision of the Central Military Commission. In a bid to ensure discipline, the Cyberspace Force centralises control previously dispersed across PLA regional commands. The overall strategic focus of the new Cyberspace Force following the reorganisation is to develop offensive cyber capabilities and plan what could prove highly escalatory operations that put critical infrastructure of target countries at risk.

Risk acceptance

For operations below the threshold of the use of force — especially sustained efforts to collect information on targets of political and economic interest — responsibility has been delegated to the MSS and the contractor model it oversees. This fleet of contractors, managed by "digital quartermasters" that coordinate the assigned tasks, has evolved into an ecosystem of more than 100 companies. The proliferation of actors involved has led to the emergence of complex networks and overlaps in private and state-sponsored activity.

The close cooperation between clusters such as I-Soon, APT27 and Silk Typhoon highlights the difficulty of disentangling operational relationships between contractors and state actors. This applies, in particular, when contractors not only develop tools but actively compromise overseas targets. Part of the business model of contractors is the development of shadow infrastructure by meshing together hijacked network equipment (so-called ORBs) of unwitting organisations in third countries. Channelling operations through ORBs provides state actors with the means to obfuscate their activities.

For the high-confidence identification of state-sanctioned actions, careful parsing is required, as contractors are liable to pursue financially motivated activities on their own accord — for example, by using access points to drop ransomware. These ostensible criminal crossovers may be either deliberate or symptomatic of the clash of divergent (state, company or individual) interests. Threat actors may opportunistically seek to monetise access before they are locked out of compromised systems. Or they may endeavour to misdirect investigative efforts by making the compromise appear to have been financially motivated. Irrespective of whether ransomware deployments are carried out for profit or to avoid detection, the sensitive access the MSS encourages contractors to develop illustrates the risks that such destructive pivots pose. With contractors crowding the operational space, the risks for miscalculations increase.

In April 2020, a security researcher working for the contractor Sichuan Silence used a novel vulnerability to target 81,000 firewalls and break into the organisations protected by those devices. To cover up intrusions, the researcher deployed ransomware when remediation efforts were detected. The

indiscriminate nature of these clean-up attempts has potentially far-reaching consequences. In 2024, the US Treasury noted in a sanctions communication that without preventive measures, the ransomware could have caused the malfunctioning of oil rigs operated by a targeted US energy company, endangering the lives of its employees. This incident highlighted the potential for collateral damage, underscoring the risks that are outsourced to contractors engaged in the development of shadow infrastructure. More critically, the prioritisation of deniability and the disparate risk-evaluation processes across the contractor ecosystem may lead to inadvertent high-risk acceptance by the MSS quartermasters tasked with overseeing that system.

North Korea: Breaking out of isolation

The cyber activities of the Democratic People's Republic of Korea (DPRK) are both a strategic continuation of and operational departure from the political, economic and military self-reliance strongly emphasised in the country's state ideology. While the DPRK is attempting to break out, at least partly, of its self-imposed isolation through its cyber programme — thereby demonstrating the political will and the capability to innovate means of subverting international sanctions — it is also making considerable efforts to leverage non-state capabilities beyond its own borders. Despite its diplomatic isolation, the DPRK has been able to enlist foreign tools and know-how to steal cryptocurrency and use blockchain-based technologies developed by a global decentralised community of engineers to launder funds and thereby support the development of its military capabilities. To generate revenue and alleviate the pressure of sanctions, the DPRK has sought to leverage legitimate platforms and expertise, which become criminally liable — and thus a focus of interest — only when co-opted in this way.

In 2019, Western crypto project developers were invited to a conference in Pyongyang so that the DPRK could gain insights into the various possible means of masking financial transactions and circumventing sanctions. Aware of the potential violation of US restrictions, an Ethereum developer notified the US authorities about his plans to speak at the conference but ultimately ignored FBI warnings not to travel. Upon returning to the US, he was arrested and sentence to more than five years in prison. The FBI also issued an arrest warrant for a British crypto entrepreneur who subsequently sought political asylum in Russia.

Crypto platforms have served not only as a tool but also as a target for DPRK threat actors. A large portion of the US$3 billion DPRK operators are estimated to have raked in between 2017 and 2023 through cyber-enabled theft was stolen from crypto exchanges or other crypto projects. Cyber operation units within the Reconnaissance General Bureau (RGB), the DPRK's main military intelligence agency, are called on to engage in cyber-enabled theft so that espionage operations aimed at advancing the country's nuclear programme and military capabilities can be financed. For example, between 2021 and 2023 the RGB-linked group Andariel used ransoms obtained from US and South Korean victims in the healthcare sector to fund attack infrastructure. The use of this equipment was subsequently observed in network intrusions targeting government agencies, armed forces and companies involved in the development of missile, aerospace and uranium-processing technologies.

Bridgehead beyond borders

Owing to limited connectivity and regime control over telecommunications infrastructure, cyber activities conducted from within the DPRK are comparatively traceable. To blend in, DPRK groups have expanded geographically as they scout for safe operational spheres in neighbouring China and Southeast Asian countries.

Similarly, Pyongyang's concerted campaign to plant North Korean IT specialists working undercover at international firms

requires a personal and physical footprint outside the DPRK. Although North Korean IT professionals seek out remote work arrangements, the scheme relies on what are often unwitting facilitators in-country that set up laptops or file employment records. Through the development of this support network, a bridgehead of laptop farms has been established across at least eight states in the US and in Europe — the cybersecurity firm CrowdStrike has identified clusters in the United Kingdom, Poland and Romania.

In late 2024, individual operatives began to deviate from this playbook, originally conceived to generate revenue for the regime, by threatening upon discovery to publish stolen data in order to extract maximum financial value. The Google subsidiary Mandiant considered this extortionist shift to be part of an exit scheme. For its part, the security firm DTEX observed that in rare instances, extortion extended to the explicit threat of network access being given to North Korean APTs for further exploitation.

Repatriating knowledge

In March 2025, the RGB began to set up a new offensive research centre with a focus on "developing offensive hacking technologies and programmes". The goal is to "respond immediately to real-time information from RGB hacking groups deployed overseas". Research Centre 227 recognises the value offered by the access and visibility achieved through the bridgehead abroad. Its creation points to a strategic interest in harnessing the lessons learned from those deployments in order to refine and advance the DPRK's cyber capabilities overall.

Calibrating responses

Efforts by authoritarian states to take advantage of non-state cyber capabilities have led to a diversified spectrum of state nexus threats. While the resulting complex composition of threats is unlikely to fundamentally challenge the ability to trace threats and their sponsors, it raises the bar for the international coordination of both political and legal responses. Providing confident assessments about accountability and reaching a consensus on consequences will depend increasingly on information sharing and trusted partners.

In the absence of an integrated understanding of how authoritarian actors leverage non-state resources, the potential of tactics to slow down and fragment attribution efforts may weaken the response toolkit developed by EU member states. Currently, key cyber diplomacy tools — such as sanctions — remain closely tied to attribution. Addressing senior officials responsible for developing cyber policies/practices in May 2025, Germany's cyber ambassador, Maria Adebahr, recognised that efforts to hold threat actors accountable are dependent on this link to attribution. Implicit in this recognition is the need to develop response options that are independent of attribution.

Capturing non-state capabilities allows authoritarian states to increase their capabilities pool and step up their operational tempo. Diplomatic measures that address the interweaving of state and non-state capabilities have a strong complementary potential. They include not only initiatives aimed at restricting access for threat actors to legitimate platforms and disrupting criminal tools; information sharing — as part of a regular exchange with friendly jurisdictions — with a view to developing a common threat perception could support due diligence efforts to constrain the room for manoeuvre overseas and facilitate the takedown of shadow infrastructure. A response framework that remains fit for purpose requires a range of tools that can match the changing scope of the threat.

Jakob Bund is an Associate in the EU/Europe Research Division of SWP and a member of the research consortium managing the European Repository of Cyber Incidents (EuRepoC, www.eurepoc.eu). *The research informing this report has been made possible by support from the German Federal Foreign Office.*

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2025C30