INTRINSEC
Innovative by design

Geographical Threat Landscape

H1 2026





North America



Middle East



Europe & Russia



Asia

2026 Intrinsec, Inc. All rights reserved

Table of contents

1. Introduction 3
2. Executive summary 4
3. Methodology 6
4. Regional Threat Assessment 7
4.1. Europe and Russia 7
4.1.1. Strategic Evolution: The "Access-First" Doctrine and AI-Augmentation 8
4.1.2. The Ukrainian War Theater 10
4.1.3. Russian Hybrid Warfare in Europe 15
4.1.4. Outlook 20
4.2. North America and strategic partners 21
4.2.1. Coruna iOS exploit kit, proliferation of a high end capability across competing threat actors 21
4.2.2. BlackCore, Rokh Solis, and Alleged Israeli Information Operations Against La France Insoumise During France's 2026 Municipal Elections 26
4.2.3. Outlook 29
4.3. Middle East 30
4.3.1. Iran-Centric Cyber Operations: The Primary Regional Driver 31
4.3.2. Hacktivism: the new porous constant 32
4.3.3. Rain of sanctions and arrest warrants 38
4.3.4. Outlook 41
4.4. Asia 42
4.4.1. China 42
4.4.2. North Korea 48
4.4.3. South-East Asia 53
4.4.4. East-Asia 57
4.4.5. Outlook 60
5. Conclusion 61
Recommendations 62

1. Introduction

The first half of 2026 further demonstrated that cyberspace has become an integral component of geopolitical competition. Cyber operations are no longer conducted in isolation but increasingly support broader national objectives, including intelligence collection, military operations, political influence, economic competition, and strategic deterrence. As geopolitical tensions continue to shape the international environment, cyber capabilities have become a key instrument through which states and state-aligned actors pursue their interests below the threshold of conventional armed conflict.

This report provides a geographical assessment of the cyber threat landscape observed between January and June 2026 across four strategic regions: Europe and Russia, North America, the Middle East, and Asia. Rather than attempting to catalogue every significant cyber incident, the report focuses on developments that best illustrate the evolution of regional cyber ecosystems and the strategic dynamics shaping today's threat landscape.

The analysis examines how geopolitical developments, military conflicts, diplomatic tensions, and technological competition influenced cyber activity throughout the reporting period. Particular attention is given to state-sponsored operations, hybrid campaigns, cyber-enabled influence activities, offensive innovation, and emerging operational trends that are likely to shape the cyber environment beyond the reporting period. Where relevant, specific case studies are included to illustrate broader strategic developments and the evolution of adversary capabilities.

2. Executive summary

The first half of 2026 confirmed that cyber operations have become a central instrument of geopolitical competition. Across Europe, North America, the Middle East, and Asia, cyber capabilities were increasingly integrated into broader state strategies supporting military objectives, intelligence collection, political influence, and economic competition. While regional dynamics differed, several common trends emerged, demonstrating that cyber threats continue to evolve toward greater sophistication, persistence, and strategic coordination.

A defining characteristic of the reporting period was the growing emphasis on long-term access rather than immediate disruption. Multiple state-sponsored actors prioritized the establishment of persistent footholds within government networks, cloud infrastructures, telecommunications providers, edge devices, and critical infrastructure. This "access-first" approach enables adversaries to maintain strategic positioning that can be activated rapidly in response to future political or military developments. Russia's cyber operations particularly illustrated this evolution, combining long-term espionage, hybrid influence activities, and support to military operations in Ukraine.

Artificial Intelligence also emerged as a significant operational force multiplier. Threat actors increasingly integrated Generative AI and Large Language Models into phishing campaigns, malware development, social engineering, and operational automation. Rather than fundamentally changing attacker objectives, AI significantly accelerated operational tempo while lowering the technical barriers required to conduct sophisticated campaigns. Organizations should therefore expect increasingly personalized, scalable, and difficult-to-detect attacks throughout the remainder of the year.

The reporting period further demonstrated the increasing convergence between state-sponsored actors, cybercriminal groups, exploit brokers, initial access brokers, and ideologically motivated hacktivists. Capabilities, infrastructure, and offensive tooling continue to circulate across these ecosystems, complicating attribution while increasing the availability of advanced offensive capabilities. At the same time, influence operations became increasingly sophisticated, combining AI-generated content, coordinated social media activity, fabricated media ecosystems, and cross-platform amplification to influence political discourse and exploit societal polarization.

Critical infrastructure remained a primary target across multiple regions. However, threat actors increasingly shifted their attention toward less protected assets,

including VPN gateways, routers, telecommunications equipment, industrial remote access systems, and distributed edge infrastructure. These systems provide attractive opportunities for persistent access while often benefiting from weaker security controls and slower patch management than traditional enterprise environments.

Looking ahead, organizations should expect geopolitical tensions to remain a primary driver of cyber activity. Continued integration of AI into offensive operations, persistent targeting of edge infrastructure, expansion of hybrid influence campaigns, and increasing cooperation between state and criminal ecosystems are likely to shape the threat landscape during the second half of 2026. Consequently, organizations should prioritize strengthening identity security, protecting Internet-facing infrastructure, accelerating risk-based vulnerability management, improving visibility across cloud and edge environments, and integrating geopolitical intelligence into cyber risk assessment processes to better anticipate emerging threats.

3. Methodology

This assessment is based on the continuous monitoring and analysis of publicly available cyber threat intelligence collected throughout the first half of 2026. The analysis draws upon a broad range of trusted sources, including government advisories, national CERTs, security vendors, technical research publications, industry reports, academic research, and publicly available reporting on cyber incidents and geopolitical developments.

Rather than providing an exhaustive inventory of cyber events, this report adopts a geographical and strategic approach. Events were selected according to their intelligence value, regional significance, and ability to illustrate broader developments affecting the cyber threat landscape. Particular attention was given to activities reflecting the evolution of state-sponsored operations, hybrid warfare, influence campaigns, offensive innovation, and strategic changes in adversary behaviour.

Each regional chapter combines technical reporting with geopolitical context. Cyber incidents were therefore assessed not only according to their technical characteristics but also with regard to their strategic implications, including the actors involved, targeted sectors, regional security dynamics, military conflicts, diplomatic developments, and broader political objectives. This approach aims to better understand how cyber operations increasingly support wider national and geopolitical ambitions.

Several case studies are included throughout the report to illustrate significant developments observed during the reporting period. These examples were selected because they represent emerging trends, demonstrate noteworthy technical or operational innovations, or provide insight into evolving adversary capabilities. They should therefore be understood as representative examples rather than an exhaustive overview of all observed activity.

Finally, it should be recognized that cyber threat intelligence remains inherently constrained by collection biases, reporting disparities, and the availability of public information. Attribution assessments may evolve over time as additional evidence becomes available, while some operations remain undisclosed or only partially documented. Consequently, the findings presented in this report represent an analytical assessment of the information available during the reporting period rather than a comprehensive account of all cyber activity.

4. Regional Threat Assessment

This section presents a regional review of the most significant cyber developments observed between January and June 2026. The analysis is organized by geographical area, highlighting the differences in threat activity, actor presence, and operational trends across regions. The topics covered in each chapter reflect the events and intelligence assessed as the most relevant during the reporting period. As a result, the themes addressed may vary from one region to another depending on the nature of the observed activity and the availability of reporting. The purpose of this assessment is not to provide an exhaustive record of all cyber incidents, but rather to identify the developments that best illustrate the evolution of the regional cyber environment during the first half of 2026.

4.1. Europe and Russia



The first half of 2026 has seen a fundamental shift in Russian cyber operations, transitioning from isolated disruptive events to a systemic "access-first" strategy. This approach prioritizes long-term, low-visibility persistence in critical networks and the communications layer, allowing for the rapid activation of disruptive effects when strategically required[1].

A defining characteristic of this period is the operational integration of Generative AI (GenAI) and Large Language Models (LLMs) to accelerate the attack lifecycle, from lure generation to the creation of custom malware [2]. The threat landscape is now bifurcated between the direct support of the war effort in Ukraine and a broad, hybrid campaign of destabilization across NATO and EU member states, focusing on critical national infrastructure (CNI) and the "distributed edge" of the grid [3].

[1] Recorded Future, 2026-02-12, https://assets.recordedfuture.com/insikt-report-pdfs/2026/cta-2026-0212.pdf

[2] The Record, 2026-05-20, https://therecord.media/ukraine-says-russia-using-ai-malware-on-battlefield

[3] DomainTools, 2026-06-16, https://dti.domaintools.com/research/threat-intelligence-report-russia-router-dns-and-messaging-layer-collection-operations

4.1.1. Strategic Evolution: The "Access-First" Doctrine and AI-Augmentation

The "Access-First" Strategy

Russian intelligence has shifted its focus toward "quiet and lasting" access. Rather than immediate disruption, the goal is persistent visibility and control over the paths people use to communicate and authenticate. This is operationalized through two distinct technical profiles targeting edge infrastructure.

The GRU (Unit 26165) treats SOHO routers as a primary collection terrain to build a "surveillance dragnet." In campaigns such as **FrostArmada**, operators exploit vulnerable home and small office routers (specifically targeting TP-Link (e.g., WR841N) and MikroTik devices) to modify DNS and DHCP settings [4] [5] [6]. By exploiting vulnerabilities like **CVE-2023-50224**, actors extract administrative credentials via crafted HTTP GET requests and push victims through Russian-controlled resolvers to enable Adversary-in-the-Middle (AiTM) capabilities. This infrastructure supports the interception of **OAuth authentication tokens** after multi-factor authentication (MFA) has been completed, granting direct access to cloud accounts. Furthermore, the GRU employs **TLS interception**, spoofing DNS responses for targeted domains and serving fraudulent certificates to read encrypted traffic in plaintext. This operation, known as **Operation Masquerade**, has impacted over 200 organizations and 5,000 consumer devices across 120 countries.

In contrast, the FSB's signals-intelligence unit (Center 16) targets critical national infrastructure (CNI) using low-tech but highly effective configuration exfiltration. The primary technique involves scanning for SNMP agents accepting default or weak community strings, where actors issue snmpset requests abusing the **CISCO-CONFIG-COPY-MIB** (OID 1.3.6.1.4.1.9.9.96) to force the device to upload its running-config via TFTP to an attacker-controlled VPS [7]. The FSB also aggressively leverages **CVE-2018-0171** and the legacy **CVE-2008-4128**. Stolen configurations are mined for local credentials, specifically targeting weak Cisco password hashes (Types 0, 4,

[4] Malwarebytes, 2026-04-08, https://www.malwarebytes.com/blog/news/2026/04/russian-state-sponsored-hackers-hijack-home-and-small-office-routers-for-espionage
[5] The Hacker News, 2026-04-07, https://thehackernews.com/2026/04/russian-state-linked-apt28-exploits.html
[6] KrebsOnSecurity, 2026-04-07, https://krebsonsecurity.com/2026/04/russia-hacked-routers-to-steal-microsoft-office-tokens/
[7] Picus Security, 2026-07-14, https://www.picussecurity.com/resource/blog/fsb-center-16-how-russian-hackers-exploit-routers-via-snmp-and-cisco-smart-install

and 7), which are trivially reversible. Post-compromise activity includes the creation of rogue local accounts and the establishment of **GRE tunnels** to reroute strategic traffic.



Figure 1 - FSB Center 16 activity and mitigations (source: Joint Cybersecurity Advisory)

Moreover, the 16th Center (also known as "military unit 71330") operates a geographically distributed network of **11 interception centers** across Russia, including sites in Sochi, Crimea, and Pskov, allowing for targeted SIGINT collection across Europe, the US, and Asia. Specifically, Military Unit 61240, located near Krasnoye Selo, is tasked with targeting French interests, maintaining close ties with front companies like AO AST and NPP Gamma to support its offensive cyber operations [8].

Parallel to edge exploitation, there is a systemic focus by Russian intelligence services on compromising the secure messaging platforms **Signal and WhatsApp** in vast campaigns targeting senior political, military and diplomatic figures, as well as investigative journalists. Alerts have been given in Germany [9], the USA [10] and in

[8] CERT-FR, 2026-07-13, https://www.cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-004/
[9] The Record, 2026-02-10, https://therecord.media/germany-warns-phishing-campaign-signal-gov-officials-journalists
[10] CISA/FBI, 2026-03-20, https://www.ic3.gov/PSA/2026/PSA260320

the Netherlands [11]. In Germany, some high profiles have been compromised, like the former chief of the foreign intelligence agency BND [12].

AI-Augmentation of Offensive Operations

AI is no longer experimental but is a core operational enabler. The group GREYVIBE, Russian-nexus threat actor, demonstrates the systematic use of GenAI (ChatGPT, Gemini, Ideogram AI) across the attack lifecycle. This includes generating high-fidelity images and sites for campaigns like *PrincessClub* and *PhantomClick*, as well as using LLMs to develop custom obfuscators (LOOKVALJS, DAYLIGHT, TEASOUP) and the LegionRelay RAT, a lightweight PowerShell-based tool used for file exfiltration and browser data theft. The group has also expanded into "DroneLink" operations, leveraging fake charity websites supporting the Armed Forces of Ukraine to deliver LegionRelay scripts [13].

Furthermore, AI is being embedded directly into malware to generate malicious commands "on the fly," as seen in 2025 with the LameHug strain (APT28), making detection by traditional pattern-based security products significantly harder. Russian operators also used AI to refine malware, including the ScopeCreep backdoor, adding features designed to evade detection and escalate privileges inside compromised systems [14].

The Ukrainian War Theater

Kinetic-Cyber Synchronization

Cyber operations have evolved from being precursors to becoming real-time guidance tools for kinetic strikes. This synchronization manifests as a closed-loop intelligence cycle where cyberattacks on the energy grid are used to map facility layouts, identify critical components, and track the movement of repair crews in real-time. This high-fidelity intelligence guides the timing and precision of missile

[11] BleepingComputer, 2026-03-09, https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-signal-whatsapp-account-hijacking-attacks/
[12] Security Affairs, 2026-03-16, https://securityaffairs.com/189509/intelligence/former-germanys-foreign-intelligence-vp-hit-in-signal-account-takeover-campaign.html
[13] WithSecure, 2026-05-28, https://labs.withsecure.com/publications/greyvibe
[14] National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf#page=24

strikes, ensuring that physical destruction is maximized by targeting the most critical nodes identified via cyber-reconnaissance [15].

This integration allows Russian commanders to assess the effectiveness of a kinetic strike by monitoring the immediate cyber-response of the targeted infrastructure, such as automated failovers or emergency alerts, which then informs the next wave of attacks. This creates a symbiotic relationship where cyber-capabilities act as the "eyes" for kinetic "fists".

Key Actors and Tooling

Gamaredon (Primitive Bear) maintains a high operational tempo targeting Ukrainian government and military institutions. The group, attributed to the **18th Center the FSB**, employs a sophisticated, multi-stage "Matryoshka" infection chain where loaders load other loaders, designed for invisibility and to exhaust defenders. The architecture is nearly entirely fileless and driven by VBScript using native Windows COM APIs to blind automated sandboxes. Sekoia aligns with CERT-UA's taxonomy, grouping the arsenal by function: GammaPhish (initial access), GammaLoad (intermediary loaders), GammaWorm (worm), GammaSteel (stealer), and GammaWipe (wiper) [16]. The latest Gamaredon toolset was also analyzed by ESET, using a different taxonomy [17].

Technical TTPs for GammaLoad include a priority-based failover mechanism that first attempts to retrieve cached C2 URLs from the Windows registry before falling back to **Dead Drop Resolvers (DDR)** on platforms like Telegram and Telegra.ph. The group employs **Alternate Data Streams (ADS)** within %TEMP% to hide payloads, with persistence maintained via scheduled tasks like DsSvcCleanup. Victim machines are uniquely identified by collecting the %COMPUTERNAME% and the hexadecimal serial number of the system drive, exfiltrated via crafted User-Agent strings.

The GammaSteel stealer employs high-end evasion by operating almost entirely from memory, using the **Windows Data Protection API (DPAPI)** to encrypt and stage 71 distinct payload functions inside the HKCU\Printers registry key. A central orchestrator manages these functions, triggered via a detached hidden PowerShell

[15] The Record, 2026-02-23, https://therecord.media/ukraine-cyberattacks-guiding-russian-missile-strikes
[16] Sekoia, 2026-06-04, https://blog.sekoia.io/fsbs-matryoshka-3-3-gamaredons-gifts-that-keeps-unpacking-gammasteel/
[17] ESET, 2026-06-25, https://www.welivesecurity.com/en/eset-research/gamaredon-2025-leveraging-tunnels-workers-dead-drops-new-alliances/

process. The stealer actively hunts for documents via recurring scans of local/network drives and real-time surveillance of files as they are saved. Candidate files are locally deduplicated against MD5 hashes before being uploaded to S3-compatible cloud storage, such as Tebi.io. Since 2025, there is also evidence of **strategic cooperation with Turla** to amplify operational impact, specifically utilizing the PteroPaste tool in joint operations.

Turla (Secret Blizzard) focuses on high-end espionage using redundant malware ecosystems. This intrusion set is operated by the **16th Center of the FSB** (Military Unit 71330), leveraging the center's global SIGINT infrastructure to maintain long-term persistence in strategic targets [18]. The **StockStay framework** is a sophisticated .NET backdoor used for ongoing cyber espionage against government and military organizations in Ukraine and entities related to Italian foreign policy [19]. The framework is designed as a multi-component ecosystem communicating via secure WebSocket connections.

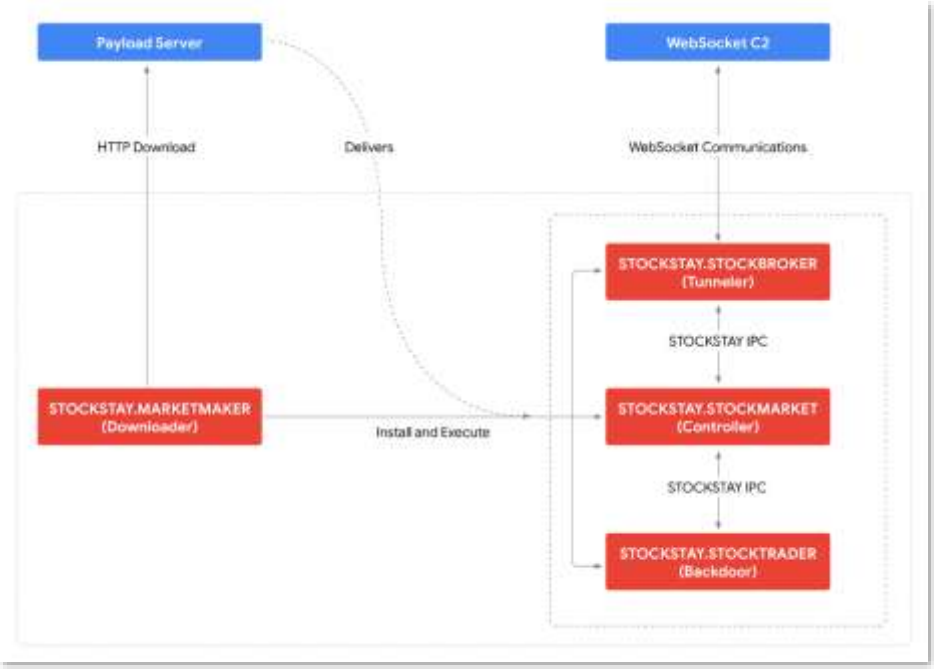

Figure 2 - Stockstay Backdoor mechanism (source: Google)

The system is split into specialized components interacting via an IPC channel using WM_COPYDATA messages. STOCKSTAY.STOCKBROKER acts as a proxy-aware tunneler, while STOCKSTAY.STOCKMARKET serves as the orchestrator managing configuration and commands via an encrypted on-disk file that masquerades as a stock market tool. STOCKSTAY.STOCKTRADER executes commands on the infected

[18] CERT-FR, 2026-07-13, https://www.cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-004/
[19] Google Threat Intelligence, 2026-06-25, https://cloud.google.com/blog/topics/threat-intelligence/stockstay-turla-intelligence-gathering?hl=en

host. Upon first execution, the implant generates a unique 4096-bit RSA key pair to encrypt outbound data. StockStay shares significant code and functional overlaps with the **Kazuar toolkit**, an older malware family attributed to Turla that has expanded from a relatively traditional backdoor into a highly modular peer-to-peer (P2P) botnet ecosystem designed to enable persistent, covert access to target environments [20].

APT28 (Fancy Bear) continues to target the defense industrial base using high-end zero-days—such as CVE-2026-21513 in MSHTML [21] —and tailored lures, including "Starlink-themed" content and the deployment of the new BadPaw and MeowMeow malware families [22] (low attribution confidence). The **PRISMEX Campaign** is a sophisticated operation targeting the Ukrainian defense supply chain and its allies. The campaign utilizes a suite of interconnected components: **PrismexDrop**, **PrismexLoader**, and **PrismexStager** (Covenant Grunt implant) [23].

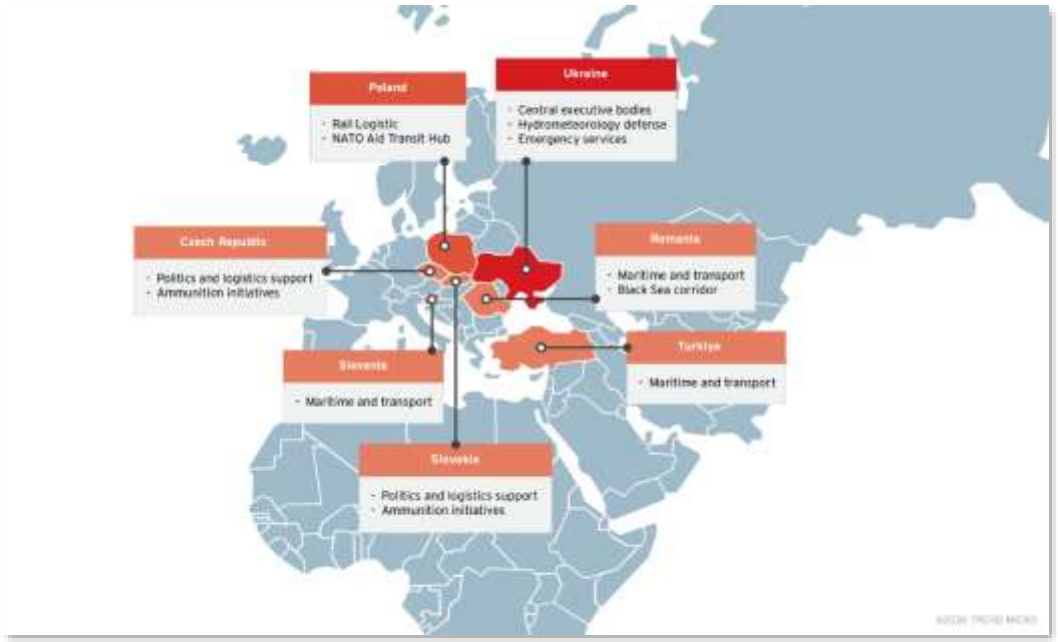

Figure 3 - Victimology of Prismex campaign (source: TrendMicro)

[20] Microsoft, 2026-05-14, https://www.microsoft.com/en-us/security/blog/2026/05/14/kazuar-anatomy-of-a-nation-state-botnet/
[21] Akamai, 2026-02-20, https://www.akamai.com/blog/security-research/2026/feb/inside-the-fix-cve-2026-21513-mshtml-exploit-analysis
[22] ClearSky, 2026-03-03, https://www.clearskysec.com/wp-content/uploads/2026/03/BadPaw_and_MeowMeow.pdf
[23] Trend Micro, 2026-03-26, https://www.trendmicro.com/en_us/research/26/c/pawn-storm-targets-govt-infra.html

The operation is characterized by the rapid weaponization of vulnerabilities, leveraging **CVE-2026-21509** to force the instantiation of the Shell.Explorer.1 COM object, which retrieves a malicious .lnk file from a remote WebDAV server. This often chains into **CVE-2026-21513** to achieve code execution outside the browser sandbox. The final payload utilizes the **Covenant** C2 framework for fileless execution and encrypted communications. Targeting is concentrated on the operational backbone of defense, including meteorological data providers, transport hubs, and international aid corridors.

Defensive Response

The SBU has neutralized over 16,000 critical cyber incidents since the start of the invasion [24]. This effort involves the active disruption of Russian C2 infrastructure and the proactive identification of "sleeper" implants. The SBU's capacity for detection has evolved to include the identification of AI-generated lures and the neutralization of multi-stage loaders.

In a strategic move, Ukraine has begun converting seized cryptocurrency from Russian cybercrime groups into war bonds to fund its defense, effectively weaponizing the recovery of stolen digital assets to finance military hardware and critical infrastructure repair [25].

Regional resilience is further bolstered by the "Odessa Triangle," a collective cyber-defense framework established as a "Triple Cyber Alliance" between Romania, Ukraine, and Moldova. Launched during the Munich Security Conference, this alliance is operationalized through a Memorandum of Understanding between the National Directorate for Cyber Security (DNSC) and its partner institutions to strengthen regional resilience [26]. Additionally, the SBU is implementing a nationwide project to increase the cyber-resilience of regional media outlets.

[24] SBU, 2026-07-01, https://ssu.gov.ua/novyny/z-pochatku-povnomasshtabnoi-viiny-sbu-neitralizuvala-ponad-16-tysiach-rosiiskykh-kiberatak-ta-kiberintsydentiv
[25] The Record, 2029-06-29, https://therecord.media/ukraine-uses-seized-crypto-cybercrime-for-war-bonds
[26] Calea Europeană, 2026-02-15, https://www.caleaeuropeana.ro/triunghiul-odesa-romania-ucraina-republica-moldova-au-convenit-la-munchen-sa-lanseze-tripla-alianta-cibernetica/

4.1.3. Russian Hybrid Warfare in Europe

Strategic Sabotage of Critical National Infrastructure

Russia is targeting the "distributed edge" of European infrastructure to create systemic instability, shifting focus from centralized control centers to the decentralized components of the grid.

In Poland, the threat group **ELECTRUM** (exhibiting strong overlaps with **Sandworm**, a cyber warfare unit attributed to the GRU) targeted over 30 renewable energy facilities and a major combined heat and power (CHP) plant on December 29, 2025 [27] [28]. This represents a strategic shift toward targeting **Remote Terminal Units (RTUs)** and the communications systems managing distributed energy resources. By exploiting the standardized configurations and lower security investment typical of smaller generation sites, the adversary achieved scale across the distributed edge of the grid. Access was achieved through exposed **Fortinet FortiGate** devices, leveraging VPN interfaces lacking MFA, reused credentials, and unpatched vulnerabilities, preceded by months of reconnaissance into SCADA systems.

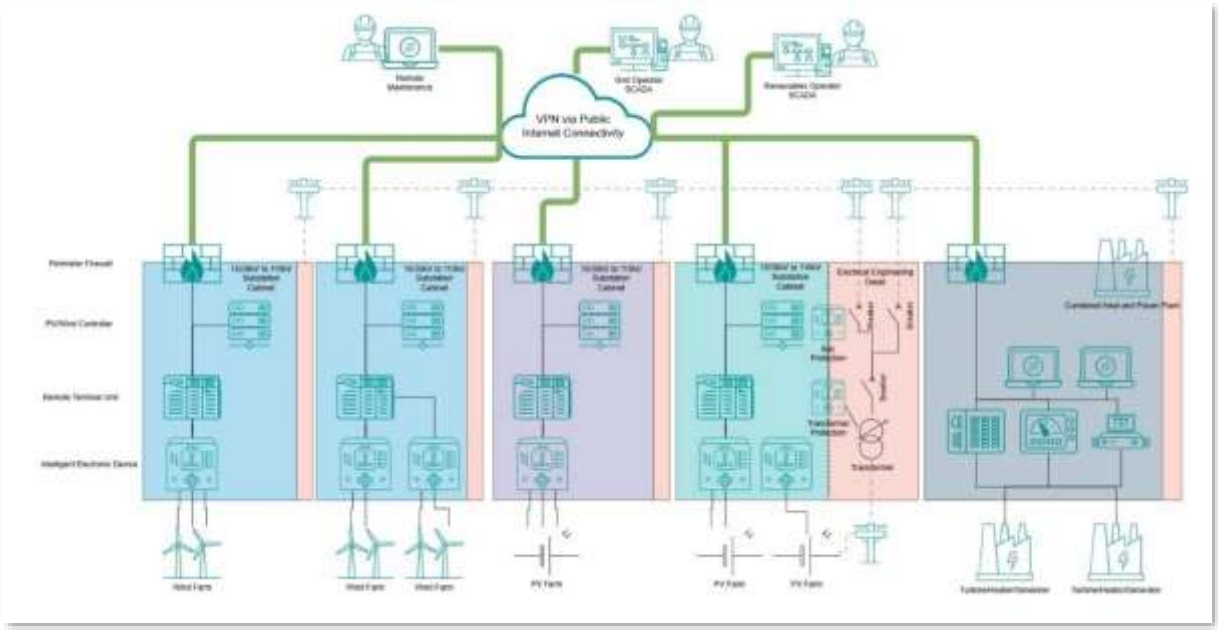

Figure 4 - Typical renewable energy infrastructure (source: Dragos)

[27] ESET, 2026-01-23, https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/
[28] Dragos, 2026-01-28, https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

The attack deployed **DYNOWIPER**, a destructive malware designed for rapid, irreversible data corruption. Rather than overwriting entire files, DYNOWIPER uses a **Mersenne Twister PRNG** to generate pseudorandom data, overwriting the file header and up to 4,096 random offsets with 16-byte sequences [29]. The wiper deliberately avoids system-critical directories to ensure the OS remains stable until the destruction phase is complete. Upon completion, the malware obtains SeShutdownPrivilege to force a system reboot, preventing immediate recovery. Behavioral detection using **canary files** proved critical; at one major CHP plant, EDR solutions utilizing canary monitoring halted the wiper on over 100 machines.

More recently, Polish intelligence said hackers breached **water treatment facilities in five towns** in 2025, in some cases gaining access to industrial control systems that could have disrupted water supplies [30]. No official attribution has been made, but Russian origin seems likely given the intense hostile cyber activity of Russian special services in this country.

In Germany, the national rail operator, **Deutsche Bahn**, was targeted by high-volume DDoS attacks in February 2026, disrupting ticketing and timetable systems [31]. This attack was operated by the group **NoName057(16)** [32] and occurred after a series of physical sabotage, including arson on railway lines and the cutting of overhead electrical cables, mirroring a broader Russian hybrid strategy of combining digital disruption with physical kinetic effects to maximize public distress.

In Romania, a pattern of **"geopolitical ransomware"** has emerged, exemplified by the attack on the national oil pipeline operator (**Conpet**) by the **Qilin** group. Romanian authorities assess this as systematic hybrid operations aligned with Russian strategic interests rather than purely profit-driven crime [33] [34].

[29] Elastic, 2026-02-06, https://www.elastic.co/security-labs/dynowiper
[30] The Record, 2026-05-07, https://therecord.media/polish-intelligence-warns-hackers-attacked-water-treatment
[31] Deutsche Welle, 2026-02-18, https://www.dw.com/en/deutsche-bahn-says-cyberattack-hit-ticket-and-info-systems/a-76024130
[32] Tagesschau, 2026-02-18, https://www.tagesschau.de/inland/gesellschaft/deutsche-bahn-cybersicherheit-100.html
[33] Security Affairs, 2026-02-09, https://securityaffairs.com/187736/cyber-crime/romanias-national-oil-pipeline-firm-conpet-reports-cyberattack.html
[34] The Record, 2026-02-23, https://therecord.media/ransomware-gangs-advancing-moscow-geopolitical-interests-warns-romania

Influence Operations and State Proxies

The SVR has formally absorbed the **Wagner influence branch**, transforming it into a state-directed propaganda machine. While this transition primarily targets the Global South—orchestrating disinformation campaigns in Africa and Latin America (e.g., Mali, Bolivia) to undermine European and US influence—it reflects a broader SVR strategy of integrating former proxy networks into direct state control [35]. This "quiet" strategic approach to influence and diplomatic espionage contrasts with the more aggressive, technically-driven SIGINT and sabotage operations conducted by the FSB's Center 16.

A separate, highly organized effort is seen in the **Roska Bridge** IMS. This operation focuses on exploiting the architectural flaws of decentralized platforms (the Fediverse/Mastodon) and using services like **Brid.gy** to cross-post coordinated anti-Western and anti-Ukrainian propaganda to Bluesky and Mastodon. Roska Bridge launders content from sanctioned outlets and is linked to the **Portal Kombat** infrastructure, targeting both Western and domestic Russian audiences [36].

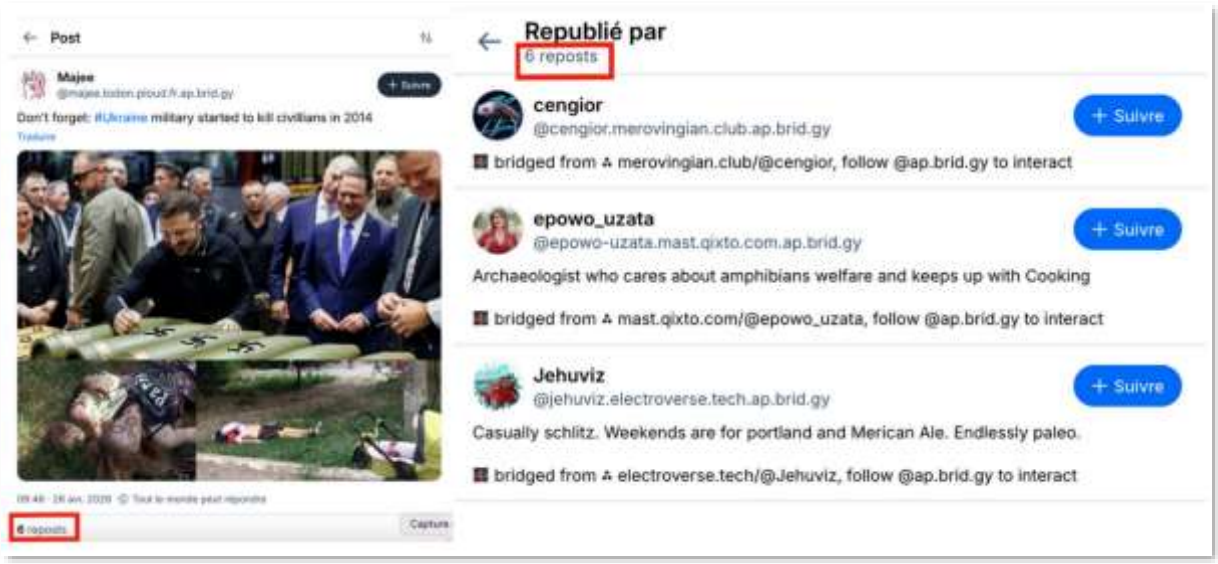

Figure 5 - Example of a reshared post from Roska Bridge (source: CheckFirst)

Vienna has emerged as Russia's largest **Western spy hub for targeting NATO** and other sensitive communications. This operation leverages diplomatic compounds and rooftop satellite clusters to monitor traffic across NATO, the Middle East, and

[35] AllEyesOnWagner, 2026-02-14, https://alleyesonwagner.org/2026/02/14/a-new-chef-in-the-kitchen-the-svr-takes-control-of-the-wagners-influence-branch-for-offensive-operations-in-the-global-south/

[36] CheckFirst, 2026-07-02, https://checkfirst.network/roska-bridge-how-a-pro-russian-ims-exploits-vulnerabilities-of-decentralised-platforms-to-spread-propaganda/

Africa. A primary node is the "Russencity" complex, which utilizes movable lenses and satellite dishes to track geostationary satellites. With approximately 500 diplomats in the city, up to a third are assessed to be covert operatives. Despite warnings from Austria's intelligence agency (DSN), legal constraints limiting the prosecution of espionage that does not directly target Austria have hindered large-scale expulsions [37].

The Russian state has also deployed networks such as **"Storm-1516"** to target political events and spread disinformation. One of its latest operations focused on the French municipal elections in March 2026. The operation involved the creation of over a hundred fraudulent news sites that meticulously mimicked the branding and visual identity of regional daily press (PQR) to deceive local voters. These sites were used to inject disinformation and influence the outcome of local campaigns. This effort was countered by the French state and Viginum, which identified and removed the fraudulent sites prior to the vote [38] [39].

A more general overview of the current pro-Russian influence ecosystem has been published by Google in June 2026 [40].

Hacktivists

The group **NoName057(16)** serves as a primary tool for disruptive, high-visibility attacks. The group launched a series of DDoS attacks against the Milano Cortina Winter Olympics, targeting hotels, government websites, and national Olympic committees [41] [42]. A US indictment of one of its operators revealed that the group was created as a covert project within the CISM (Center for the Study and

[37] Security Affairs, 2026-03-19, https://securityaffairs.com/189653/intelligence/russia-establishes-vienna-as-key-western-spy-hub-targeting-nato.html
[38] RTL, 2026-02-06, https://www.rtl.fr/actu/politique/info-rtl-l-approche-des-elections-municipales-l-etat-a-deja-supprime-une-centaine-de-sites-d-information-pro-russes-7900598005
[39] Viginum, 2026-06-11, https://www.sgdsn.gouv.fr/viginum/actualites/bilan-des-ingerences-numeriques-etrangeres-ayant-cible-les-elections-municipales
[40] Google, 2026-06-29, https://cloud.google.com/blog/topics/threat-intelligence/pro-russia-influence-ecosystem?hl=en
[41] Intel 471, 2026-02-11, https://www.intel471.com/blog/winter-olympics-2026-hacktivism-surges-ahead-of-protests-and-suspected-sabotage
[42] Security Affairs, 2026-02-05, https://securityaffairs.com/187654/hacktivism/pro-russian-group-noname05716-launched-ddos-attacks-on-milano-cortina-2026-winter-olympics.html

Network Monitoring of the Youth Environment), with the Kremlin providing funding and target selection [43].

Russian-linked operations rely on a complex web of European-based infrastructure to maintain anonymity and circumvent sanctions. Recent investigations in the Netherlands revealed the use of hosting providers (such as MIRhosting and WorkTitans) to provide the same servers and VPN/proxy connections used by the **NoName057(16)** group for DDoS attacks and the **Doppelgänger** network for coordinated disinformation campaigns [44]. This infrastructure is often shifted to newly established front companies to evade EU sanctions and maintain operational persistence.

The line between "hacktivism" and state-directed sabotage is often blurred, with pro-Russian groups employing a strategy of "perceived sophistication" to maximize psychological impact [45]. Rather than complex ICS-specific exploits, groups such as **Z-Pentest Alliance**, **NoName057(16)**, **QuietSec**, and **Overflame** utilize opportunistic scanning for unauthenticated **Virtual Network Computing (VNC)** sessions on Human-Machine Interface (HMI) devices. This allows them to gain visibility into industrial processes without requiring advanced malware.

The **Infrastructure Destruction Squad (IDS)**, a pro-China and pro-Russia collective, employs simple Python-based scanning scripts to identify exposed HMI devices, particularly in Italy, Taiwan, and South Korea. Their operations are characterized by a lack of specific target intelligence, often compromising devices without prior knowledge of the entity's identity.

To enhance the perceived impact of their intrusions, these actors frequently target exposed webcams within corporate offices. By leaking internal imagery alongside claims of SCADA compromise, they create a sense of total compromise. These operations are heavily dependent on media coverage to amplify the perceived success of their attacks, transforming unsophisticated access into a tool for public destabilization. The 2026 Winter Olympics saw a combination of DDoS attacks and suspected physical sabotage, mirroring patterns observed during the 2024 Paris Olympics.

[43] BleepingComputer, 2025-12-10, https://www.bleepingcomputer.com/news/security/ukrainian-hacker-charged-with-helping-russian-hacktivist-groups/
[44] The Record, 2026-05-26, https://therecord.media/dutch-authorities-arrest-suspects-over-russian-cyber-operations
[45] Intrinsec, 2026-03-03, Review of intensified hacktivist attacks on SCADA systems amidst the Winter Olympics

Outlook

The first half of 2026 confirms that Russian cyber operations are no longer just a supporting element but a core component of a broader hybrid strategy. The "AI-augmentation" of these operations has significantly shortened the window between vulnerability discovery and operational impact.

For the remainder of 2026, the focus is expected to shift toward increased targeting of "Edge" infrastructure to maintain a dormant presence in NATO networks, further integration of AI to automate the creation of tailored phishing and social engineering campaigns, and a continued focus on CNI sabotage as a tool for political coercion within the EU.

4.2. North America and strategic partners



Understanding the geographic distribution and operational patterns of intrusion sets associated with the United States and its strategic partners was always an important component of modern cyber threat intelligence (CTI) and maybe more today. As cyberspace continues to serve as a domain for geopolitical competition, nation-state and state-aligned cyber actors increasingly conduct operations that support broader national security, intelligence collection, military, and foreign policy objectives.

Monitoring intrusion sets linked to the United States and closely aligned nations, including key strategic partners such as Israel, provides valuable insight into evolving tactics, techniques, and procedures (TTPs), targeting priorities, and operational trends. These actors have historically demonstrated sophisticated capabilities and have been associated with cyber espionage, counter-proliferation efforts, influence operations, and targeted campaigns against government, defense, telecommunications, critical infrastructure, and technology sectors.

This section examines the geographic landscape of intrusion sets associated with the United States and its strategic allies for H1 2026, highlighting observed patterns, areas of activity, and the broader intelligence implications for defenders, policymakers, and security practitioners.

4.2.1. Coruna iOS exploit kit, proliferation of a high end capability across competing threat actors

Coruna

Coruna is a modular iOS exploit kit assessed to enable remote compromise of iPhones through web delivered exploitation chains that progress from WebKit code execution to sandbox escape and ultimately kernel level privilege.

Google Threat Intelligence Group (GTIG) reported discovering Coruna in February 2025 and described a capability set targeting iOS 13 through iOS 17.2.1, with 23 exploits organized into five end to end chains designed to maximize reliability

across device and version combinations.[46] iVerify has tracked what it refers to as the same capability under the name CryptoWaters and characterizes it as nation state grade tooling with strong indicators of operational maturity.[47] The most significant strategic takeaway is not only the depth of the exploit inventory, but the evidence that the capability, or at minimum key components of it, has circulated across multiple actors with divergent alignments and motivations, including Google tracked clusters UNC6353 and UNC6691. This pattern is consistent with an ecosystem in which high end exploit capabilities can spread beyond a single sponsor through contractor led development, potentially on behalf of the National Security Agency (NSA) as the ultimate customer, and then further proliferate to other state sponsored advanced and persistent threat groups via insider theft and exploit broker networks.

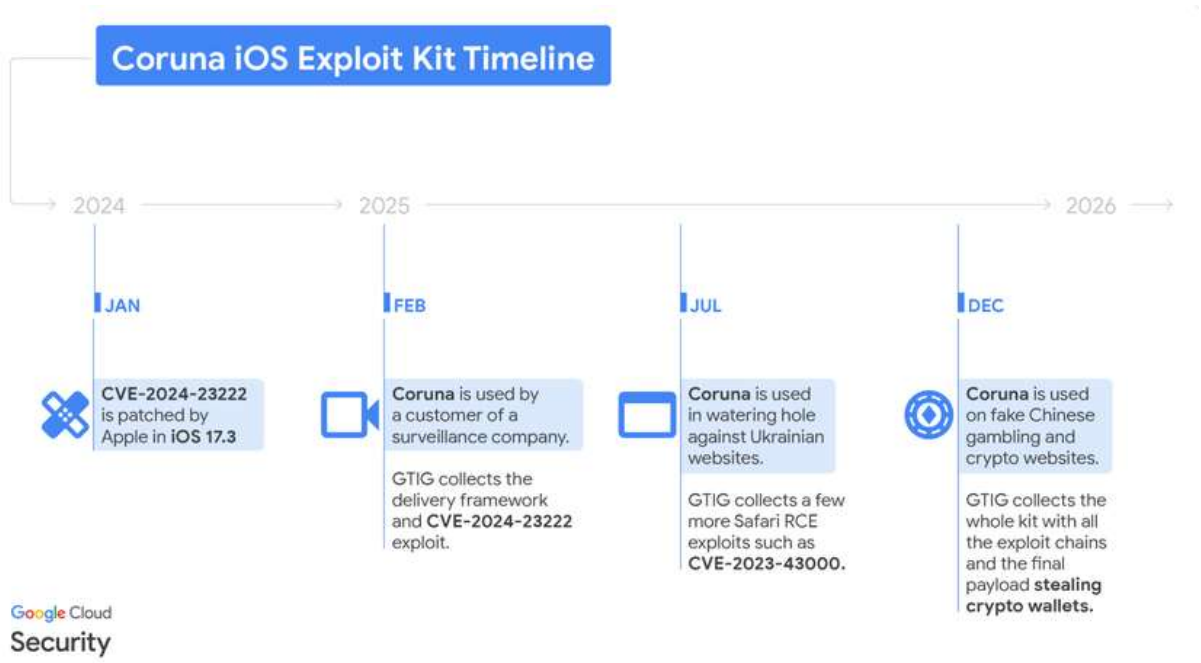

Figure 6- Timeline of the Corum iOS exploit kit timeline (source: Google)

Operational workflow

Public reporting consistently describes an infection flow triggered by a victim visiting a malicious or compromised website. A JavaScript based fingerprinting stage profiles the device and selects an appropriate exploitation chain. This selection step is important because it indicates the operator expects heterogeneous targets and is actively managing compatibility, rather than delivering a single exploit broadly and hoping for success.

[46] https://cloud.google.com/blog/topics/threat-intelligence/coruna-powerful-ios-exploit-kit/
[47] https://iverify.io/blog/coruna-inside-the-nation-state-grade-ios-exploit-kit-we-ve-been-tracking

The exploitation sequence described by GTIG and echoed in subsequent coverage follows the standard progression seen in sophisticated iOS compromises. The initial stage achieves remote code execution in WebKit within the browser context. Follow on stages escape the sandbox and then elevate privileges to reach kernel level control. The presence of multiple complete chains implies the operators can adapt to different iOS versions and mitigation configurations and still complete the full privilege escalation path.

Linkage to Operation Triangulation

Kaspersky's more recent reporting strengthens the linkage between Coruna and Operation Triangulation[48]. In its March 2026 analysis,[49] Kaspersky describes Coruna as an exploit framework and details technical ties to Operation Triangulation, including reuse and evolution of exploitation logic previously seen in the 2023 campaign. This framing is important because it suggests continuity at the level of exploit development and engineering practices rather than mere coincidence in vulnerability selection. In analytic terms, Kaspersky's findings support the assessment that at least part of Coruna's capability set shares provenance with the Triangulation toolchain, whether through shared upstream sourcing, transfer through an exploit brokerage channel, or direct reuse by operators with access to the earlier exploit inventory. This also reinforces the broader proliferation hypothesis, since a framework that incorporates updated variants of Triangulation-linked exploits is more consistent with iterative maintenance and re-deployment than with a one-off reuse event.

Attribution signals and the problem of shared capabilities

GTIG reported Coruna being used by at least two tracked clusters, UNC6353 described as state aligned Russian activity and UNC6691 described as a financially motivated cluster operating from China. In isolation, either linkage would be significant. Taken together, they imply either deliberate resale or reuse of the same kit, compromise of the developer or customer environment, or a brokered distribution model in which components of the exploit inventory were sold or traded.

[48] https://securelist.com/operation-triangulation/109842/
[49] https://securelist.com/coruna-framework-updated-operation-triangulation-exploit/119228/

Media reporting[50] adds another layer by suggesting that Trenchant[51], associated with L3Harris, partially developed Coruna, with Wired[52] discussing a potential United States government customer context. TechCrunch later reported that iPhone hacking tools likely built by a United States military contractor were used by Russian spies in Ukraine. These narratives are not perfectly reconcilable without additional evidence, but they are compatible with a single underlying dynamic: development, intended customer, and observed user can diverge over time when exploit material is copied, stolen, or resold.

Proliferation hypothesis via exploit brokerage and insider theft

The strongest publicly described mechanism for Coruna's apparent multi actor use is the intersection of insider theft and exploit brokerage. TechCrunch reported that Peter Williams, described as a former Trenchant manager, pleaded guilty to selling cyber weapons to foreign powers and stealing at least eight zero day exploits during the 2022 to 2025 period, including alleged dealings involving Operation Zero. Separately, on 24 February 2026 the United States Treasury[53] announced sanctions against an exploit broker network, including Operation Zero, under a framework focused on protecting American intellectual property.

Intelligence Online[54] describes Operation Zero, also known as Matrix LLC, as an expanding international prospecting, and notes the broker's claims about only selling to non NATO customers, a positioning that aligns with a business model serving adversarial or at least non allied state demand. While marketing claims from brokers should not be taken at face value, the broader picture supports a plausible chain of custody for exploit material moving from a contractor ecosystem into broker channels and then into multiple operational hands.

Implications for defenders

Coruna's reported targeting range through iOS 17.2.1 implies risk even for relatively modern devices when patching cadence lags behind exploitation. Web

[50] https://techcrunch.com/2026/03/10/us-military-contractor-likely-built-iphone-hacking-tools-used-by-russian-spies-in-ukraine/
[51] https://www.l3harris.com/all-capabilities/trenchant
[52] https://www.wired.com/story/coruna-iphone-hacking-toolkit-us-government/
[53] https://home.treasury.gov/news/press-releases/sb0404
[54] https://www.intelligenceonline.fr/europe-russie/2024/06/28/le-broker-de-vulnerabilites-russe-operation-zero-prospecte-a-l-international,110250313-art

based delivery lowers operational cost for the attacker and makes watering hole and lure based targeting viable. The multi stage nature of the chains means that defenders who only monitor network indicators may miss compromise events, particularly when payload delivery is tightly coupled to the browsing session and infrastructure is short lived.

The most consequential implication is that defenders should treat Coruna as an ecosystem level risk rather than a single actor tool. If the same exploit kit or key exploit components are available to multiple actors, then exposure observed in one theater can forecast exposure elsewhere, and incident response teams should avoid overfitting attribution based solely on the presence of an iOS exploitation chain consistent with Coruna.

Recommended actions aligned to this threat model

Organizations with elevated exposure to targeted surveillance should prioritize rapid iOS updates and harden web attack surface where feasible, including use of iOS Lockdown Mode for high risk users. Mobile device management policies should enforce minimum OS versions, restrict risky browsing contexts, and ensure rapid isolation and triage paths for devices suspected of compromise.

Detection and response should assume that evidence may be transient. Mobile telemetry collection, timely forensic acquisition, and playbooks specific to iOS exploitation are critical. When an organization lacks internal mobile forensic depth, pre arranging access to specialist support is advisable because the window for collecting useful artifacts can be short.

4.2.2. BlackCore, Rokh Solis, and Alleged Israeli Information Operations Against La France Insoumise During France's 2026 Municipal Elections

Blackcore operation

What French reporting often calls the BlackCore scandal is more precisely the exposure of a foreign information operation that VIGINUM[55,56], the French state service in charge of tracking foreign digital interference, identified under the name Rokh Solis. In practical terms, the operation targeted La France Insoumise, the France's main left wing political movement, during the municipal elections held on 15 and 22 March 2026.

The name BlackCore does not refer to the official French label for the campaign. It refers to the Israeli influence entity that VIGINUM says is probably linked to the technical infrastructure and tradecraft behind the operation. The core of the scandal is therefore not just one fake website or one smear story, but a broader coordinated interference effort that combined fabricated narratives, impersonation, artificial amplification, and attempts to polarize the French public debate around LFI and Muslims.

According to VIGINUM's June 2026 reporting, the operation was prepared well before election day. Some supporting assets appear to have been prepositioned as early as 2025, while the main websites used against LFI were created between 9 and 19 February 2026. The campaign became visible in March 2026, during the municipal race itself, and was partially exposed by the press on 9 March 2026, after which several assets were deleted or became inactive. The affair then moved from technical exposure to political and judicial scrutiny in May and June 2026, when Reuters, French media, and the Paris prosecutor's office reported on the possibility of foreign interference targeting LFI candidates, and when VIGINUM published both a public election report and a more detailed technical report on Rokh Solis.

The operation had two main lines of effort. The first was the direct reputational targeting of LFI and specific candidates. VIGINUM identified coordinated assets aimed at Sébastien Delogu in Marseille, François Piquemal in Toulouse, and David Guiraud in Roubaix. Delogu was targeted through false rape accusations and a

[55] https://www.sgdsn.gouv.fr/files/files/viginum/Publications/20260611_SGDSN_VIGINUM_Rapport-technique_Rokh-Solis.pdf
[56] https://www.sgdsn.gouv.fr/files/files/viginum/Publications/20260611_SGDSN_VIGINUM_Rapport-public_Elections-municipales.pdf

fabricated story presenting him as selling sexually suggestive images of himself to raise money for Gaza. Piquemal was targeted through false accusations of pedophilia, violence, and support for Hamas, including the impersonation of a legitimate child protection association to give credibility to the smear. Guiraud was attacked for his pro Palestinian positions in relation to the war between Israel and Hamas. In each case, the operational goal was not simply to criticize LFI politically, but to inject scandal, criminal suspicion, and moral contamination into the campaign environment.

The second line of effort was broader and more strategic. It tried to polarize the national digital debate by portraying LFI as aligned with Muslim communal separatism. One fake ecosystem revolved around a supposed initiative called L'Alternative 2026, presented as a platform helping Muslim voters identify local candidates who would best serve explicitly Muslim interests. This site listed numerous left wing candidates, mainly from LFI or supported by LFI, in order to suggest an ideological alignment between the party and a communitarian project. A second layer then simulated a radical Islamist endorsement of this initiative by reviving the name of Forsane Alizza, a dissolved extremist group. A third layer created the opposite pole, a fake conservative Catholic nationalist structure calling itself Renaissance Catholique Nationale, which denounced the supposed Islamist threat.This is a classic synthetic polarization tactic. The same operator appears to have manufactured both sides of the controversy in order to inflame identity tensions, draw engagement, and damage LFI by associating it with radicalism.

Technically, the campaign showed multiple markers of coordination and inauthenticity. The sites shared hosting features, overlapping metadata, common templates, and common image generation traces. VIGINUM also found organized amplification across Facebook, X, TikTok, and Instagram, using networks of fake or highly suspect accounts. Some of these accounts used AI generated profile images, generic French sounding names, synchronized comment patterns, and identical posting behavior. Others had histories suggesting re use across foreign influence operations in other countries, including Angola and possibly English speaking audiences. The campaign even spilled into the physical world. Fake tracts linked by QR codes were photographed and distributed in Marseille, and at least one TikTok account promoted physical activism in Paris. This mix of fake narratives, cross platform amplification, and limited street level staging is why the case matters operationally even though VIGINUM ultimately assessed its public reach as relatively low.

VIGINUM assessed that Rokh Solis constituted a foreign digital interference operation involving a non state actor located in Israel. Its evidence included Hebrew characters in file metadata, Israeli geolocation signals linked to some accounts,

repeated overlap with networks relaying content associated with the pro Israeli organization ELNET, and technical links to infrastructure associated with BlackCore, an Israeli influence entity that appears to provide artificial amplification and covert online influence services. VIGINUM also traced BlackCore related infrastructure to a wider Israeli cyber and influence ecosystem involving linked entities, developers, and business intermediaries. At the same time, VIGINUM explicitly stated that it could not, at this stage, identify the ultimate clients or commanditaires who may have used these services. That means the Israeli nexus is technically substantial, but the exact chain of direction remains partly unresolved in public reporting.

The political context nevertheless matters. LFI has been one of the most visible French political forces opposing Israel's military campaign in Gaza. Its leaders and candidates have repeatedly denounced what they describe as war crimes against Palestinians, participated in protests, amplified these themes in parliament and in the media, and turned the Palestinian issue into a sustained part of domestic political contestation in France.[57] This does not prove state direction, but it does provide a plausible motive for why LFI and especially strongly pro-Palestinian figures such as David Guiraud would be selected for hostile influence activity. The structure of the campaign also supports that reading, because some of the narratives were designed not only to damage candidates personally, but also to weaponize LFI's association with Gaza, Islam, and Middle East politics.

From a national security perspective, the significance of the affair is that French authorities treated it as a genuine foreign interference case affecting an election, even though its online visibility remained limited. VIGINUM included it among the four foreign digital interference cases detected during the 2026 municipal cycle. The RCPE framework informed victims, engaged platforms, and helped reduce the campaign's reach. After media exposure, a number of the accounts and sites were removed, and the activity slowed significantly.

This case also matters because it fits a pre existing pattern of pressure against LFI from Middle Eastern actors. The alleged Israeli linked Rokh Solis and BlackCore operation recalls an earlier Gulf episode involving an LFI figure, Carlos Martens Bilongo, where French reporting said that TRACFIN appeared to have looked into him under pressure from the United Arab Emirates, in a context often read politically as part of broader hostility from the Saudi Emirati sphere toward LFI's positions.[58] In other words, the BlackCore affair should not be understood as a totally new

[57] https://www.radiofrance.fr/franceculture/podcasts/culture-de-l-info/coup-de-colere-europeen-apres-qu-une-flottille-pour-gaza-a-ete-instrumentalisee-par-l-extreme-droite-israelienne-4602567

[58] https://www.humanite.fr/politique/cop-28/tracfin-aurait-enquete-sur-le-depute-carlos-martens-bilongo-sous-la-pression-des-emirats-arabes-unis

phenomenon. It looks more like the digital and information warfare version of a pattern that had already touched LFI before, namely the use of foreign pressure, reputational damage, and institutional leverage against a movement whose positions on Palestine and the Middle East openly clash with the interests of powerful regional actors.

4.2.3. Outlook

The second half of 2026 is expected to see continued competition between the United States and its principal strategic adversaries in cyberspace, with a sustained emphasis on intelligence collection, cloud compromise, and supply chain access. Chinese actors are likely to further expand long-term pre-positioning within critical infrastructure, while Russian services will continue targeting government institutions and defence-related organizations. The rapid integration of AI into offensive operations, combined with the increasing exploitation of edge infrastructure and trusted third-party providers, is expected to shorten operational timelines and complicate attribution. Increased cooperation between Five Eyes partners and continued public attribution efforts should enhance collective defence but are unlikely to deter long-term espionage campaigns.

4.3. Middle East



During the first half of 2026, the Middle East cyber threat landscape was **shaped by the convergence of regional conflict**, **state-sponsored cyber operations**, and increasingly **aggressive hacktivist activity**. Escalating tensions involving **Iran**, **Israel**, and their respective allies drove a significant increase in cyber operations that ranged from **espionage**, illustrated notably by intrusion sets such as **Muddy Water**, to **disruptive campaigns** targeting public and private-sector organizations, illustrated primally by the hacktivist persona **Handala**.

While highly visible activities such as **distributed denial-of-service** (DDoS) attacks, **website defacements**, and **data leak** operations remained prevalent, threat actors increasingly shifted toward more sophisticated objectives, including **long-term network access**, **intelligence collection**, and targeting of **critical infrastructure**.

Iranian-aligned threat groups remained among the most active actors in the region, focusing on government, defense, energy, telecommunications, and technology sectors, while cyber activities increasingly **mirrored and supported ongoing geopolitical and military developments**.

At the same time, cyber-enabled **influence operations** and **hacktivist campaigns** became a **persistent feature of the threat environment**, blurring the lines between state-directed activity and ideologically motivated actors. Collectively, these developments reinforced the Middle East's position as one of the **world's most dynamic cyber conflict arenas during H1 2026**, where cyber operations served not only as tools of espionage and disruption but also as **instruments of strategic competition and regional power projection**.

4.3.1. Iran-Centric Cyber Operations: The Primary Regional Driver

In 2026, the conflict involving Iran demonstrated that **datacenters in the Gulf could be directly exposed to the effects of drone warfare**. Three AWS datacenters in the Middle East were affected by drone strikes. Two facilities in the United Arab Emirates were directly hit. A third site, located in Bahrain, sustained damage following a strike in the immediate vicinity.[59]

If Microsoft datacenters in the region were affected in a comparable manner, customers could experience temporary degradation or outages impacting **Azure services**, **Microsoft 365 applications**, and **Microsoft Entra ID authentication**, despite Microsoft's built-in redundancy and disaster recovery capabilities

In Iran's case, the events of 2026 showed how physical attack capabilities, particularly **drones and missiles**, can compensate for limitations in cyber sophistication. The incidents also highlighted that the resilience of cloud environments depends not only on cybersecurity but also on protection against kinetic attacks on the underlying physical infrastructure.

According to *Politico*, Israel **also employed kinetic strike** early in the conflict in March, to target what the Israel Defense Forces (IDF) described as the cyber warfare headquarters of Iran's Islamic Revolutionary Guard Corps (IRGC) in Tehran.[60] The IDF stated that it conducted a "wide-scale strike" against a complex of military facilities on the eastern outskirts of the capital, claiming that the IRGC's "**cyber and electronic headquarters**" and Intelligence Directorate were among the sites hit.

According to *Iran International*, the Israeli military announced that it killed several senior Iranian intelligence officials during the opening strike of Operation **Roaring Lion**, including **Yahya Hamidi**, Iran's deputy minister of intelligence.[61] According to sources, He was also a **senior leader of the Handala hacktivist group**.[62]

While Israeli officials argued that the strike could significantly disrupt Iran's ability to conduct cyber operations, However, Iran's cyber apparatus extends beyond the Ministry of Intelligence and includes the Islamic Revolutionary Guard Corps (IRGC), specialized cyber units, contractors, and affiliated hacker groups that can continue operations **even when senior leaders are removed**.

---

[59] *https://www.usine-digitale.fr/informatique/cloud/guerre-en-iran-trois-data-centers-aws-touches-par-des-frappes-de-drones-au-moyen-orient.JHHELZZOFNCV5HEEHONED7NBUE.html*
[60] *https://www.politico.com/news/2026/03/04/israel-iran-cyber-headquarters-00813364*
[61] *https://www.iranintl.com/en/202603029390*
[62] *https://x.com/NarimanGharib/status/2028405938793701758*

Moreover, as noted in *Politico*, Iranian cyber operations frequently rely on **external proxy actors and ideologically aligned groups**, including networks operating outside Iran. Experts quoted in the article emphasized that "cyber is now embedded in modern conflict" and does not require all operators to be physically located in Tehran. As a result, even successful kinetic strikes against intelligence leaders or cyber headquarters may disrupt command-and-control, coordination, and planning in the short term, but they are **unlikely to eliminate Iran's overall cyber-spying and cyberattack capacity**, which is **decentralized** and resilient by design.

4.3.2. Hacktivism: the new porous constant

Handala



In the first half of 2026, the Iran-linked hacktivist group **Handala** significantly escalated its operations, expanding from its traditional focus on Israeli targets to include high-profile U.S., Gulf, and regional organizations. Early in the year, the group claimed compromises of an Israeli energy exploration company, attacks against Israeli civilian healthcare systems, and intrusions affecting Jordanian fuel infrastructure. In March, Handala launched its **"RedWanted"** platform, which publicly listed individuals and organizations perceived as supporting Israel, while simultaneously claiming major breaches against **Israel Opportunity Energy** and the **Sharjah National Oil Corporation**, allegedly exfiltrating large volumes of sensitive corporate data.

The same month marked the group's most prominent activity, including a destructive cyberattack against U.S. medical technology company **Stryker**, where security reporting indicated the use of wiper techniques designed to cause widespread operational disruption rather than generate financial gain. Discussing the alleged **Stryker attack**, **Tim Haugh** (former NSA director) explained that the operation did not rely on sophisticated malware or novel exploits. Instead, the

attackers reportedly used **social engineering and legitimate credentials** to obtain access and then leveraged authorized capabilities to delete systems and data.[63]

During the internet disruptions and blackouts that affected Iran,[64] Check Point Research observed signs that Handala's operational security deteriorated, with some activity reportedly originating from Iranian IP addresses as well as **Starlink satellite internet connections**.[65] The use of Starlink may have provided the group with an alternative means of maintaining connectivity and supporting cyber operations during periods when Iran's domestic internet access was restricted or unstable.

A noteworthy parallel emerges between Handala operators' use of Starlink and recent reporting that Israel developed capabilities to identify or geolocate Starlink users. According to a *Haaretz* investigation,[66] two Israeli-linked cyber intelligence companies have developed technologies capable of **locating Starlink terminals worldwide and, in some cases, identifying the people using them** without hacking Starlink itself. Instead, the systems rely on large-scale **data fusion**, combining geolocation data, advertising identifiers, smartphone telemetry, browsing activity, and other digital traces to correlate satellite terminals with real-world users. An *Intelligence Online* article from May 2026, confirms the growing demand for such capabilities in the Gulf and broader Middle East, where satellite internet is increasingly used in conflict zones, sanctions environments, and similar internet-blackout scenarios as in Iran.[67]

Later in March, Handala also claimed responsibility for compromising the personal email account of FBI Director **Kash Patel**, publishing hundreds of messages and documents online.[68] Security researchers and government agencies increasingly assessed Handala as a front or proxy persona linked to Iran's Ministry of Intelligence and Security (MOIS), rather than an independent hacktivist collective.[69]

---

[63] *https://therecord.media/iran-cyber-warfare-haugh*

[64] *https://www.kentik.com/blog/internet-and-airstrikes-tracking-irans-extended-communication-blackout/*

[65] *https://x.com/_CPResearch_/status/2013349461070586054*

[66] *https://www.haaretz.com/israel-news/security-aviation/2026-05-12/ty-article-magazine/.premium/starlink-users-beware-israeli-tech-can-reveal-your-identity/0000019e-17f1-d618-adde-17f3e27d0000*

[67] *https://www.intelligenceonline.com/middle-east-and-africa/2026/05/11/israeli-cyber-industry-veteran-in-the-gulf-tracking-starlink-users,110731012-art*

[68] *https://www.lemonde.fr/pixels/article/2026/03/27/des-hackeurs-iraniens-revendiquent-le-piratage-de-la-boite-mail-personnelle-du-directeur-du-fbi_6674660_4408996.html?*

[69] *https://www.ic3.gov/CSA/2026/260320.pdf*

Exposed PLC exploitation galore by Iran-aligned threat actors

In April 2026, CISA's advisory **AA26-097A** warned on Iranian-affiliated threat actors actively targeting **internet-exposed programmable logic controllers (PLCs)** across multiple U.S. critical infrastructure sectors, including energy, water and wastewater, and local government organizations.[70] The main method consisting of scanning ranges of IPs from a specifically targeted country, looking for open VNC sessions with authentication on various default ports, and hoping for it to be connected to an HMI instance.

Attacking exposed VNC assets is a **low-sophistication yet highly effective tactic for hacktivists** because it exploits one of the most common weaknesses in remote-access hygiene: publicly accessible systems protected only by weak or default credentials. Unlike advanced intrusions that require custom malware or deep OT expertise, scanning the internet for open VNC ports and attempting credential stuffing or brute-force attacks demands **minimal technical skill** and readily available tools. Once accessed, these systems can provide direct control over servers, operator consoles, or even OT interfaces, which can cause **real operational disruption**, including temporary outages and **physical consequences.** these groups seek **visibility and notoriety**, frequently exaggerating claims of damage while still demonstrating a willingness to inflict real harm. It warns that the simplicity and replicability of their TTPs increase the likelihood of **copycat activity** by other malicious actors.

In January and February 2026, the same techniques continued to be employed by by smaller groups such as pro-Russia *QuietSec*, *Hider_Nex*, *OverFlame*, *Perun Svarog*, Pro-China *Infrastructure Destruction Squad* (IDS), and pro-Iran *Fattahh Cyber Team*, *APT Iran*. **Primarily targeting systems in Italy amidst the Winter Olympic Games**.

[70] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a*

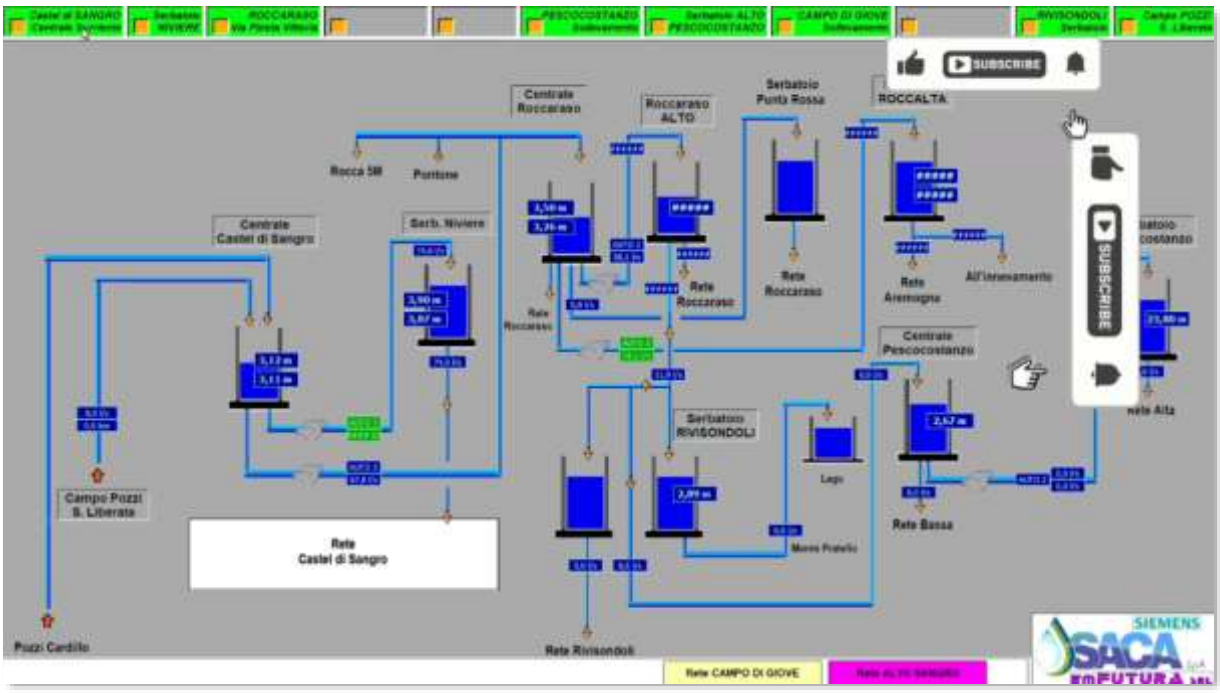

Figure 7. Screenshot of a video posted by OverFlame on its Telegram channel in January 2026, in which a threat actor is seen modifying values of a HMI located in Italy, in the context of the winter Olympic.

Compared with many Iranian hacktivist groups that focus on DDoS attacks, website defacements, and publicity-driven hack-and-leak operations, **Ababil of Minab** and **Nasir Security** have distinguished themselves through more targeted and impactful campaigns. **Ababil of Minab** stood out with intrusions involving data theft, deletion of virtual machines, destruction of databases, and wiping of backup infrastructure at transportation and enterprise organizations in the United States, Israel, Saudi Arabia, and Turkey.[71] According to *Gambit Security*, ties campaigns operated by the intrusion set to infrastructure and activity previously attributed by Israel's National Cyber Directorate (INCD) to Iran's Ministry of Intelligence and Security.

By contrast, **Nasir Security** has primarily followed a disclosure and breach-focused model, publicly claiming intrusions into government, aviation, and energy-sector organizations across the Middle East and publishing alleged stolen data to support pro-Iran messaging. Its operations have emphasized espionage, data exposure, and influence objectives, often targeting critical infrastructure and supply-chain

[71] *https://gambit.security/blog-posts/babil-of-minab-iran-mois-destruction-campaign*

vendors, rather than the service disruptions commonly associated with other Iranian hacktivist groups.[72]

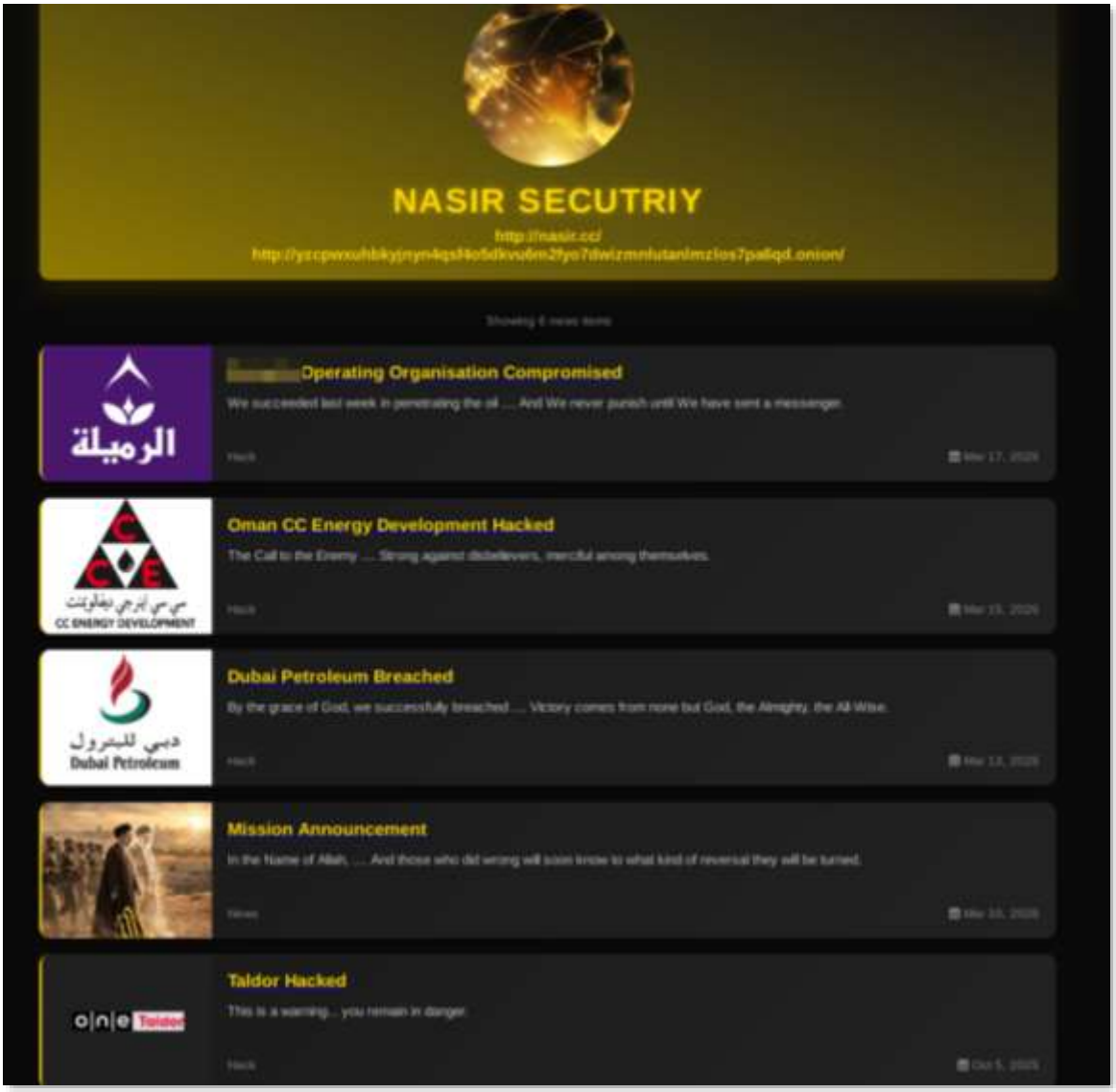

Figure 8. Front page of the DLS operated by the Nasir Security hacktivist persona.

Pay2Key occupied a much blurrier space between state-sponsored activity, hacktivism, and cybercrime. Pay2Key has been linked to Iranian state interests, yet the group operates through ransomware and ransomware-as-a-service (RaaS) models that resemble conventional criminal enterprises.[73] It has solicited affiliates on Russian-language cybercrime forums, offered revenue-sharing schemes, collected ransom payments, and even attempted to sell parts of its infrastructure,

[72] *https://www.resecurity.com/es/blog/article/pro-iranian-nasir-security-is-targeting-the-energy-sector-in-the-middle-east*
[73] *https://www.halcyon.ai/ransomware-research-reports/pay2key-iranian-linked-ransomware-is-back-back-again*

all while disproportionately targeting organizations aligned with Iran's geopolitical adversaries, particularly in Israel and the United States. Analysts have therefore described Pay2Key as a form of**"pseudo-ransomware"**, using criminal tactics and financial incentives to support strategic state objectives.

In this sense, Pay2Key reflects a broader trend in modern cyber conflict: rather than presenting itself as a hacktivist or intelligence operation, it leverages the **criminal ransomware ecosystem**, affiliate networks, and darknet marketplaces as cover, providing Tehran with **greater deniability** while still enabling cyber operations that advance national interests. The group's activity often intensifies during periods of heightened tension involving Iran, reinforcing suspicions that **geopolitical objectives play a role alongside any financial motivation**.

Targeting Iran

In June 2026, a cyberattack disrupted the operations of several major Iranian banks, causing interruptions to banking and card-payment services. Iranian authorities initially described the incident as a **limited attack against the shared communications infrastructure** of four state-owned banks, Bank Melli (National Bank of Iran), Bank Tejarat, Bank Saderat, and Export Development-related banking infrastructure—while maintaining that customer data was not compromised and no records were deleted. Recovery efforts focused on restoring connectivity and banking operations after the disruption affected interbank services and card transactions.[74]

According to reporting by *The Telegraph*,[75] the targeted banks were viewed as being connected to the Islamic Revolutionary Guard Corps (IRGC), and the attack forced some institutions to suspend card-related services. While no actor publicly claimed responsibility, Israeli security sources and analysts interviewed by the newspaper suggested the operation bore similarities to previous campaigns attributed to **Predatory Sparrow (Gonjeshke Darande)**, a well-known anti-Iranian hacking group widely suspected of links to Israeli cyber operations. The timing of the attack—shortly after a US-Iran agreement involving the release of frozen Iranian funds—led

[74] *https://en.yenisafak.com/technology/iran-says-cyberattack-disrupted-four-major-banks-3719521?*

[75] *https://www.telegraph.co.uk/world-news/2026/06/23/israel-behind-cyber-attack-on-iranian-banks/*

some observers to speculate that the objective was to hinder Iran's ability to access or move financial resources.

The incident strongly reflected the pattern established by **Predatory Sparrow's operations a year earlier**. In 2025, the group reportedly targeted Bank Sepah and other strategic Iranian infrastructure as part of a broader campaign designed to create economic disruption and undermine systems connected to the Iranian state. Rather than stealing customer funds or conducting conventional financially motivated cybercrime, Predatory Sparrow's hallmark has been **strategic disruption of critical services**: railways, fuel distribution, steel production, and banking systems, to create operational and psychological pressure on the Iranian government. The 2026 attacks on IRGC-linked banks fit this model: they disrupted services and targeted institutions of strategic value while avoiding widespread destruction of customer data, indicating an objective centered on economic pressure and signalling rather than direct financial theft.

In a less sophisticated manner but still noticeable, **VXSECT**, a pro-Kurdish hacktivist collective, who usually targeted Turkish entities, started attacking Iranian companies in June 2026, and notably a nuclear facility, with the same hack-and-leak methods on *Telegram* as other hacktivists.

4.3.3. Rain of sanctions and arrest warrants

Western governments increasingly used **cyber sanctions, financial restrictions, public attribution, rewards programs, and law-enforcement actions** to raise the cost of Iranian cyber operations and limit Tehran's ability to fund, conduct, and benefit from malicious cyber activity.

The **European Union** expanded its cyber diplomacy toolbox by directly sanctioning Iranian cyber actors linked to operations affecting EU member states. In March 2026, the Council of the EU imposed restrictive measures on **Emennet Pasargad**, an Iranian cyber company accused of accessing a French subscriber database, attempting to sell the data on the dark web, compromising advertising billboards during the 2024 Paris Olympics to spread disinformation, and attacking a Swedish SMS service. The sanctions included **asset freezes**, a prohibition on EU persons providing funds or economic resources to the company, and travel restrictions where applicable. The move demonstrated the EU's willingness to publicly attribute

malicious cyber activity and use economic measures as a deterrent rather than relying solely on criminal prosecutions.[76]

The **United States** complemented sanctions with a mixture of financial pressure and public exposure. Through the State Department's **Rewards for Justice** program, Washington offered rewards of up to **$10 million** for information on Emennet Pasargad[77] and associated individuals involved in cyber-enabled election interference. U.S. authorities accused the company of conducting a multi-faceted influence operation targeting the 2020 U.S. presidential election, including voter intimidation, disinformation campaigns, unauthorized access attempts against election-related systems, and broader cyber espionage activity targeting sectors such as finance, telecommunications, transportation, and energy. The rewards program effectively turned cyber operators into internationally wanted targets while encouraging intelligence collection from third parties.

The United States also expanded financial sanctions beyond individual hackers to the infrastructure that allegedly enabled Iranian cyber operations and sanctions evasion. In June 2026, the Treasury Department designated **Nobitex**, Iran's largest cryptocurrency exchange, together with several other Iranian digital-asset exchanges and senior executives.[78] Treasury alleged that these platforms facilitated sanctions evasion, supported transactions linked to the Islamic Revolutionary Guard Corps, enabled movement of funds associated with Iran-linked ransomware actors, and helped the regime access international financial networks. By targeting cryptocurrency exchanges rather than only hackers, Washington sought to disrupt the financial ecosystem supporting Iranian state activities and cyber operations.

Alongside sanctions, Western governments increasingly employed **"naming and shaming" and judicial actions**. Public initiatives such as the Iranian Threat Actors database catalogued individuals linked to the IRGC and Ministry of Intelligence and Security,[79] helping expose their identities and affiliations. Meanwhile, U.S. investigations continued to pursue Iranian cyber operators years after their alleged activities occurred. A notable example was the 2026 arrest in Montenegro of an Iranian national wanted by the United States in connection with a large-scale

[76] *https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/*
[77] *https://rewardsforjustice.net/fr/rewards/emennet-pasargad/*
[78] *https://home.treasury.gov/news/press-releases/sb0519*
[79] *https://iranianthreatactors.com/*

university-hacking campaign that allegedly benefited the IRGC.[80] The case illustrated how sanctions, indictments, international cooperation, and extradition efforts can work together to impose long-term consequences on Iranian cyber actors.



Figure 9. FBI poster warrant for the arrest of nine Iranian hackers charged in 2018 over the Mabna Institute campaign. Source: https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers.

[80] *https://www.iranintl.com/en/202606267117*

4.3.4. Outlook

The cyber landscape in the Middle East is expected to remain closely tied to regional geopolitical developments throughout the remainder of 2026. Escalating tensions involving Iran, Israel, and their regional partners are likely to continue driving retaliatory cyber operations targeting government institutions, financial services, energy infrastructure, and telecommunications providers. Hybrid campaigns combining cyber disruption, information operations, and strategic messaging are expected to intensify, while hacktivist collectives will likely remain active as force multipliers for broader state interests. The increasing use of cyber capabilities alongside kinetic operations suggests that cyberspace will remain a key instrument of regional deterrence and escalation management.

4.4. Asia



For H1 2026, focus on the Asian region was made particularly on China, North Korea, South-East Asia and other countries of interest (Japan, South Korea, Taiwan). The main subjects were related to espionage operation, state-sponsored threats targeting critical infrastructure, supply-chain compromises, AI for automating social engineering and influence operations, as well as various scams and cybercrime activities.

4.4.1. China

China is the main country of interest in the Asian region. Having the most developed cyber capabilities, threat actors linked to the country perform a variety of activities, including espionage against critical sectors of foreign nations, compromising devices to use as infrastructure or recruiting insiders to help make targeted attacks. In the first quarter of 2026, we noted a focus on the Chinese cybercrime ecosystem, with more phishing-as-a-service kits and a scaling of infrastructure for botnets.
Due to the size of its information technology sector and its role as a global manufacturer, the country was also a prominent target for dataleak and ransomware threats. Several high-profile companies and large-scale compromise against Chinese assets were claimed, sometimes impacting organizations worldwide.

State-linked operations: critical sectors (telecom, gov, law enforcement, military), new clusters, and stealthy tooling

Chinese state-linked cyber operations have demonstrated a strategic focus on long-term "positioning" and high-precision intelligence collection, moving away from bulk data theft toward the establishment of "sleeper cells" within critical infrastructure[81]. A primary focus is the global telecommunications sector, where actors like Red Menshen and UNC3886 embed stealthy access mechanisms deep

[81] https://origin-unit42.paloaltonetworks.com/espionage-campaign-against-military-targets/

within the telecom backbone to monitor sensitive communications and track high-value geopolitical targets[82] . These operations often target the "central nervous system" of digital connectivity, including routing systems and authentication services, to gain visibility into subscriber metadata and signaling flows[83].

The targeting scope is extensive, spanning military, government, and law enforcement sectors across Southeast Asia, Europe, the Middle East, and North America[84]. Notable incidents include a "major incident" breach of an internal FBI surveillance system containing law enforcement sensitive information[85] and the compromise of the Cuban embassy in Washington to monitor diplomatic communications[86]. In Southeast Asia, clusters like CL-STA-1087 and "TrueChaos" have targeted military organizations and government entities, often utilizing zero-day vulnerabilities in applications like TrueConf to deploy payloads[87].

Tooling has evolved to include a mix of legacy frameworks and highly specialized, stealthy implants. While several actors continue to use established tools like PlugX and Cobalt Strike for rapid deployment, as seen in campaigns targeting Qatar[88] and the Persian Gulf[89], some are also deploying new, custom-built assets[90]. These include the AppleChris and MemFun backdoors, the "FIRESTARTER" implant for Cisco devices[91], and the "Gridtide" backdoor, which conceals C2 communications within Google Sheets[92]. Additionally, the "VoidLink" framework represents a move toward AI-enabled, compile-on-demand tools that can create implants dynamically for operators[93].

Operational stealth is further enhanced through the use of "covert networks" and advanced persistence techniques. Actors frequently employ DLL sideloading of legitimate signed binaries to execute modular RATs, such as LOTUSLITE[94] and

[82] https://therecord.media/researchers-warn-volt-typhoon-still-active-critical-infrastructure
[83] https://www.rapid7.com/blog/post/tr-bpfdoor-telecom-networks-sleeper-cells-threat-research-report/
[84] https://www.politico.com/news/2026/04/01/fbi-hack-surveillance-system-major-incident-00854237
[85] https://www.wsj.com/politics/national-security/china-suspected-in-breach-of-fbi-surveillance-network-2c9d1691
[86] https://www.bloomberg.com/news/articles/2026-04-29/chinese-hackers-spied-on-cuban-embassy-as-us-prepared-blockade
[87] https://research.checkpoint.com/2026/operation-truechaos-0-day-exploitation-against-southeast-asian-government-targets/
[88] https://blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions/
[89] https://www.zscaler.com/blogs/security-research/china-nexus-threat-actor-targets-persian-gulf-region-plugx
[90] https://www.proofpoint.com/us/blog/threat-insight/id-come-running-back-eu-again-ta416-resumes-european-government-espionage
[91] https://blog.talosintelligence.com/uat-4356-firestarter/
[92] https://therecord.media/china-cyber-espionage-google-disrupt
[93] https://blog.talosintelligence.com/voidlink/
[94] https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/#-m_BvsUlu9

ShadowPad[95]. In some high-OpSec environments, such as "Operation Highland Velvet Ant," attackers have replaced critical system components like PAM modules and OpenSSH binaries with backdoored versions to control the entire authentication stack while disabling credential logging to erase their forensic footprint[96]. This level of discipline is mirrored in the use of "Operational Relay Boxes" (ORBs) to mask the origin of attacks and the exploitation of edge devices to create mass-scanning proxy nodes[97].

Acquiring strategic intelligence by leveraging a multi-layered approach

Chinese threat actors have increasingly shifted their focus toward the exploitation of trusted developer ecosystems, the use of compromised devices and the recruitment of insiders to achieve strategic intelligence goals. A primary example is the "Lotus Blossom" campaign, which subverted the Notepad++ update pipeline to deliver the "Chrysalis" backdoor[98]. Rather than a broad attack, this operation was characterized by extreme precision, selectively diverting malicious updates only to high-value targets, such as administrators and developers, to maintain a low operational profile and avoid detection[99].

The use of compromised devices has evolved into the strategic deployment of "covert networks" or Operational Relay Boxes (ORBs)[100]. These networks consist of compromised SOHO routers, IoT devices, and VPSs, which allow actors like Volt Typhoon and Flax Typhoon to mask their origins, bypass geofencing, and pre-position themselves within critical national infrastructure months before an attack[101]. This infrastructure is further augmented by tools like "DKnife," an adversary-in-the-middle framework that hijacks binary downloads and application updates via edge devices to deliver backdoors like ShadowPad[102].

Parallel to these technical efforts, there is a concerted push to recruit insiders through deceptive social engineering and economic incentives[103]. Intelligence services use fake consulting firms, AI-generated personas, and professional

[95] https://www.trendmicro.com/en_us/research/26/d/inside-shadow-earth-053.html
[96] https://www.sygnia.co/blog/operation-highland-velvet-ant/
[97] https://blog.talosintelligence.com/uat-9244/
[98] https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/
[99] https://dti.domaintools.com/research/lotus-blossom-and-the-notepad-supply-chain-espionage-campaign
[100] https://www.ic3.gov/CSA/2026/260423.pdf
[101] https://www.team-cymru.com/post/tracking-orbs-on-singapores-telecommunications-networks
[102] https://blog.talosintelligence.com/knife-cutting-the-edge/
[103] https://therecord.media/five-eyes-warns-chinese-spies-are-using-job-sites-to-recruit-insiders

networking sites like LinkedIn to target government employees, military personnel, and academics with access to privileged information[104]. These efforts range from requesting policy assessments for payment[105] to the direct theft of trade secrets, as seen in the conviction of a former Google engineer who stole AI infrastructure secrets for the benefit of the PRC[106].

The breadth of these insider threats extends to the direct recruitment of specialized expertise for military advancement. In one instance, a former U.S. Air Force officer was accused of conspiring with a convicted hacker to provide combat aircraft training to the People's Liberation Army Air Force[107]. Together, these tactics combining the abuse of trusted software supply chains, the scaling of covert device networks, and the aggressive recruitment of human insiders, demonstrate a multi-layered approach to acquiring sensitive technological and geopolitical intelligence.

Infrastructure scaling: hosting ecosystems, botnets, and phishing-as-a-service (PhaaS)

Chinese infrastructure has become a central hub for large-scale malicious operations, characterized by a heavy concentration of Command-and-Control (C2) servers hosted on high-capacity networks[108]. Analysis shows that nearly half of observed C2 servers are hosted by China Unicom, with Alibaba Cloud and Tencent also serving as preferred, scalable platforms for both C2 and phishing activity. This infrastructure supports a diverse range of threats, from state-linked APTs and RATs to cryptominers and framework-driven abuse using tools like Cobalt Strike and Vshell[109].

The region is a powerhouse for botnet scaling, particularly through the exploitation of IoT and SOHO devices. The JDY botnet, linked to actors like Volt Typhoon, utilizes over 1,500 compromised devices as high-performance scanners to map exposed

[104] https://www.justice.gov/opa/pr/justice-department-fbi-disable-13-websites-backed-suspected-chinese-agents-sought-sensitive
[105] https://www.nextgov.com/people/2026/01/suspected-chinese-spies-targeted-former-state-official-venezuela-research/410943/
[106] https://www.justice.gov/usao-ndca/pr/former-google-engineer-found-guilty-economic-espionage-and-theft-confidential-ai
[107] https://therecord.media/former-air-force-officer-arrested-for-working-with-hacker-flight-training-china

[108] https://hunt.io/blog/china-hosting-malware-c2-infrastructure
[109] https://censys.com/blog/vshell/

services at scale[110]. Similarly, the Badbox 2.0 botnet is powered by malware pre-installed on Android TV streaming boxes, creating a vast network of infected devices[111]. This trend extends to the firmware level, where the Keenadu backdoor is integrated directly into device firmware during the build phase or via OTA updates, linking it to other prolific botnets like Triada and Vo1d[112].

A sophisticated "Phishing-as-a-Service" (PhaaS) ecosystem has emerged within the Chinese-language underground, moving beyond simple password harvesting toward real-time interception of one-time passcodes (OTPs) to bypass multi-factor authentication (MFA)[113]. These services are often marketed openly on Telegram and focus on transforming stolen payment data into tokenized assets within digital wallets]. This ecosystem is highly professionalized, offering a complete suite of ancillary services, including the sale of PII, VPS hosting, and money laundering.

The scale of these operations is further evidenced by the "Outsider Enterprise," a China-based network that distributes phishing kits to blast fake text campaigns, resulting in millions of fraudulent URLs and millions of spam messages sent to Android users[114]. Additionally, these actors employ large-scale SEO poisoning campaigns, such as those using BADIIS malware, to compromise thousands of Windows servers globally for the purpose of monetizing illicit gambling advertisements[115].

Influence operations: automation + persistent targeting

China-linked influence operations continued to target victims of political interest for the Communist Pary in H1 2026. The use of AI models to automate bot operations is a growing theme which fuels the expansion of these influence operations.

The main narratives pushed are related to areas of interest for the Communist Party, linked to the overall news cycle. For instance, pro-Iran claims were pushed by

[110] https://www.lumen.com/blog/en-us/expanded-jdy-iot-and-soho-botnet-enables-rapid-vulnerability-exploitation
[111] https://krebsonsecurity.com/2026/01/who-operates-the-badbox-2-0-botnet/
[112] https://securelist.com/keenadu-android-backdoor/118913/
[113] https://cloud.google.com/blog/topics/threat-intelligence/chinese-language-phishing-services/?hl=en
[114] https://blog.google/innovation-and-ai/technology/safety-security/combatting-ai-scams/

[115] https://www.elastic.co/security-labs/badiis-to-the-bone-new-insights-to-global-seo-poisoning-campaign

state media and pro-China social media accounts, with the aim of influencing the opinion of residents in Taiwan, China and the Chinese diaspora[116]. Going further into themes related to the war between the United States and Iran, narratives were pushed by Chinese accounts stating that Taiwan would run out of liquefied natural gas (LNG) and face electricity blackouts due to Iran's restrictions on tankers passing through the Strait of Hormuz. The Taiwanese Ministry of Economic Affairs had to publicly rebuke the false claims[117].

The Spamouflage operation, active since 2017, targeted Tibetans voting for their parliament-in-exile during elections taking place in April 2026[118]. By promoting content discrediting candidates, the election process and the in-exile government, the aim is to drive wedges within the Tibetan community, erode trust in the government and weaken its voice and international support. However, analysts noted that the actual output of the operation was limited.

Related to AI, Chinese actors used AI models such as OpenAI's ChatGPT to help create influence campaigns aimed at American audiences[119]. These operations promoted content related to debate surrounding AI, mainly linked to claimed rising cost of electricity for American family due to AI datacentre electricity consumption. Other accounts promoted content claiming that Trump's tariffs were domination attempts and contrary to the legitimate tech competition. They also falsely claimed that OpenAI's user data were compromised.

Data exposure / leak narratives: high-value targets and alleged large-scale compromise

China was targeted by leak operations against high-value targets and critical sectors. This highlights that in the context of a global cyberwar, the country is concurrently an attacker and a victim. Some of these breaches may have a high impact.

For example, a RansomHub attack against the Chinese electronic component manufacturer Luxshare exposed files belonging to Apple, Nvidia, Tesla, LG[120]. This

[116] https://www.newsguardrealitycheck.com/p/china-pushes-pro-iran-war-claims
[117] https://www.taipeitimes.com/News/taiwan/archives/2026/03/29/2003854659
[118] https://dfrlab.org/2026/04/24/china-linked-spamouflage-targets-tibetan-parliament-in-exile-elections/
[119] https://openai.com/index/prc-linked-influence-operations-ai-debates/
[120] https://cybernews.com/security/luxshare-apple-iphone-assembler-breach/

incident reveals that the role of China as a global manufacturer makes the country a prominent target of interest. Other manufacturer of high-value multinational companies can be targeted for financial or espionage purposes. We remember that in 2025, several leaks against companies linked to the government sector and APT groups were exposed. In 2026, this trend continued and critical sectors linked to the Military, AI, were the target of dataleak operations. Data from the National Supercomputing Center (NSCC) in Tianjin was allegedly leaked, with documents related to highly classified defense documents and missile schematics[121] [122].

Fake applications regularly target Chinese-speaking users, specifically in the crypto industry, with the aim of stealing user data and finances[123]. We noted one specific instance, where the fake wallet stealer was embedded in fake crypto wallet applications.

Supply-chain attacks are another type of threats that can impact China. We noted that such attack impacted the Apifox Desktop Client, developed by Guangzhou Ruihu Technology Co, via a compromised official CDN Script[124].

4.4.2. North Korea

The DPRK (Democratic People's Republic of Korea), also known informally as North Korea, is the second most important country in the Asian region in terms of cyber capabilities. For H1 2026, the country continued to perform what it does best: compromising developers to perform supply-chain attacks, with a specific focus on npm packages as AI prompted their popularity, infiltrating foreign companies by masquerading as legitimate remote IT workers, stealing cryptocurrencies and laundering them for financial reasons.

The analysis of those intrusions reveals that North-Korean operations can be interconnected. A threat actor can perform fake interviews to lure a developer of a large-scale cryptocurrency project by redirecting him to compromised npm packages, which will enable a high-volume cryptocurrency theft.

[121] https://edition.cnn.com/2026/04/08/china/china-supercomputer-hackers-hnk-intl
[122] https://netaskari.substack.com/p/chinas-massive-data-leak-of-military
[123] https://securelist.com/fakewallet-cryptostealer-ios-app-store/119474/
[124] https://slowmist.medium.com/security-alert-supply-chain-attack-on-apifox-desktop-client-via-compromised-official-cdn-script-bc3870992564

"Contagious Interview" becomes a dominant intrusion lane for developer compromise

The North Korean operations referred as "contagious interview" is a cluster of threats that use job-themed lures to blend into routine developer workflows and increase the likelihood of code execution[125]. It has grown into a prominent threat for developers worldwide and several instances of such operations were documented.

Threat actors use platforms like LinkedIn, Facebook, Telegram, and Reddit to approach victims with tailored job offers or partnership proposals[126] involving elaborate narratives centered around blockchain and cryptocurrency exchanges to lure high-value targets[127].

The infection vectors are designed to exploit the trust inherent in technical hiring workflows[128] . Attackers utilize fake corporate identities to invite victims to fraudulent meetings on platforms impersonating Zoom, Google Meet, or Microsoft Teams, where they may be prompted to install "missing" SDKs or execute technical assessment materials[129]. Other methods include directing victims to malicious GitHub repositories or using "ClickFix-style" prompts to deliver payloads. Some campaigns have even compromised public package registries, such as the bigmathutils npm package, to distribute malicious code[130].

The deployed malware is typically cross-platform, targeting Windows, macOS, and Linux. These payloads range from custom framework and updated variants of RAT-like malware to JavaScript that establishes command-and-control (C2) communication. The primary goals of these operations are financial theft, system reconnaissance, and the capture of voice and video recordings to enhance future social engineering efforts.

Furthermore, some actors have evolved their tactics into self-propagating supply chain threats. Void Dokkaebi (overlapping with Famous Chollima) uses compromised developer repositories and malicious VS Code tasks to create a worm-like propagation chain, affecting over 750 repositories and organizations like

[125] https://www.microsoft.com/en-us/security/blog/2026/02/24/c2-developer-targeting-campaign/
[126] https://www.proofpoint.com/us/blog/threat-insight/dont-fear-repo-unkdeaddrop-phishing-campaign-targets-developers-steal
[127] https://www.validin.com/blog/i_cant_hear_you_unc1069/
[128] https://www.microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews/
[129] https://www.microsoft.com/en-us/security/blog/2026/02/24/c2-developer-targeting-campaign/
[130] https://www.reversinglabs.com/blog/fake-recruiter-campaign-crypto-devs

DataStax and Neutralinojs[131]. To evade traditional takedowns, these actors have begun using blockchain infrastructure, such as Tron and Binance Smart Chain, for payload staging.

Infostealers & supply-chain abuse as scalable access

Highly sophisticated supply-chain attacks have become a marker of North Korean threat actors, specifically targeting the trust and authority of open-source maintainers. A prominent example is the compromise of the axios library, where attackers hijacked a lead maintainer's npm account to distribute a multi-stage payload[132]. This attack was particularly dangerous because the malicious code was not inside axios itself but was injected via a new dependency, and the malware would replace itself with a clean version after execution to evade detection. This pattern of targeting high-impact Node.js maintainers through social engineering has become a "new normal" across the ecosystem.

Beyond account hijacking, actors are utilizing "factory-model" distribution across multiple ecosystems, including npm, PyPI, Go Modules, crates.io, and Packagist[133]. They often employ a two-layer distribution strategy: publishing benign wrapper packages that clone legitimate libraries (such as big.js) to pull in a hidden malicious dependency[134]. In these cases, the postinstall hook is frequently used to trigger loaders that execute the final payload. Other campaigns have seen the distribution of the PylangGhost RAT via npm packages published by throwaway accounts[135].

The technical delivery of these payloads has evolved to integrate deeper into the developer's local workflow. While previous campaigns relied on .vscode/tasks.json or package.json scripts, Lazarus has begun hiding stage-2 loaders within Git hooks[136]. This allows the malware to fire immediately when a victim clones a "coding assessment" repository, executing the payload before a commit object is even written.

The primary objective of these operations is the deployment of RAT-enabled infostealers[137], such as OtterCookie and PylangGhost, designed to exfiltrate credentials, browser data, password-manager contents, and cryptocurrency wallet

[131] https://www.trendmicro.com/en_us/research/26/d/void-dokkaebi-uses-fake-job-interview-lure-to-spread-malware-via-code-repositories.html
[132] https://therecord.media/google-links-axios-supply-chain-attack-north-korea
[133] https://socket.dev/blog/attackers-hunting-high-impact-nodejs-maintainers
[134] https://panther.com/blog/tracking-an-ottercookie-infostealer-campaign-across-npm
[135] https://kmsec.uk/blog/pylangghost-npm/
[136] https://opensourcemalware.com/blog/lazarus-group-uses-git-hooks-to-hide-malware
[137] https://www.ox.security/blog/north-korean-npm-infostealer-rat/

data[138]. Some variants, such as license-utils-kit, provide extensive post-compromise functionality, including remote shell execution, keylogging, and the installation of SSH public key backdoors on Linux systems. Some of these operations are directly linked to "Contagious Interview" campaigns[139].

"IT worker" infiltration: an enabling service for fraud and access

According to the United States' Office of Foreign Assets Control (OFAC)[140], DPRK-facilitated IT teams commonly rely on fraudulent documentation, stolen identities, and fabricated personas to conceal their true identities and gain employment with legitimate companies, including those in the United States and allied countries. The DPRK government reportedly appropriates most of the wages earned by these overseas IT workers, generating hundreds of millions of dollars to support the regime's WMD and ballistic missile programs, in violation of U.S. and United Nations sanctions. In certain instances, DPRK-affiliated workers have also covertly introduced malware into company networks to extract proprietary and sensitive information.

To perform these infiltration, DPRK IT-workers rely on fraudulent remote systems access facilitated by nationals of the targeted country[141], enabling them to pose as local residents and obtain work as remote worker inside companies. In some complex schemes, a Ukrainian national maintained a website selling or renting stolen identities to North Korean workers and paid U.S. nationals to receive and host computers to make it look like the North Koreans were working from American homes[142]. The use of stolen identities is sometimes linked to the abuse of legitimate LinkedIn profiles[143] to pass reference checks[144]. However, as noted in public research, most IT workers do not pass a second interview or a job offer, just like with many legitimate job candidates. As such, some north korean workers may have specialized in obtaining interviews and passing them to other workers, by using formulas that previously worked for crafting fake identities and online profile.

These operations were linked to crypto heists by a team of eleven countries, as both are designed to bring in funding for North Korea's regime, simplify weapons purchases and circumvent multiple UN security resolutions[145].

---

138 https://socket.dev/blog/contagious-interview-campaign-spreads-across-5-ecosystems
139 https://assets.recordedfuture.com/insikt-report-pdfs/2026/cta-nk-2026-0121.pdf
140 https://home.treasury.gov/news/press-releases/sb0416
141 https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker
142 https://therecord.media/north-korea-laptop-farm-ukraine
143 https://www.group-ib.com/blog/dprk-fake-remote-developers/
144 https://www.okta.com/blog/threat-intelligence/the-north-korean-on-your-payroll/
145 https://therecord.media/40-countries-impacted-nk-it-thefts-united-nations

Monetization: crypto thefts and rapid laundering

North Korea remained the number one threat to the cryptocurrency ecosystem, with record-breaking crypto thefts and rapid laundering using complicit banking infrastructure. Since the beginning of the year, $643 million's worth of cryptocurrency is estimated to have been stolen by North Korean attackers[146]. This represents around 2.5% of the countries estimated GDP only for the first half of 2026, which could make it closer to 5% if the trend continues into the full year, making it an important source of financing for the regime's activities[147].

Several high-profile crypto thefts occurred in H1 2026, with Lazarus stealing and laundering around 220 million in stolen funds from Kelp DAO[148] in just six weeks after the attack. The attackers mainly used Tornado Cash, which was sanctioned and then de-sanctioned by the OFAC[149], to launder their illicit proceedings[150]. Usually, this is one of the first steps of the laundering process, which will then make use of complicit banks, sometimes in China, to convert these cryptocurrencies in cash usable by North Korea's regime. These attacks usually target decentralised platforms and crypto infrastructure, as security is lesser in these ecosystems. The Drift crypto hack of $280 million is another example of such attacks[151]. The specific threat actor was not identified but they showed a high level of sophistication which probably involved weeks of preparation and staged execution[152].

Other DPRK actors were also linked to crypto thefts against a large volume of private users. For instance, Famous Chollima extracted close to $12 million from 26 584 wallets held on 2 726 systems[153], and Lazarus targeted web3 developers to steal cryptocurrencies and NFTs, with as much as $12M stolen in 3 months[154]. Additionally, the "Contagious Trader" campaign highlights the conjunction of developer compromise and cryptocurrency theft, as a North Korean threat actor performed a malware campaign on npm and GitHub projects related to cryptoccurency trading bots[155]. These highlights the different strategies of North Korean actors to steal cryptocurrency from unsuspecting users.

---

146 https://www.trmlabs.com/resources/blog/h1-2026-crypto-hacks-reach-record-high-as-losses-fall-below-usd-1-billion
147 https://eastasiaforum.org/2026/02/05/a-wealthier-north-korea-widens-kim-jong-uns-options/
148 https://x.com/LayerZero_Core/status/2046081551574983137
149 https://home.treasury.gov/news/press-releases/sb0057
150 https://cointelegraph.com/news/kelp-dao-recovery-hacker-launders-most-funds-293m-exploit
151 https://therecord.media/drift-crypto-confirms-280-million-stolen-north-korea
152 https://therecord.media/drift-crypto-confirms-280-million-stolen-north-korea
153 https://therecord.media/north-korean-hackers-siphon-12-million-from-crypto-users
154 https://expel.com/blog/inside-lazarus-how-north-korea-uses-ai-to-industrialize-attacks-on-developers/

155 https://kmsec.uk/blog/contagious-trader/

4.4.3. South-East Asia

In South-East Asia, the most prominent topic was related to the scam compounds fuelling online investment frauds targeting victims worldwide. This type of fraud is also known as "pig-butchering". With billions in revenue and a lot of attention from powers such as the United States and China, the issue has grown into a legal challenge for the countries involved, such as Cambodia, Thailand, Malaysia. Due to mounting pressure, scammers are now relocating to other countries (Indonesia, Timor Leste and even the Middle East). In the broader region, notable cybercrime activity was noted coming from Vietnam and the Philippines, and we can identify a trend towards professionalisation of activities and services provided.

Scam-center ecosystem: industrial scale, enforcement, and sanctions

One of the key cybercriminal topics emerging from Southeast Asia in recent years is "pig-butchering" scams. Fuelled by scam compounds (i.e. facilities housing thousands of workers, organised as a workplace) in Myanmar, Cambodia and to a lesser extent in Vietnam and Thailand, it has grown into a billion dollars industry, extorting money from victims worldwide. The UN, based on a report from Global Initiative, estimates that this industry resulted in annual global profits of $64 billion.

The growth of these scam compounds in the region can be traced to the onset of the Myanmar civil war in 2021. This type of infrastructure existed prior to the conflict, but due to the generated instability, they started to grow a lot, which enabled their operators to scale up in terms of revenue and worldwide impact. As for any profitable activity inside war zones, local armed groups, militias and border forces reportedly tolerated scam operations in exchange for revenue or local control.

On 24 February 2026, the FBI announced that the United States are "fully committed to leading the global fight" against transnational criminal networks that have set up scam compounds throughout Southeast Asia[156]. This is a significant development as until recently, this problem was addressed mainly by China and the region's countries, as well as various western-backed army groups in the Myanmar civil war. It could also be used by the United States as an excuse to gain more leverage in the region, as they are more inclined to use brute force against various criminal organisations for geopolitical gains (recently in Venezuela and Ecuador). As first evidence of this strategic positioning, Meta announced that they successfully cooperated with the FBI and the Thai police to disrupt online accounts

[156] https://therecord.media/us-committed-to-fighting-southeast-asia-scam-compounds

associated to these scam networks, which also led to the arrest of 21 individuals in Thailand[157].

During a Joint Economic Committee hearing on scam compounds on 25 March 2026[158], the United States accused China of profiting and exploiting the cyber scam crisis in Southeast Asia. According to the U.S Commissioner of the Committee, China only cracked down on scam compounds targeting Chinese citizens and, in some instances, released the jailed scam kingpins in exchange of promoting the Chinese Communist Party and its interests, including investing in the "Belt and Road Initiative".

The transnational nature of these operations is also evidenced as a South African fixer[159] was accused of washing money for scam operations into a Singapore-based business, with shares held by Thai politicians. This individual is on the run and subject to an Interpol red notice. Since then, the business was dismantled by Singapore authorities.

Regulatory/legal responses and public-policy tightening

Since the subject was pushed to the front of local and international headlines, pressure has mounted on the government implicated and it has attracted the attention of police forces of the region, with Malaysia and South Korea signing a cooperation agreement against transnational scams[160]. Chinese authorities have also stepped up with more border controls to enter Myanmar and legal actions against these scam bosses, while some participants in the Myanmar civil war have made crackdowns on these compounds (which for some may only be for show, while the operators relocate elsewhere).

Related to Cambodia, some politicians were sanctioned by the United States on claims of having links to these scam operations[161]. We can suspect that these sanctions were effective in motivating other politicians to better respond to this challenge, as the country has announced the creation of anti-scam agencies[162] and

[157] https://about.fb.com/news/2026/03/meta-global-law-enforcement-disrupt-major-southeast-asia-criminal-scam-networks/
[158] https://therecord.media/china-scam-compounds-southeast-asia
[159] https://www.lemonde.fr/international/article/2026/03/25/en-thailande-la-traque-du-grand-argentier-presume-de-la-cyberfraude_6674137_3210.html
[160] https://www.koreatimes.co.kr/foreignaffairs/20260204/police-authorities-of-korea-malaysia-agree-to-boost-cooperation-against-transnational-scams
[161] https://home.treasury.gov/news/press-releases/sb0469
[162] https://freshnews.com.kh/index.php/localnews/425630-2026-04-24-17-11-04

new laws to tighten the net on online scams[163]. The country's authorities have allegedly dismantled scam centers[164], deported foreign workers working in the centers to their origin countries[165] and extradited associates of criminal conglomerate to China[166].

Vietnam, which started to become plagued by relocation of scammers fleeing arrests and extraditions, made efforts to counter operations of these criminals. For instance, Vietnam police busted a group suspected of planning a large-scale online scam centre[167]. In response to the mounting pressure, scammers started relocating to other countries in the region such as Indonesia, Timor-Leste[168], Sri Lanka[169].

Enabling infrastructure: malware-as-a-service, "fraud ops" tooling, and ecosystem professionalization

Another subject of interest for the subregion in the surge of various infrastructure enabling services. In Indonesia, the W3LL phishing tool was taken down by the FBI[170]. This tool enabled attacker to create fake websites that looked like legitimate login portals for $500. It was mainly used to target Microsoft365 accounts in Western countries. Another service from Indonesia dubbed "GoldFactory" is composed of a shared infrastructure used to deploy multiple malware families such as Gigabud.RAT and MMRat[171]. It was leveraged in a fraud campaign involving fake application masquerading as Coretax, the official Indonesian tax payment platform.

In Cambodia, victims of labor-trafficking in scam compounds are forced to operate extensive fraud campaigns. These operations utilize a sophisticated Android banking trojan that grants attackers full control over infected devices, enabling real-time surveillance, biometric theft, and financial fraud. The operational structure is highly organized, featuring segmented command-and-control (C2) panels divided by target country, such as "Indonesia Group" and "Brazil Group", indicating a coordinated, global management approach[172].

---

163 https://mekongindependent.com/2026/04/cambodia-says-new-law-tightens-net-on-online-scams/
164 https://www.nationthailand.com/news/asean/40061975
165 https://freshnews.com.kh/index.php/localnews/426254-2026-04-30-15-30-10
166 https://www.occrp.org/en/news/cambodia-extradites-another-executive-from-alleged-criminal-conglomerate-to-china
167 https://www.businesstimes.com.sg/international/asean/vietnam-police-bust-group-planning-large-scale-online-scam-centre
168 https://www.theguardian.com/world/ng-interactive/2026/apr/06/prince-group-timor-leste-links-to-alleged-scam-empire
169 https://www.straitstimes.com/asia/south-asia/sri-lanka-arrests-37-chinese-at-suspected-scam-centre-police
170 https://therecord.media/phishing-takedown-indonesia-fbi
171 https://www.group-ib.com/blog/indonesia-tax-impersonation-goldfactory-malware/
172 https://www.infoblox.com/blog/threat-intelligence/scams-slaves-and-malware-as-a-service-tracking-a-trojan-to-cambodias-scam-centers/

A critical enabler of this ecosystem is Funnull Technology Inc., a Philippines-based company that functions as a "scam-specific cloud". Funnull (also tracked as Triad Nexus) provides "computer infrastructure for hundreds of thousands of websites involved in virtual currency investment scams" and "pig-butchering" frauds by purchasing IP addresses in bulk from major cloud providers and selling them to cybercriminals[173]. To maintain resilience and evade takedowns, Funnull employs domain generation algorithms (DGAs) and provides web design templates that allow scammers to impersonate trusted brands and rapidly rotate their infrastructure. The group has also been observed maliciously altering open-source code repositories to redirect legitimate website visitors to scam and gambling sites linked to Chinese money laundering operations.

Despite significant international efforts, including sanctions by the US Treasury's Office of Foreign Assets Control (OFAC) in 2025, these syndicates exhibit extreme resilience[174]. The operators behind Funnull have matured their operational security by using geographic fencing to blind investigators and laundering their infrastructure through account muling and rotating "clean" front companies[175]. These networks have industrialized brand theft on a global scale, creating "pixel-perfect" clones of luxury brands, as well as global banking and logistics portals to facilitate large-scale credential harvesting.

The financial impact of these operations is staggering, with Funnull alone reportedly causing over 300 million in daily losses, and individual victim losses averaging 150,000. The ecosystem's reach is truly global, targeting victims across four continents, including Southeast Asia, Europe, and Latin America. This model demonstrates a shift toward a professionalized, tiered supply chain where infrastructure providers like Funnull enable a vast array of "pig butchering" and PII theft operations, transforming human trafficking compounds into high-tech hubs for global financial crime.

Espionage / state-linked activity co-exists with cybercrime (phishing / RAT / infostealer)

Broader cyber activity in Southeast Asia is characterized by a mix of highly targeted state-aligned activity and opportunistic financially oriented attacks. Vietnam-aligned OceanLotus has recently shifted its operational focus toward

[173] https://home.treasury.gov/news/press-releases/sb0149
[174] https://blog.xlab.qianxin.com/exposing-funnull-how-ringh23-maccms-are-poisoning-the-web/
[175] https://www.silentpush.com/blog/triad-nexus-funnull-2026/

domestic espionage, utilizing the SPECTRALVIPER backdoor to target a Vietnamese infrastructure and transport construction company and conducting a selective supply-chain attack against stock investors via the FireAnt Metakit platform[176]. Similarly, the Khmer Shadow cluster has targeted Cambodian government entities in the defense and military intelligence sectors, using government-themed lures to deploy the NIGHTFORGE loader, which executes a Havoc Demon payload in memory[177].

Technical sophistication varies across these regional actors, ranging from advanced evasion to rapid, repetitive deployment. The NIGHTFORGE loader demonstrates a moderate level of sophistication by employing NTDLL unhooking and "Hell's Gate" syscall resolution to bypass user-mode monitoring, although the group's tendency to reuse identical payloads and infrastructure suggests a relatively low retooling tempo. In contrast, OceanLotus continues to exhibit a high level of craftiness in its tooling, maintaining a long-term presence through aggressive and selective targeting.

Parallel to these state-aligned efforts, there is a rise in opportunistic supply-chain attacks targeting global technology giants. An Indonesian actor operating under the alias "frank" launched a coordinated campaign involving 38 malicious npm packages targeting developers and CI/CD infrastructure impersonating Apple, Google/GCP, and Alibaba/Aliyun[178]. This actor primarily utilized dependency confusion, weaponizing -internal- package naming conventions to trick automated build pipelines into resolving malicious public packages instead of legitimate private ones.

The primary objective of these developer-centric attacks is the exfiltration of high-value credentials and access tokens from internal engineering ecosystems. By impersonating internal developer tooling, the actor "frank" sought to compromise the secrets of software engineers and DevOps infrastructure, using a specialized toolkit designed for stealth and exfiltration. Together, these activities illustrate a regional landscape where traditional state-sponsored espionage coexists with opportunistic attacks on everyday users.

4.4.4. East-Asia

[176] https://www.welivesecurity.com/en/eset-research/oceanlotus-external-espionage-domestic-targeting/
[177] https://www.acronis.com/en/tru/posts/behind-khmer-shadow-targeted-espionage-against-cambodian-government-entities/
[178] https://panther.com/blog/frankly-malicious-inside-a-38-package-npm-supply-chain-campaign-targeting-tech-giants

The main other region of interest for Asia is East-Asia, which, if we exclude China and North-Korea as we already covered them, is composed of Taiwan, South-Korea and Japan. These entities are important to mention as they are regular targets of the main cyber powers of the region due to their strategic partnerships with the United States, their technological developments and broader geopolitics. We can also note a tendency of enabling better cyberdefense and legal response to the challenges they face, which was an important topic for the first semester of 2026.

Taiwan: persistent pressure (attribution warnings, campaigns, disinformation)

As we have seen in the section about China, Taiwan is a prominent focus for the Communist Party. This directly translates into cyber operations aiming to spy on targets of interest, practice attacks on critical infrastructure, and sow dissent into pro-Taiwan communities. Taiwanese authorities and research from cybersecurity companies have reported on these operations.

Taiwan's government published a lengthy report in H1 2026, highlighting an increase in cyberattacks attributed to China against their critical infrastructures[179] for 2025. Technical documents leaked from an unsecured FTP server revealed the existence of Expedition Cloud, a cyber training platform developed by the Chinese company CyberPeace to simulate attacks on nearby critical infrastructure[180]. The platform replicates networks in the energy, transportation, and home automation sectors in the South China Sea and Indochina regions. This can indicate that espionage operations can be repurposed by exploiting network information obtained to train for future operations.

Further sophistication is seen in the activity of the UAT-10362 cluster, which targets Taiwanese NGOs and universities using a tiered toolkit[181]. This actor deploys LucidRook, a sophisticated stager that embeds a Lua interpreter and Rust-compiled libraries within a DLL to execute staged Lua bytecode payloads. To ensure precision, the associated dropper, LucidPawn, includes region-specific anti-analysis checks that restrict execution exclusively to Traditional Chinese language environments associated with Taiwan.

Another significant threat to Taiwan is ransomware. The CrazyHunter ransomware, a Go-developed fork of the Prince ransomware has specifically targeted the

[179] https://www.nsb.gov.tw/en/#/News%20and%20Releases/Press%20Releases%20and%20News%20Coverage/2026-01-04/Analysis%20on%20China%E2%80%99s%20Cyber%20Threats%20to%20Taiwan%E2%80%99s%20Critical%20Infrastructure%20in%202025
[180] https://therecord.media/leaked-china-documents-show-testing-cyber-neighbors
[181] https://blog.talosintelligence.com/new-lua-based-malware-lucidrook/

Taiwanese healthcare sector[182]. The attackers leverage the critical nature of hospital services to pressure victims, utilizing a dedicated data leak site to publicize the information of organizations that refuse to cooperate.

Additionally, the country regularly announces arrest of individuals on their soil[183], linked to various cyber operations from Chinese attackers or to international scam schemes[184].

Japan/South Korea: ransomware/leak reality + institutional posture shift

Japan and South Korea were mainly mentioned as targets of ransomware attacks and leak operations, while also preparing shifts in institutional posture to catch up on cyber defense and resilience against cyber threats. In fact, both countries are significantly behind other developed nations in terms of capabilities and legal framework, which made these shifts a necessity to be better prepared against the growing number and new methods of cyber threats.

Ransomware is a prominent threat affecting these countries, with authorities of both countries regularly publishing advisories warning of such attacks[185] and public institutions noting a surge of 40% year-over-year on the number of affected organisations. Surveys show that close to half of companies were affected by ransomware attacks, with 60% of companies paying ransoms not recovering their data[186].

In response, the countries have started increasing their legal and operational capabilities. South Korea's KISA (Korea Internet & Security Agency) launched the "Ransomware Full Lifecycle Response Task Force"[187] to respond more systematically to ransomware threat with plans to identify key tasks for each stage of the ransomware response and establish an integrated response system that organically links these tasks. The Japanese government allowed its Self-Defense Force to conduct "proactive cyber-defense" operations aimed at attacking and disabling "infrastructure used to run cyberattacks", as the Chief Cabinet announced that the country faces "the most complicated national security environment since World War II"[188]. The country's parliament also passed a bill to create the first post-

182 https://www.trellix.com/blogs/research/the-ghost-in-the-machine-crazyhunters-stealth-tactics/
183 https://www.dw.com/en/taiwan-indicts-62-linked-to-alleged-scam-center-in-cambodia/a-76207992
184 https://www.caixinglobal.com/2026-03-06/taiwan-indicts-dozens-linked-to-prince-group-cybercrime-empire-102419931.html
185 https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20260416133126296
186 https://databreaches.net/2026/04/29/over-200-japanese-firms-have-paid-ransomware-attackers-60-fail-to-recover-data/
187 https://www.kisa.or.kr/402/form?postSeq=2580&page=1
188 https://www.theregister.com/security/2026/03/18/japan-to-allow-proactive-cyber-defense-from-october-1st/5229816

war national intelligence agency[189], composed of a National Intelligence Council and a National Intelligence Bureau, unifying and coordinating the currently fragmented intelligence capabilities, in the face of "growing Chinese and Russian threats"[190].

4.4.5. Outlook

Asia is expected to remain one of the most dynamic theatres of state-sponsored cyber activity during the second half of 2026. Chinese cyber operations will likely continue prioritizing long-term strategic access to government, telecommunications, semiconductor, and defence-related sectors, while maintaining pressure around Taiwan and the South China Sea. North Korean actors are expected to sustain financially motivated operations supporting sanctions evasion, alongside intelligence collection and cryptocurrency theft. Across the region, growing technological competition, military modernization, and expanding AI capabilities are likely to further accelerate offensive innovation, making Asia a major driver of emerging cyber techniques and strategic cyber competition.

[189] https://www3.nhk.or.jp/nhkworld/en/news/20260527_12/
[190] https://theweek.com/defence/japan-to-create-first-post-war-intelligence-agency

5. Conclusion

The first half of 2026 confirms that cyber operations have become an integral component of geopolitical competition rather than an isolated technical domain. Across every region covered in this assessment, cyber capabilities were employed to support strategic national objectives, ranging from intelligence collection and influence operations to military support, economic coercion, and political destabilization. While the nature of the threats varied between Europe, North America, the Middle East and Asia, several common trends emerged, illustrating a broader transformation of the global cyber landscape.

One of the most significant developments observed during the reporting period is the continued shift from disruptive, high-visibility operations toward long-term, intelligence-driven access. Rather than immediately deploying ransomware or destructive malware, many state-sponsored actors increasingly prioritized the establishment of persistent footholds within government networks, cloud infrastructures, telecommunications providers, edge devices, and critical infrastructure. These operations seek to provide strategic options that can be activated whenever political or military circumstances require, reinforcing the concept of cyber capabilities as pre-positioned instruments of national power rather than merely offensive tools.

The reporting period also highlighted the growing convergence between cyber operations and broader hybrid strategies. Cyber espionage, information operations, hacktivism, economic pressure, diplomatic disputes, and conventional military activities increasingly reinforced one another instead of occurring independently. Russian operations supporting military objectives in Ukraine, influence campaigns targeting European democratic processes, Middle Eastern cyber activities accompanying regional tensions, and Chinese intelligence collection supporting long-term strategic competition all illustrate that cyber operations are becoming deeply embedded within wider geopolitical campaigns.

Artificial Intelligence has similarly evolved from an emerging capability into an operational force multiplier. Multiple threat actors demonstrated the ability to integrate Generative AI and Large Language Models throughout the attack lifecycle, enabling faster malware development, improved phishing campaigns, automated social engineering content, and increasingly adaptive offensive tooling. While AI has not fundamentally changed attackers' objectives, it has significantly reduced the cost, time, and expertise required to execute sophisticated operations. As these capabilities continue to mature, defenders should expect attack campaigns to become more personalized, scalable, and difficult to distinguish from legitimate communications.

Another recurring observation throughout H1 2026 is the progressive erosion of traditional distinctions between state-sponsored groups, cybercriminal organizations, exploit brokers, initial access brokers, and ideologically motivated hacktivists. Technical capabilities, infrastructure, malware families, and operational services increasingly circulate between these ecosystems, creating a highly interconnected threat environment. The proliferation of advanced capabilities illustrates that strategic offensive tooling can rapidly extend beyond its original developers, making attribution more complex while increasing the overall threat surface.

Critical infrastructure remained among the highest-priority targets throughout the reporting period. However, threat actors increasingly shifted their attention away from centralized systems toward distributed and less protected assets, including routers, VPN gateways, telecommunications equipment, renewable energy facilities, industrial remote access solutions, and edge devices. These systems often provide attractive opportunities for long-term persistence while benefiting from weaker monitoring and slower patch management than traditional enterprise environments. This evolution reinforces the importance of treating edge infrastructure as a strategic component of national cyber resilience.

Information manipulation also continued its transformation into a mature operational discipline. Rather than relying solely on social media amplification, recent influence campaigns combined fabricated media ecosystems, coordinated online personas, AI-generated content, impersonation, cross-platform dissemination, and selective physical-world activities. These operations demonstrated an increasing ability to exploit societal polarization while remaining below the threshold of large-scale public awareness, complicating both attribution and defensive response.

Recommendations

Based on the observations presented throughout this report, several strategic priorities should be considered by organizations operating within or alongside the regions assessed.

Organizations should first strengthen the visibility and protection of Internet-facing infrastructure, particularly VPN gateways, firewalls, routers, cloud authentication services, and remote administration platforms. As multiple campaigns demonstrated, these assets increasingly represent preferred entry points for long-term compromise.

Patch management strategies should continue evolving toward risk-based prioritization. Rather than focusing solely on vulnerability volume, organizations should prioritize vulnerabilities actively exploited by state-sponsored actors, particularly those affecting edge devices, identity infrastructure, remote access technologies, and widely deployed enterprise platforms.

Identity protection should remain a strategic priority. The increasing use of adversary-in-the-middle techniques, OAuth token theft, cloud session hijacking, and credential interception demonstrates that traditional password-based security alone is no longer sufficient. Strong phishing-resistant multi-factor authentication, privileged identity monitoring, and continuous session validation should become baseline defensive capabilities.

Given the growing operational role of Artificial Intelligence, organizations should anticipate increasingly convincing phishing campaigns, fraudulent identities, malicious documentation, and AI-assisted malware development. Security awareness programmes, detection engineering, and incident response procedures should therefore be updated to explicitly account for AI-generated content.

Threat intelligence capabilities should progressively integrate geopolitical monitoring alongside technical indicators. Political crises, sanctions, elections, armed conflicts, diplomatic tensions, and regulatory developments increasingly provide early indicators of future cyber activity. Organizations capable of correlating geopolitical developments with technical threat intelligence will be better positioned to anticipate emerging risks.

Particular attention should also be dedicated to critical infrastructure dependencies and supply chain resilience. Even organizations operating outside traditionally sensitive sectors may become indirect targets through trusted suppliers, managed service providers, telecommunications operators, software vendors, or cloud platforms. Third-party risk management should therefore extend beyond compliance assessments to include continuous monitoring of evolving threat activity affecting strategic suppliers.

Organizations should further develop detection capabilities focusing on persistence rather than solely on malware execution. Modern state-sponsored campaigns increasingly emphasize credential theft, cloud abuse, living-off-the-land techniques, legitimate administration tools, and stealthy long-term access. Behavioral detection, identity analytics, endpoint telemetry, and cloud monitoring should therefore complement traditional signature-based security controls.

Finally, executive leadership should recognize that cyber resilience has become an integral component of organizational resilience. Incident response planning should

increasingly consider hybrid scenarios combining cyber incidents with disinformation campaigns, physical disruptions, supply chain degradation, regulatory pressure, or geopolitical crises. Exercising these multidimensional scenarios will better prepare organizations for the evolving threat environment described throughout this assessment.

Ultimately, the trends observed during the first half of 2026 suggest that the global cyber landscape will continue evolving toward greater integration between state interests, technological innovation, and hybrid conflict. Organizations capable of combining robust technical security, strategic intelligence, and adaptive governance will be significantly better positioned to anticipate and withstand the increasingly complex cyber challenges expected during the remainder of 2026 and beyond.

© Intrinsec