

A Comparative Study of Russian Offensive Cyber Capabilities from 2022 to 2025

A COMPARATIVE STUDY OF RUSSIAN OFFENSIVE CYBER CAPABILITIES FROM 2022 TO 2025

NATIONAL CYBER
SECURITY CENTRE

Table of content

1. PREFACE 4

2. LIST OF ABBREVIATIONS 5

3. INTRODUCTION 6

3.1. Purpose and Scope of the Study 6

3.2. Approach and Methodology 6

3.3. Proposed Structure of the Study 6

3.4. Justification of Selecting the 2022–2025 7

4. EXECUTIVE SUMMARY 8

5. THE 2022 BASELINE: STATE OF OFFENSIVE CYBER OPERATIONS 9

5.1. Key Threat Actors: Overview of Leading Offensive Actors 9

5.2. Tactics and Techniques: Common Methods Used Reconnaissance & Target Profiling 12

5.3. Strategic Use Cases: Integration into Hybrid Warfare 17

5.4. Infrastructure and Tooling 19

6. THE 2025 LANDSCAPE: ELEVATED OFFENSIVE CAPABILITIES 20

6.1. Emerging Threat Actors and Shifts: New Players, Changing Priorities, State-Proxy Relationships 20

6.2. Advanced Techniques: AI-Driven Attacks, Polymorphic Malware, Multi-Vector Campaigns 21

6.3. Targeting Trends: Broader Attack Surfaces – OT, AI Aystems, IoT, Critical Civic Tech 24

6.4. Lessons from High-Profile Campaigns: Case Studies Ranging 2023–2025 27

7. COMPARATIVE ANALYSIS: 2022 VS. 2025 30

7.1. Tactical Evolution 30

7.2. Operational Changes 34

7.3. Strategic Objectives 38

7.4. Technological Leverage 39

8. MITIGATION RECOMMENDATIONS 41

9. CONCLUSIONS 43

9.1. Summary of Findings 43

9.2. Way forward 43

10. LIST OF REFERENCES, ANNEXES 45

1. Preface

The Russian Federation continues to be the most active state sponsor of hostile cyber operations in Europe. Since the beginning of its full-scale invasion of Ukraine in 2022, Russia has employed cyberattacks as a strategic instrument of warfare – disrupting civilian infrastructure, targeting military systems, and conducting information operations to undermine political stability. Ranging from destructive malware and credential theft to satellite sabotage and psychological campaigns, the Russian cyber activity has become a central component of the country's hybrid warfare doctrine. These operations have not only persisted throughout the war but have expanded beyond Ukraine, targeting governments and institutions across NATO, the European Union, and other states that have expressed support for Kyiv.

The NCSC Regional Cyber Defence Centre (RCDC), in collaboration with Lithuanian institutions and rotating Ukrainian experts, has developed a Study on the Russian offensive cyber capabilities (2022–2025). The purpose of this report is to document, analyze, and compare the evolution of the Russian state-linked and proxy cyber operations across the recent three-year period. By means of research into real-world incidents, technical data, and proposed strategic assessments, the Study explores the tools, tactics, and operational shifts employed by the advanced persistent threat (APT) groups, such as APT28, APT29, Sandworm, Turla, and Gamaredon, as well as emerging actors, like UAC-0184. It further examines the growing role of the pro-Russian hacktivist groups, such as KillNet and NoName057(16), which have launched DDoS and defacement campaigns in retaliation for NATO's and EU member states' political decisions.

The primary objective of the report is to outline the evolution of Russia's offensive cyber strategy over time, from short-term disruption to long-term persistence and influence, and to provide an informed basis for the understanding of current and future cyber threats. The report includes a detailed analysis of the Russian capabilities in credential theft, lateral movement, OT targeting, cloud infrastructure abuse, and early-stage adoption of artificial intelligence for espionage and disinformation. The Study also compares cyber activity displayed at the onset of the invasion to present day, emphasizing both the changes and what remains consistent. The findings aim to assist the cyber defenders, policy experts, and civil institutions in building resilience against a threat landscape that continues to grow in both scope and sophistication.

2. List of Abbreviations

Term/Abbreviation	Meaning / Explanation
SMO	Special Military Operation
TTP	Tactics, Techniques and Procedures
SVR	The Foreign Intelligence Service of the Russian Federation
GU/GRU	The Main Directorate of the General Staff of the Armed Forces of the Russian Federation
DDoS	Distributed Denial of Service
LLM	Large Language Model
FSB	Federal Security Service of the Russian Federation
SBU	Security Service of Ukraine
C2	Command and Control
APT	Advanced Persistent Threat
RAT	Remote Access Tools
CSP	Cloud Solution Provider
MFA	Multi-Factor Authentication
AI	Artificial Intelligence
API	Application Programming Interface
ICS	Industrial Control Systems
PSYOPS	Information-Psychological Operations
OT	Operational Technology
VPN	Virtual Private Network
IoT	Internet of Things
IoC	Indicator of Compromise
LOLBins	Living-off-the-Land Binaries
EDR	Endpoint Detection and Response
BYOVD	Bring Your Own Vulnerable Driver
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
RDP	Remote Desktop Protocol
PsExec	Sysinternals Remote Execution Utility
DNS	Domain Name System
.HTA	HTML Application file
.DLL	Dynamic-link library file (extension form)
.PNG	Image file (used for steganography)
.ISO	Disk image file
.LNK	Windows shortcut file

3. Introduction

3.1. Purpose and Scope of the Study

Established as a joint initiative of Lithuania and the United States, the NCSC Regional Cyber Defence Center (RCDC) aims to fill the practical cooperation niche in the field of cyber defence and to strengthen the capacity of both Lithuania and the regional partners to ensure the cyber security of their states. The RCDC is a regional platform for practical cooperation on providing assistance in the efforts to protect critical infrastructure from cyberattacks. RCDC activities focus on strengthening resilience and cyber defence capacity in critical public service providers.

The Study analyzes how the character of the Russian offensive cyber operations has evolved since the start of the full-scale invasion of Ukraine in 2022. Initially used to support rapid military gains through sabotage, wipers and psychological operations, the Russian tactics have shifted toward long-term persistence, geopolitical pressure, and broader targeting of Ukraine's allies. While Russia's strategic goal to weaken Ukraine and deter foreign support has remained consistent, its methods have adapted to incorporate stealthier infrastructure, hacktivist proxies, and emerging technologies, like AI. The report examines the changes witnessed across state-linked and proxy actors, mapping their tactics, infrastructure, and strategic objectives between 2022 and 2025. The objective of the Study is to keep the policymakers, defenders, and institutions informed about the evolving threat landscape and Russia's potential future directions in cyber conflict.

3.2. Approach and Methodology

To achieve the Project objective, the Study is developed through the following sequence of parts:

- Discussion on the Study goals and objectives;
- Collection of the input and information provided by the RCDC members and like-minded partners;
- Collection of the information from publicly available sources;
- Collaborative processing, systematization, and evaluation of the collected information with the rotating RCDC personnel.

The listed research activities come together to form the Study offering a structured analysis of Russia's most active cyber actors, their tactics, tools, and strategic evolution between 2022 and 2025. Drawing from both classified partner insights and open-source intelligence, the report provides a comprehensive overview demonstrating how the Russian offensive cyber capabilities have developed during the wartime. It further outlines key patterns, operational shifts and emerging technologies to advance practical insight and improve detection, response, and resilience-building within organizations and national cyber defence structures.

3.3. Proposed Structure of the Study

The report is proposed divided in the following separate parts:

- Chapter 4: the Executive Summary which outlines key findings and strategic insights of the Study;
- Chapter 5: a detailed breakdown of the Russian cyber threat actors, their known capabilities, and evolution during the wartime;
- Chapter 6: a comprehensive overview of the most prominent cyber operations between 2022 and 2025, including destructive attacks, infrastructure sabotage, and psychological campaigns;
- Chapter 7: a comparative analysis of the Russian offensive tactics, strategic objectives, and technological trends across the selected timeframe;
- Chapter 8: practical mitigation recommendations for national defenders, institutions, and partner organizations;
- Chapter 9: conclusions and a summary of key takeaways of the Study.

3.4. Justification of Selecting the 2022–2025

The Study focuses on the period 2022-2025 marked by rapid escalation, adaptation, and strategic transformation in the Russian offensive cyber operations. While the Russians have been active in cyber for over a decade, it has been the launch of the full-scale invasion of Ukraine in February 2022 that triggered the dramatic intensification in state-linked and proxy cyber campaigns. The period exemplifies the first sustained conflict where cyber operations were fully integrated in support of kinetic military objectives, including the use of wipers, infrastructure sabotage, and psychological attacks coordinated with physical strikes. Tracing the evolution through 2025 captures a critical window in which the Russian actors, facing hardened defenses and strategic resistance, shifted from short-term disruption goals to long-term persistence, targeting both Ukraine and its international allies. It also reflects a broader transition seen in tactics, with more use of stealth, AI experimentation, and multi-vector hybrid warfare. The Study examines the set period aiming to provide a clear view of how the Russian cyber capabilities have matured in response to wartime challenges, and what future threat trajectories may look like.

4. Executive Summary

Between 2022 and 2025, the Russian offensive cyber operations have evolved from short, destructive campaigns into long-term, hybrid warfare tools embedded deeply in military strategy. Cyberattacks were no longer isolated incidents but rather operated in lockstep with kinetic strikes, psychological operations, and geopolitical messaging. The invasion of Ukraine served as a testing ground for this integrated model, with the early campaigns focused on breaking the Ukrainian resistance through wipers, sabotage, and defacements timed with missile strikes. As Ukraine's defenses hardened, the Russian strategy shifted toward persistence – focusing on espionage, critical infrastructure access, and pressuring Ukraine's supporters through coordinated hacktivist campaigns and retaliatory intrusions.

This Study finds that Russian state-linked groups, such as APT28, APT29, Sandworm, Turla, and Gamaredon, were quickly adapting and adopting stealthier techniques, cloud-focused espionage, and living-off-the-land methods to escape detection. New and emergent actors, including UAC-0184 and UAC-0050, broadened Russia's cyber reach by employing phishing, commodity malware, and multi-stage payloads to maintain access to Ukrainian and NATO-aligned networks. Pro-Russian hacktivist groups, like KillNet and NoName057(16), grew into an auxiliary force coordinating DDoS attacks and defacements against the governments which expressed support for Ukraine, such as Lithuania, Canada, and Japan.

By 2025, Russian operators had begun to experiment with artificial intelligence–using generative models for malware crafting, phishing, and propaganda creation. Though early in development, these tools represent a turning point suggesting faster, more adaptive future cyber campaigns that will be increasingly difficult to attribute. Likewise, targeting patterns have shifted toward operational technology (OT), critical civic infrastructure, IoT, and cloud services, highlighting a broadened digital battlespace and a sustained focus on undermining both national resilience and the international support for Ukraine.

Russia's offensive cyber model is now defined by distributed, persistent, and politically reactive operations combining traditional tradecraft with emerging technologies and proxy warfare into a multi-layered threat ecosystem. As the Study demonstrates, understanding and countering such operations requires not just technical preparedness but also awarness of how cyber tools are used to shape battlefield dynamics, strategic influence, and global political outcomes.

5. The 2022 Baseline: State of Offensive Cyber Operations

5.1. Key Threat Actors: Overview of Leading Offensive Actors

In 2022, Russia explicitly integrated cyber offensive capabilities into its broader military strategy, marking a clear shift from isolated espionage and sabotage to coordinated operations conducted in direct support of kinetic campaigns. Cyberattacks were used to disrupt opponent communications, gather battlefield intelligence, and target critical infrastructure in lockstep with military action – signaling the full adoption of cyber tools as instruments of warfare (see Reference 4). Russian threat actors operated as tiered, state-directed assets under the SVR, FSB, and GRU, each responsible for specialized tasks that collectively forming a unified cyber doctrine.[1] The emerged structure enabled rapid, targeted action across multiple domains, with some groups focusing on persistent access and intelligence collection, while others executed destructive, time-sensitive attacks to align with military movements.

The year 2022 marked a turning point in the Russian cyber operations with major state-linked threat actors rapidly intensifying their activity in support of military objectives during the full-scale invasion of Ukraine. Gamaredon (FSB Centre 18) was engaged in high-volume phishing campaigns against the Ukrainian Government and military entities, relying on simple delivery methods but evolving toward a more resilient infrastructure, including Telegram-based command-and-control and early uses of serverless platforms, to sustain access and evade detection. [2] [3] The mentioned operations prioritized persistence and quick redeployment following remediation.

[1] https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-2024/Russia-Ukraine-Conflict-Laboratory/

[2] https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations

[3] https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html

2022 Russian Cyber Operations Timeline

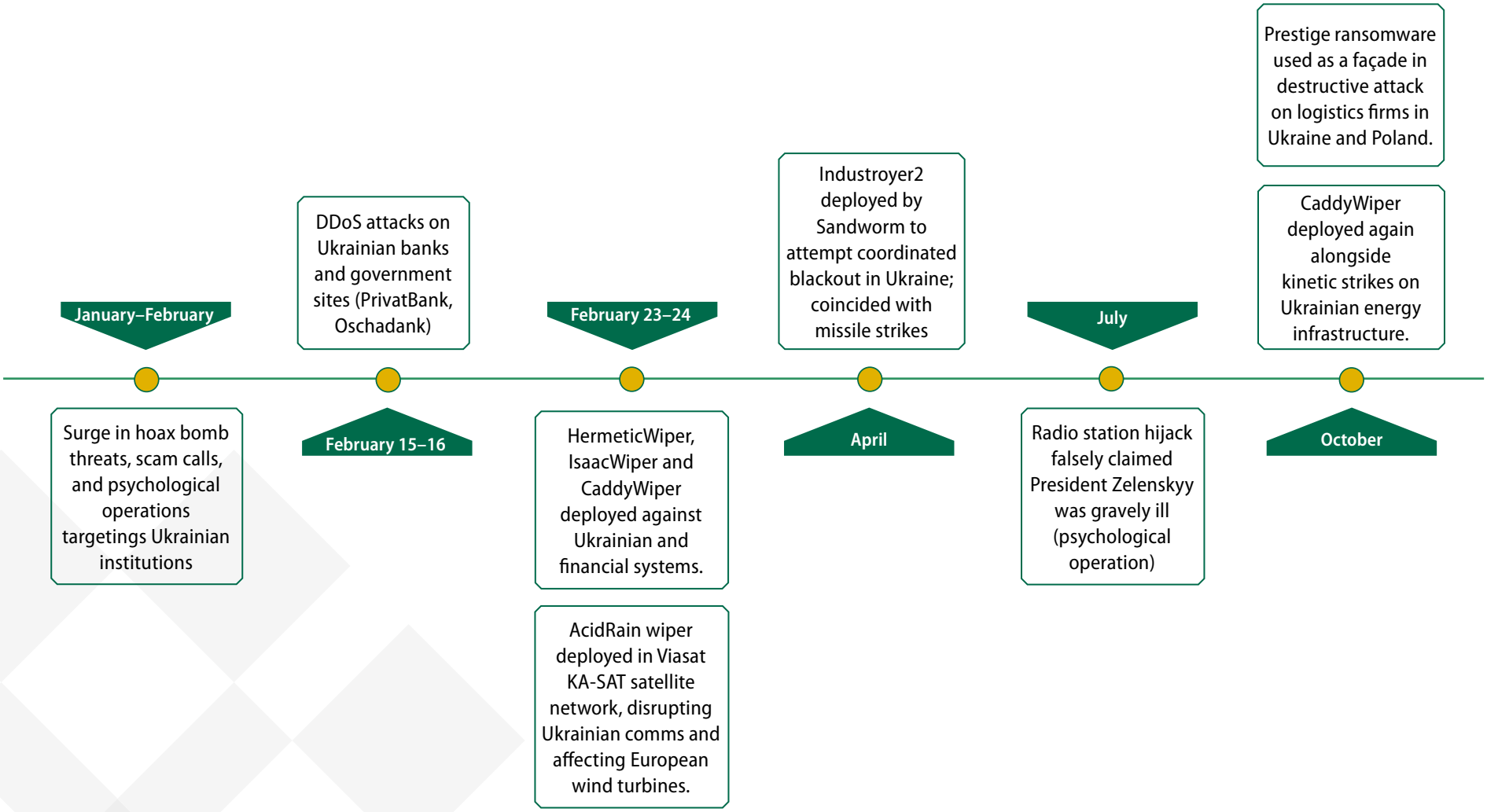


Figure 1. 2022 Russian Cyber Operations Timeline

Turla (FSB Centre 16) maintained its long-running espionage posture focusing on NATO-aligned diplomatic and defense targets. Its operations in 2022 featured stealthy malware like Kazuar and ComRAT, often deployed via hijacked third-party infrastructure.[4] APT29 (SVR) concentrated on compromising cloud services and identity platforms, employing sophisticated techniques to infiltrate diplomatic and political institutions through Azure Active Directory and OAuth token abuse. Meanwhile, APT28 and Sandworm (GRU) demonstrated a more aggressive profile.[5] [6] APT28 conducted credential theft and malware deployment using techniques such as LNK file abuse, while Sandworm launched destructive attacks timed with military actions – most notably, the Industroyer2 malware deployed in April 2022 to target Ukraine's power grid during an active missile campaign.[7] [8]

Groups such as Evil Corp, FIN7, and NoName057(16) were providing flexible, deniable assets for cyber operations. While traditionally motivated financially, these entities increasingly operationally aligned with state interests targeting critical infrastructure and commercial sectors with DDoS, ransomware, and disinformation campaigns.[9] [10]

Such groups as UAC-0050 and UAC-0184 emerged notably post-2022, demonstrating increasing sophistication and strategic alignment with Russia's intelligence and military apparatus. Their operations often bridged the gap between state-sponsored espionage and cybercriminal activity utilizing advanced Remote Access Trojans (RATs), phishing techniques, and social engineering for espionage and disruptive actions.[11] [12]

Strategic Coordination and Purpose

Russia's cyber apparatus operated with unprecedented coordination and direct alignment with military objectives in 2022. Cyber operations were not only complementary but also instrumental to tactical battlefield goals, enabling reconnaissance, communications disruption, psychological pressure, and strategic information control. The tiered structure of state-linked groups allowed for operational specialization: APT29 and Turla carried out strategic espionage, APT28 and Sandworm supported field operations with disruption and sabotage, while affiliated criminal or hacktivist proxies executed deniable campaigns that extended Russia's reach across civilian and soft infrastructure.[13] [14]

This tightly integrated approach marked the full maturation of cyber operations as a formal instrument of Russian statecraft. Threat actors functioned as embedded assets within broader campaigns, executing missions that influenced both the kinetic and informational dimensions of the conflict. The infrastructure, tactics, and operational tempo established in 2022 laid a foundational baseline for measuring the evolution of Russian cyber capability in subsequent years – demonstrating not only intent but also institutionalization of the offensive cyber power as part of Russia's modern warfare doctrine.

[4] https://threatpost.com/turla-apt-revamps-comrat/156051/

[5] https://cloud.google.com/blog/topics/threat-intelligence/apt29-continues-targeting-microsoft

[6] https://www.microsoft.com/en-us/security/blog/2022/09/22/malicious-oauth-applications-used-to-compromise-email-servers-and-spread-spam/

[7] https://www.cyware.com/resources/threat-briefings/research-and-analysis/inside-fancy-bears-arsenal-an-update-on-the-cyber-tactics-of-apt28-5186

[8] https://threatpost.com/turla-apt-revamps-comrat/156051/

[9] https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare/

[10] https://www.radware.com/cyberpedia/ddos-attacks/noname057%2816%29/

[11] https://socprime.com/blog/uac-0184-attack-detection-targeted-phishing-attacks-against-the-armed-forces-of-ukraine-using-remcos-rat-and-reverse-ssh/

[12] https://www.intrinsec.com/from-espionage-to-psyops-tracking-operations-and-bulletproof-providers-of-uac/

[13] https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing

[14] https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/

5.2. Tactics and Techniques: Common Methods Used Reconnaissance & Target Profiling

Russian cyber operators prioritized early gathering of credentials in their campaigns to enable stealthy, deep network access. Beyond using on-device dumping tools, they deployed info-stealer malware via spear-phishing in order to harvest browser passwords, login tokens, and keystrokes. In 2022, APT28 notably coupled backdoors with credential grabbers to siphon login data while attackers also leveraged large credential dumps from previous breaches as dictionaries for brute-force and stuffing attacks.[15] CERT-UA observed that many intrusions were enabled by valid credentials – either stolen or reused – rather than exploiting software vulnerabilities, underscoring how war-driven reliance on personal devices increased their effectiveness (see reference 3).

Post-compromise, the threat actors frequently abused built-in Windows tools – such as nltest, net user, and dsquery, to enumerate Active Directory users, groups, and machines – while leveraging ipconfig, arp – a, and route print for internal network mapping. They also scanned directories on critical servers (dir, type) to locate VPN, password, and configuration files. These behaviors are well-documented in MITRE ATT&CK, JPCERT's Windows Commands Abused guide, and Elastic's detection rules as standard steps in APT reconnaissance. In wartime contexts, this extended to malware targeting battlefield apps, like ArmySOS, to capture map data – the information reportedly used to geolocate Ukrainian artillery, demonstrating direct cyber support for kinetic strikes.[16]

Capturing email and messaging data was the key focus of Russian cyber groups. APT29 and Turla breached Exchange servers and mailboxes utilizing forwarding rules, exports, and the Exchange Web Services API to collect communications of high-value individuals.[17] With stolen Microsoft 365 or Google credentials, they searched cloud storage and mailboxes for wartime keywords, like "troop" or "NATO."[18] [19] This methodical targeting of official correspondence provided rich intelligence aligned with strategic objectives.

GRU units, like Sandworm (APT44), executed multi-vector cyber campaigns that tightly integrated espionage, disruption, and information warfare. The Mandiant Report 2023 outlined their five-phase model including steps to: gain access (e.g., via routers), conduct reconnaissance, steal data, deploy wipers, and launch coordinated propaganda.[20] This refined strategy, seen in the April 2022 Industroyer2 attack, often supported Russia's military goals combining grid sabotage with DDoS and phishing to sow confusion. These hybrid operations echo past efforts, like NotPetya, but are now more targeted and synchronized with battlefield or political objectives, and drawing strong international condemnation for striking civilian infrastructure.

Initial Access

Since 2022, the Russian state-aligned threat actors have relied heavily on spear-phishing, exploitation of public-facing systems, and credential theft to gain initial access. Gamaredon (FSB) repeatedly targeted the Ukrainian Government's networks using war-themed phishing emails to deliver HTA payloads that launched PowerShell backdoors.[21] Some lures, for example, "Provision of Military Assistance to Ukraine", included .LNK shortcut files to execute malware. APT28 (Fancy Bear, GRU) also executed phishing campaigns against Ukrainian and Eastern European officials stealing credentials or deploying malware. By late 2022, CERT-UA

[15] https://attack.mitre.org/groups/G0007/

[16] www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

[17] https://attack.mitre.org/groups/G0016/

[18] https://fieldeffect.com/blog/russia-linked-apt29-increasingly-targeting-cloud-services

[19] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

[20] https://www.mandiant.com/resources/reports/m-trends-2023-special-report?auHash=iTAkoIVQOJBJJ8XvjFW34KB6WJNeNAZ1HV2I3AEXdE&ref=guptadeepak.com

[21] https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf

had monitored APT28 leveraging info-stealers and pre-compromised credentials to infiltrate Ukrainian military chats on platforms like Telegram – highlighting a shift toward credential-based access that bypasses application-layer security.

In parallel, Russian units exploited unpatched, internet-facing infrastructure. Sandworm (GRU Unit 74455) continued targeting VPNs, routers, and web servers, often deploying web shells or implants through known vulnerabilities.[22] For instance, the February 24 Viasat incident was a prominent case where a misconfigured VPN appliance was exploited to send destructive commands to thousands of modems. APT28 also adopted zero-day exploits, such as CVE-2023-23397 in Microsoft Outlook, to steal authentication hashes from European targets, underscoring a growing reliance on advanced technical intrusions.[23]

While there is no proof in the public that the attackers definitively used credentials captured during battlefield interrogations, multiple open-source analyses confirm that Russian-linked actors consistently relied on valid stolen credentials – obtained via malware and compromised devices – to gain covert access to VPNs, email accounts, and internal networks, enabling them to operate under the guise of legitimate users. This integration of traditional intelligence collection with cyber intrusions demonstrates an evolving strategy in which compromised physical assets directly support digital operations.

Execution

After having gained access, the Russian threat actors typically deployed tailored malware to support espionage or disruptive objectives. Gamaredon relied on lightweight PowerShell backdoors, such as GammaSteel, to execute commands and stage additional payloads, while Turla and APT28 used custom remote access tools and memory-resident loaders to avoid leaving artifacts on disk.[24] Across multiple campaigns, Cobalt Strike was adapted for process injection and lateral movement, with operators modifying beacons to evade detection.[25] These efforts were supported by extensive use of Living-off-the-Land Binaries (LOLBins), leveraging PowerShell, Windows Script Host, mshta, and scheduled tasks to execute code natively and stealthily. In one notable case, Sandworm's October 2022 attack on a Ukrainian energy facility utilized the legitimate ICS application MicroSCADA to issue rogue operational commands, thus showcasing advanced OT-level abuse of trusted software.

Credential theft was central to the discussed execution chains as well. Russian actors routinely dumped credentials and access tokens from memory using tools like Mimikatz, thus enabling privilege escalation and the ability to execute malware as SYSTEM.[26] Some groups exploited known vulnerabilities, while others employed Bring Your Own Vulnerable Driver (BYOVD) techniques loading exploitable drivers to disable endpoint protections and deploy kernel-level payloads.[27] This allowed deeper access while avoiding modern detection mechanisms. APT29 and others often combined credential dumping with stealth escalation methods to maximize persistence and control.

In parallel, Russian APTs frequently incorporated open-source and commodity tools to accelerate operations and obscure attribution. Frameworks like Metasploit and Masscan were used to automate network discovery and exploit delivery. In many cases, groups deployed off-the-shelf backdoors or fileless loaders, like Sliver, or modified public scripts to establish persistence and execute follow-on payloads.[28] This hybrid approach, blending custom implants with widely available toolkits, allowed Russian units to operate at scale and speed, particularly under the rapid tempo of wartime campaigns.

[22] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
[23] https://thehackernews.com/2024/05/microsoft-outlook-flaw-exploited-by.html
[24] https://thehackernews.com/2025/04/gamaredon-uses-infected-removable.html
[25] https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
[26] https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping
[27] https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping
[28] https://blog.bushidotoken.net/2024/09/the-russian-apt-tool-matrix.html

Persistence

Russian threat actors, particularly Gamaredon, elaborated on long-term persistence by deploying multiple redundant backdoors and implants across compromised networks. Once inside, attackers saturated endpoints with malicious files – often leaving behind dozens of scheduled tasks, registry-run keys, and web shells. CERT-UA reported that a single host infected by Gamaredon could contain over 80 unique malware artifacts within a week, including various downloader stages and automated exfiltration scripts.[29] To extend control, the group regularly installed legitimate remote administration tools, like AnyDesk, enabling stealthy, interactive access under the guise of trusted software.

Beyond the traditional endpoints, groups like Sandworm extended their persistence effort into network infrastructure. As the case of the Cyclops Blink botnet discovered in 2022 demonstrates, infected WatchGuard firewalls and routers at firmware level, replacing the older VPNFilter botnet. Cyclops Blink's modular design, allowed it to survive reboots and firmware updates, functioning as a covert C2 relay and launchpad for remote operations – even into Ukrainian networks via compromised infrastructure in third-party countries.[30] This approach enabled Russian operators to obscure their activity, re-enter previously remediated environments, and coordinate attacks from outside the national borders.

The aim of foothold persistence also extended to system-level alterations and supply chain abuse. Russian actors frequently modified host systems by creating new services, altering authentication mechanisms, or trojanizing legitimate software.[31] InvisiMole, linked to the FSB or SVR, embedded implants into operating system ISOs and software installers placed on shared drives, or misused update channels, thus ensuring payloads were triggered by unsuspecting users or IT staff.[32] In parallel, state-linked actors embedded durable backdoors into telecom networks to silently intercept communications or reestablish access at will. Together, these efforts reflect a broader Russian doctrine of maximizing foothold durability across both endpoint and infrastructure layers – prioritizing stealth, redundancy, and operational resilience. Russian actors have invested heavily in establishing persistent access to Ukraine-based targets, enabling military commanders to adapt to the rapidly evolving battlespace. This persistent foothold has been a critical enabler of coordination between Russia's cyber and military operations, allowing timely intelligence collection, targeting support, and operational flexibility throughout the conflict.

Defense Evasion

Russian operators frequently disguised destructive operations as ransomware to mislead responders and obscure state involvement. In early 2022, WhisperGate posed as ransomware on Ukrainian systems, displaying a fake ransom note while permanently corrupting data.[33] Similarly, in October, Sandworm deployed "Prestige" against Ukrainian and Polish logistics firms – encrypting the files but with no intention to collect the ransom.[34] These pseudo-ransomware attacks aligned with GRU sabotage tactics and were timed for strategic effect, aiming to sow confusion, conceal attribution, and amplify disruption under the guise of criminal activity.

Russian APTs also relied heavily on living-off-the-land and fileless techniques to evade detection. These included abusing legitimate tools, like PowerShell, WMIC, and Windows administrative utilities, to blend malicious actions with normal system behavior.[35] In IT environments, malware was often injected into trusted

[29] https://thehackernews.com/2023/07/cert-ua-uncovers-gamaredons-rapid-data.html

[30] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-054a

[31] https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[32] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover

[33] https://www.crowdstrike.com/en-us/blog/technical-analysis-of-whispergate-malware/

[34] https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland

[35] https://cloud.google.com/blog/topics/threat-intelligence/dissecting-one-ofap

processes like explorer.exe to avoid triggering defenses, while in OT networks, Sandworm's October 2022 grid attack used only native ICS tools to disable power infrastructure before deploying custom malware. Fileless execution, process injection, and heavy obfuscation were standard: Gamaredon's droppers were layered in VBScript with multiple stages, and APT28 weaponized encrypted macros and loaders in phishing documents to bypass detection engines.[36]

To further hinder forensics, Russian threat actors actively cleansed traces from compromised systems. Sandworm employed tools like WhiteCat to wipe logs and artifacts after the attacks, thus complicating incident response.[37] During OT-IT combined operations, such as the October 2022 energy grid sabotage, they used CaddyWiper not just for destruction but also to erase digital footprints.[38] Other stealth methods included timestomping (modifying file timestamps) and using stolen code-signing certificates – for example, HermeticWiper's driver appeared legitimate.[39] Combined with diversionary DDoS attacks, these tactics extended operational cover, giving attackers more time to complete objectives or retreat without being detected.

Lateral Movement

Once inside a network, Russian operators relied heavily on credential-based lateral movement. Using stolen passwords, NTLM hashes, and Kerberos tickets, they impersonated authorized users through techniques like pass-the-hash and admin credential reuse. These methods allowed seamless access across hosts, file shares, and mail systems: as insiders rather than intruders. APT28 and APT29 frequently employed this tactic in 2022, using valid credentials (often with domain admin privileges) to move quietly across networks.[40] To execute payloads, they leveraged native tools like PsExec and WMI, and commonly enabled RDP or exploited Active Directory trusts to traverse government environments. By mimicking routine admin behavior, attackers blended in and evaded detection.

After establishing initial access, Russian actors would conduct internal reconnaissance to map out targets and expand the reach. Tools like Masscan and Nmap were used to identify open ports, exploitable services and exposed shares. In Ukraine, Gamaredon propagated via network drives and USBs where it placed malware with enticing filenames to trick the users into opening them – a semi-automated method that relied on user action for lateral movement.[41] CERT-UA documented such tactics as part of broader campaigns where worm-like scripts assisted in deploying payloads across multiple endpoints (see references). Sandworm's Industroyer2 attack in April 2022 suggested earlier movement from IT into segmented ICS environments, likely through a compromised domain bridge, enabling access to substation controls. Such combined tactics allowed Russian actors to take control of large portions of network within hours.

Russian groups also exploited trust relationships to move laterally between organizations. Targeting Ukrainian IT service providers and software vendors, they accessed downstream clients thus essentially turning supply chains into infiltration paths. Though not on the scale of NotPetya, 2022 saw a rise in such tactics. Breaching a vendor with a VPN or privileged access to a government agency allowed pivoting into core infrastructure. Ukrainian authorities warned that trusted intermediaries posed serious vulnerabilities, giving Russian operators indirect yet highly effective routes into sensitive systems.

[36] https://harfanglab.io/insidethelab/gamaredons-pterolnk-analysis https://redpiranha.net/news/threat-intelligence-report-may-20-may-26-2025
[37] https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates
[38] https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack
[39] https://thehackernews.com/2024/10/researchers-uncover-hijack-loader.html
[40] https://attack.mitre.org/groups/G0007
[41] https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-gamaredon-ukraine-phishing

Command and Control (C2)

In 2022, Russian cyber campaigns utilized multi-layered, evasive command-and-control (C2) architectures in order to manage malware while concealing operational origins. The implants typically communicated through global relay nodes or proxy chains, avoiding direct links to Russian IPs. For example, Sandworm's Cyclops Blink botnet relied on compromised routers worldwide to route commands into Ukrainian networks. The communications were often encrypted, frustrating detection and attribution efforts. Gamaredon increased stealth by automating C2 rotation and shifting IPs 3 to 6 times per day with fast-flux techniques thus hindering being blocked and tracked.

To further obscure their activity, Russian APTs leveraged trusted platforms as C2 channels. HTTP/HTTPS traffic was routed through lookalike domains, hijacked DNS, or legitimate services such as Telegram, cloud storage providers (e.g., OneDrive, Dropbox) and email infrastructure.[42] Gamaredon was able to embed encrypted C2 instructions in a seemingly benign app traffic using the Telegram API.[43] Other actors stored instructions in email drafts or cloud-hosted files, blending C2 into normal network behavior and forcing the defenders to scrutinize traffic from widely used platforms rather than relying on domain-based blocking.

Russian groups were also embedding multiple fallback domains and hardcoded IPs into malware to ensure persistent access even if the infrastructure was exposed, thus prioritizing resilience. During high-stakes operations, particularly the February 2022 invasion, attackers relied on out-of-band control – their wiper malware was likely pre-configured to trigger at specific times without any real-time input. Dormant implants may have also been activated via USB delivery or local task schedulers, thus reducing dependence on live communications. This autonomous, layered C2 design allowed Russian cyber units to maintain operational continuity throughout the conflict, even under active defense pressure.

Impact

Russia's 2022 cyber operations reflected a full-spectrum, militarized strategy closely integrated with conventional warfare. From phishing and exploits to lateral movement and credential abuse, each stage of the intrusion lifecycle was optimized for espionage, disruption, or both. Units like Sandworm, APT28, APT29, Turla, and Gamaredon coordinated cyber strikes with physical attacks to sabotage infrastructure, disrupt command and control, and support battlefield operations. Their tactics, rooted in familiar MITRE ATT&CK techniques, were adapted for wartime through innovations like wipers disguised as ransomware, OT sabotage, and credential exploitation. This fusion of cyber and kinetic tools defined the current hybrid warfare and underscored the need for defenders to be able to counter persistent, adaptive threats across the full ATT&CK spectrum.

Defacement

In the weeks leading up to Russia's full-scale invasion of Ukraine, the Russian-aligned threat actors carried out a coordinated wave of cyber defacements targeting at least 70 Ukrainian Government's websites, including the Ministry of Foreign Affairs, Cabinet of Ministers, and the National Defense Council, on 14 January 2022.[44] Site visitors were faced with ominous messages in Ukrainian, Russian, and even intentionally misspelled Polish, warning to "Be afraid and wait for the worst". These altered pages aimed to sow fear, undermine public confidence, and psychologically prime the population just over a month before kinetic action began.

[42] https://dergipark.org.tr/en/download/article-file/3704452 https://www.tanium.com/blog/cyber-threat-intelligence-roundup-july-27

[43] https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations

[44] https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers

The follow-up defacement extended the campaign on 15 February 2022, targeting additional government and financial service sites – in an action mirroring the escalating geopolitical tensions.[45] Cyber security experts later identified the discussed defacements as part of a deliberate Russian soft-power offensive, leveraging psychological operations (psy-ops) to destabilize Ukraine's civil resilience and readiness ahead of the invasion. While non-destructive from a technical standpoint, these defacements carried significant symbolic weight as the digital precursor to physical aggression.

In early 2022, Russia's cyber campaign was marked by aggressive use of wiper malware designed to destroy data and cripple systems in advance of its invasion of Ukraine. At least six distinct wipers – including HermeticWiper, WhisperGate, and AcidRain – were deployed against the Government, banking and infrastructure targets.[46] HermeticWiper alone struck hundreds of machines hours before the invasion, functioning as a "cyber artillery counter-preparation bombardment" aiming to disrupt Ukraine's response. GRU-linked units, like Sandworm, continued using wipers throughout the year, often pairing them with kinetic strikes – such as the successful substation blackout aligned with missile attacks on the grid in October.

The Russian actors also expanded the attacks into the field of operational technology. Industroyer2, deployed in April 2022, targeted Ukrainian substations using industrial protocols, though it was neutralized before causing outages.[47] Other efforts, like the Viasat breach that deployed AcidRain to satellite modems, succeeded in disrupting civilian infrastructure across Ukraine and parts of Europe, showcasing in use cyber operations to amplify physical assaults.

Meanwhile, DDoS attacks by groups like KillNet and XakNet overwhelmed banks, Government portals, and news outlets, to create confusion and strain resources.[48] Though basic in execution, these attacks supported psychological operations and diverted defender attention. Hack-and-leak campaigns were further blurring the lines between cyberwarfare and disinformation. Russian operatives were exfiltrating and releasing sensitive data, often tied to pro-Kremlin narratives, including a high-profile breach of the Ukrainian National News Agency. These hybrid tactics combined sabotage, disruption, and information warfare, forming an integrated strategy to destabilize Ukraine and erode the people's trust in its institutions.

5.3. Strategic Use Cases: Integration into Hybrid Warfare

In 2022, the Russian Federation showcased sophisticated integration of cyber operations and broader hybrid warfare strategies during its full-scale invasion of Ukraine. Russian cyber actors strategically utilized offensive cyber capabilities to directly amplify and synchronize with conventional military operations, psychological influence campaigns, and political objectives.

Cyber-Enabled Psychological and Information Operations

In the weeks leading up to Russia's full-scale invasion, a targeted psychological campaign aimed at destabilizing Ukraine was launched. In late January 2022, Ukrainian schools, banks, and public buildings faced a wave of hoax bomb threats via phone, SMS, and email, falsely warning of planted explosives – prompting a widespread panic and straining emergency services.[49] At the same time, scam calls pressured staff to shut down systems or transfer data, blending financial fraud with strategic disinformation. Finally, on February 15–16, Ukrainian defense and finance sectors, including major banks, like PrivatBank and Oschadbank, were

[45] https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15

[46] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

[47] https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack

[48] https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine

[49] https://www.reuters.com/world/europe/ukrainian-schools-grapple-with-hoax-bomb-alerts-amid-russia-tension-2022-01-28/

hit by a massive DDoS campaign which severely disrupted mobile apps, call centers and online services just days before the invasion; Western intelligence later attributed the attacks to Russian-backed actors.[50] Together, the discussed tactics – fake bomb alerts, deceptive phone calls, and disruptive DDoS attacks – formed a multi-layered psy-ops effort designed to weaken public trust, disrupt essential services, and pave the way for kinetic operations.

Critical Infrastructure Disruption Aligned with Military Actions

The Russian cyberattacks conducted against Ukraine's critical infrastructure in 2022 were closely synchronized with military operations aiming to maximize the disruption, degrade defenses, and erode the civilian morale. The GRU's Sandworm unit played a central role, launching the AcidRain malware on February 24 to cripple the Viasat KA-SAT satellite network just hours before the invasion, thus severely disrupting the Ukrainian military communications and affecting thousands of wind turbines in Germany.[51] In April, Sandworm attempted an Industroyer2 attack on Ukraine's power grid, timed with a major eastern offensive, aiming to trigger blackouts and sow battlefield confusion.[52] A similar operation in October combined cyberattacks on regional energy systems with missile strikes, illustrating Russia's integrated cyber-physical warfare strategy.[53]

Meanwhile, the Russian cyber espionage directly supported battlefield intelligence. Groups like Gamaredon (FSB) and APT28 (GRU) breached the Ukrainian Government and military communications to extract targeting data APT28 exploited credentials, some of it captured from the soldiers, to access private communications, including Telegram and secure messaging apps, and allowing Russia to monitor, manipulate, or disrupt frontline command.[54] [55] Together, the mentioned operations demonstrated how cyber capabilities were tightly woven into the bigger offensive operations, serving as a source of intelligence and enhancing tactical effectiveness.

Destructive Operation

A particularly aggressive form of cyber-kinetic integration seen in 2022 involved deployment of wiper malware timed with conventional military strikes. As the Russian forces mobilized, cyber actors launched destructive attacks on the Ukrainian Government, military, and infrastructure networks seeking to sow chaos and confusion. On February 23, the eve of the invasion, HermeticWiper was deployed across key systems – disrupting governmental communications, delaying Ukraine's initial response and giving the Russian troops a tactical advantage.[56] The pattern continued throughout the year, with Sandworm pairing malware attacks to missile strikes on energy and transport sectors.[57] The October assaults, for example, combined cyber intrusions with physical attacks on energy infrastructure, each magnifying the impact of the other. These coordinated operations aimed to paralyze systems, erode civilian morale, and undermine confidence in the Government's ability to ensure crisis response.

Conclusion: Cyber Operations as Integral Warfare Components

In 2022, the Russian cyber operations functioned as integral components of the broader invasion strategy rather than just isolated digital events. The pre-invasion psychological campaigns, ranging from bomb threats and scam calls to DDoS attacks on the banking systems, were designed to sow panic and erode trust. These

[50] https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/
[51] https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[52] https://cyberscoop.com/ukrainian-electrical-grid-industroyer2-russia-sandworm
[53] https://therecord.media/sandworm-attack-ukraine-energy-facility-missile-strikes
[54] https://therecord.media/kremlin-linked-apt29-hackers-target-ukrainian-state-agencies-espionage
[55] https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf
[56] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a
[57] https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

were followed by cyber strikes on satellite and energy infrastructure, timed precisely with missile attacks and ground offensives. Espionage units supported battlefield operations by compromising military apps and frontline communications, while wiper malware, like HermeticWiper, was deployed to paralyze the systems at critical points in time. Together, the actions reflected a deliberate fusion of cyber and kinetic force aimed at overwhelming Ukraine's defenses through disruption, deception, and direct tactical support.

5.4. Infrastructure and Tooling

Russia's cyber operations in 2022 indicate a fully integrated doctrine that combines advanced state-led intrusions with disruptive proxy activity. While some high-profile attacks had failed – such as Sandworm's Industroyer2 attempt on Ukraine's power grid and the early exposure of Cyclops Blink, the efforts revealed Russia's intent to synchronize cyber and kinetic campaigns for maximum disruption.

Despite the setbacks, Russian APTs achieved extensive operational success in the analyzed period of time. Groups like APT28 and APT29 blended custom malware with red-team tools, rapidly adopting exploits, like Follina, to deliver payloads, such as .NET-based CredoMap stealer.[58] The APTs increasingly relied on the evasive C2 infrastructure, abusing services like Telegram and GitHub to mask the traffic. They also compromised network hardware at scale, deploying implants, like Jaguar Tooth, on vulnerable Cisco routers and expanding footholds through infected firewalls and hijacked routers.

Destructive malware was featured prominently: in February, HermeticWiper, AcidRain and other wipers hit Ukrainian networks hours before the invasion. In April, Sandworm deployed wipers and Industroyer2 in a failed but coordinated OT-IT sabotage campaign. Espionage units, like Turla, used PowerShell tools, like Capibar, to hijack Exchange servers, deploy backdoors, like Kazuar, and harvest cloud credentials while often leveraging existing infections for stealth.

APT29 advanced to cloud-first attacks, exploiting Azure AD and deploying tools like MagicWeb to bypass authentication silently.[59] These operations highlighted a shift toward persistence, stealth and cloud exploitation over traditional malware deployment.

Parallel to state APTs, pro-Russian hacktivist fronts, like KillNet, NoName057(16) and XakNet, were engaged in DDoS attacks, defacements, and data leaks. Though technically crude, their scale and coordination were significant. KillNet amassed over 100,000 Telegram followers and aligned their attacks with the Russian messaging. NoName057(16)'s "DDoSia" campaign incentivized volunteers to run automated attack tools. XakNet leaked sensitive Ukrainian data in sync with APT28 activity, suggesting GRU links.

These proxy groups relied on anonymized infrastructure, bulletproof hosting and Telegram for coordination. While their disruptions were often brief, they served to amplify Russian narratives and create plausible deniability for the Russian Government.

To sum up, Russia's 2022 cyber campaign operated on two levels: high-impact APT intrusions and mass-scale hacktivist disruption. These operations were not random – they were calculated to strike Ukraine hard and fast in the opening phases of the war, softening defenses, spreading panic, and impairing the country's ability to respond. Together, they formed a hybrid model of "information confrontation," blending elite tradecraft with volunteer-driven chaos to destabilize critical infrastructure, amplify psychological pressure, and directly support the objectives of Russia's military invasion. Notably, after the full-scale invasion, Russian cyber forces appeared to have exhausted much of their prepared toolsets. After unleashing a surge of malware, wipers, and coordinated disruptions, both APT groups and state-sponsored threat actor groups went largely silent – entering a period of operational inactivity, marking a sharp pause in major offensive cyber activity.

[58] https://securityscorecard.com/research/apt28s-stealer-called-credomap/

[59] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

6. The 2025 Landscape: Elevated Offensive Capabilities

6.1. Emerging Threat Actors and Shifts: New Players, Changing Priorities, State-Proxy Relationships

Since the start of Russia's 2022 invasion of Ukraine, Moscow has significantly expanded and reorganized its offensive cyber forces. This included forming new cyber units, reinforcing existing ones, and mobilizing affiliated hacker groups and IT specialists. The expansion increased the number of operatives and broadened the range of tactics, techniques and procedures in use. As a result, Russia has been able to scale its cyber operations more effectively, both within Ukraine and against foreign targets, boosting the reach and adaptability of its campaigns.

New and Emerging Threat Actors (2022–2025)

A key development from 2022 to 2025 has been the emergence of new or previously obscure Russian-linked threat actors. Beyond the well-known APTs, groups designated as UAC-0125, UAC-0149, UAC-0184, UAC-0195, UAC-0200, and UAC-0226 have become active during the war, as identified by Ukraine's CERT. These actors are expanding their capabilities, often aligning with Russian strategic interests. Notably, UAC-0184, first reported in late 2023, focuses on espionage against Ukraine's military and Government, using military-themed phishing and social engineering to target defense institutions, including one in Finland.[60] UAC-0184's use of multistage malware and adaptive techniques reflects the evolving nature of the conflict and the growing diversity within Russia's cyber ecosystem. While not always directly linked to state intelligence, groups like UAC-0184 are assessed with high confidence as pro-Russian actors, illustrating Moscow's increasing reliance on both established units and newer operatives to sustain its cyber pressure.

Changing Operational Priorities of Established APT Groups

From 2022 to 2025, Russia's cyber operations expanded in both scale, coordination and complexity. In addition to the long-standing APTs, Ukraine's CERT identified a range of newer or previously obscure pro-Russian actors, such as UAC-0184, that became active during the war. These groups have adopted increasingly sophisticated tactics, including military-themed phishing, multistage malware, and adaptive targeting. UAC-0184, for instance, focused on espionage against Ukraine's military and Government, with the activity extending to at least one NATO country. While not always formally tied to the Russian intelligence services, such groups consistently align with Moscow's strategic objectives, reflecting the state's growing reliance on auxiliary cyber operators to sustain pressure.

Meanwhile, the Russian-established APTs (Gamaredon, Turla, APT28, APT29, and Sandworm) have remained highly active, refining their capabilities and shifting focus in response to wartime demands. APT28 pivoted from global espionage to targeting Ukraine and NATO states, running coordinated campaigns across at least 14 countries.[61] It adopted newly discovered exploits, like Follina, and pursued military and critical infrastructure targets to gather actionable intelligence. APT29 expanded its operations to include cloud compromise and supply chain attacks, focusing on diplomatic and defense entities while emphasizing stealth through living-off-the-land techniques and credential abuse.[62]

[60] https://www.darkreading.com/cyberattacks-data-breaches/uac-0184-targets-ukrainian-entity-finland-remcos-rat

[61] https://veroot.com/cyber-resources/russian-military-hacker-group-target-nato-allies-with-new-masepie-malware

[62] https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing

Gamaredon ramped up high-volume phishing against Ukrainian government and military institutions, evolving its delivery methods by abusing legitimate services, like Cloudflare Tunnels, Mega, and Telegram, to improve persistence and evade detection.[63] Turla reoriented its campaigns toward Ukraine and nearby allies, supporting Russian military efforts through targeted intrusions and new malware families, like Kazuar.[64] It increasingly relied on compromised third-party infrastructure to maintain operational cover. Sandworm has evolved from a destructive Russian cyber unit into a hybrid espionage entity. While still capable of disruptive campaigns, it now conducts complex, multi-phase intrusions – combining initial access via perimeter devices, living-off-the-land techniques, persistent data exfiltration, and influence operations aligned with battlefield and political objectives.[65] While it continued targeting critical infrastructure, its methods emphasized access and control over blunt disruption.

Throughout this period, Russian APTs have grown more agile and coordinated. Their tactics now emphasize stealth, speed, and strategic alignment with military goals. Increased reliance on cloud abuse, rapid exploit deployment, and infrastructure obfuscation reflects an adaptive, professionalized cyber apparatus designed for sustained access and support of Russia's broader war effort.

State–Proxy Relationships: Hacktivists and Cybercriminal Groups

By 2025, Russia's state-proxy cyber model has become a key force multiplier. Its cyber apparatus spans a multitiered network: elite intelligence-linked APTs, mid-level emerging groups, and lower-tier hacktivist or criminal actors – all operating in coordination to serve Moscow's goals. The Russian command structures appear able to guide these actors as needed. NoName057(16), for instance, launched DDoS attacks on European transport and government sites backing Ukraine,[66] reinforcing Russia's push to weaken Western support. In 2023, another hacktivist group, KillNet, leaked stolen data belonging to individuals with ties to the North Atlantic Treaty Organization (NATO).[67] These proxies blur the line between patriotic activism and state-linked operations, serving as useful assets in Russia's hybrid warfare strategy.

Such a hierarchy enables complex workflows, e.g., an APT gathers intelligence while a proxy group disrupts the same target, thus complicating attribution. From 2022 to 2025, Russia expanded its cyber force by blending legacy units with semi-official proxies, intensifying campaigns against Ukraine and its allies. This integrated model offers flexibility, reach, and deniability – powering everything from stealthy espionage to overt sabotage across multiple fronts.

The Kremlin's reliance on hacktivist and criminal proxies has been further blurring the line between state and non-state operations, producing a layered and adaptive threat landscape. Such developments mark maturation of Russia's cyber warfare model: fusing official units with semi-autonomous proxies to achieve strategic outcomes. By 2025 this ecosystem has become more expansive and coordinated, compared to 2022 as it supports Russia's military and geopolitical aims through a blended cyber force.

6.2. Advanced Techniques: AI-Driven Attacks, Polymorphic Malware, Multi-Vector Campaigns

Between 2022 and 2025, Russian state and proxy cyber actors were adopting and adapting global innovations thus significantly advancing their offensive capabilities. The use of AI-driven tools was on a marked rise in the

[63] https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations

[64] https://socprime.com/blog/capibar-and-kazuar-malware-detection-turla-aka-uac-0024-or-uac-0003-launches-targeted-cyber-espionage-campaigns-against-ukraine/

[65] https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm

[66] https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

[67] https://cloud.google.com/blog/topics/threat-intelligence/killnet-new-capabilities-older-tactics

period enhancing social engineering, malware creation, and influence operations. Simultaneously, Russian groups deployed polymorphic malware with improved evasion techniques thus additionally impeding detection and response. These developments were often integrated in coordinated, multi-vector campaigns combining technical intrusions, psychological operations, and real-world conflict. The following section examines key TTPs from the discussed period, revealing how Russian actors have both mirrored and shaped global cyber trends to expand their strategic reach.

AI-Driven Attacks and Machine-Augmented Operations

Russia has integrated artificial intelligence in its cyber operations in a major development observed by 2025. Russian threat actors began leveraging generative AI to scale up phishing, improve malware, and boost operational stealth – mirroring the trends seen in China, Iran, and North Korea. OpenAI reported shutting down multiple ChatGPT accounts linked to Russian operatives who used the tool to craft malware, build command-and-control infrastructure, and fine-tune Windows payloads. In one case, the malware developed using AI included credential theft, privilege escalation, and Telegram-based exfiltration, deployed first against gaming communities in a campaign dubbed "ScopeCreep."

AI also became central to social engineering and influence campaign: Russian-linked actors used LLMs to generate realistic phishing emails at scale, contributing to a sharp global spike in email-based attacks.[68] Despite the safeguards, adversaries employed jailbreak models or black-market tools, like WormGPT, to bypass restrictions. Some accounts using ChatGPT to create pro-Russian propaganda aimed at NATO and Western elections which was then distributed on Telegram and X.[69] [70]

One of the earliest wartime uses of generative AI was a deepfake video of President Zelenskyy calling for Ukraine to surrender, broadcast during Russia's assault on Kyiv in 2022. Although low in quality and quickly debunked, it marked the first use of deepfakes in active conflict. Since then, synthetic profile images and AI-generated voices have been in use to support fake personas and online propaganda.

While not leading in innovation, Russian operators have demonstrated adaptability by co-opting both Western AI platforms and likely developing domestic tools. From 2022 to 2025, AI significantly enhanced their speed, precision, and deniability. Looking ahead, Russian threat actors are likely to further automate reconnaissance, exploit development and information warfare while ushering in more autonomous and scalable cyber campaigns.

Polymorphic Malware and Advanced Evasion Techniques

Faced with improved defenses and rapid incident response during the Ukraine war, Russian threat actors have increasingly emphasized stealth through polymorphic and multi-stage malware.[71] [72] Polymorphic techniques (where malware continuously alters its signature or execution logic via obfuscation or recompilation) have surged in sophistication and frequency over 2022–2025. The trend of detectingn evasion through generative AI-enabled malware self-modification has been accelerated by early AI experimentation and blending of criminal and state tools.

[68] https://www.recordedfuture.com/research/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale

[69] https://www.theregister.com/2025/06/06/chatgpt_for_evil/

[70] https://www.engadget.com/ai/foreign-propagandists-continue-using-chatgpt-in-influence-campaigns-161509862.html

[71] https://www.globenewswire.com/news-release/2025/05/20/3085225/0/en/ESET-Research-APT-Report-Russian-cyberattacks-in-Ukraine-intensify-Sandworm-unleashes-new-destructive-wiper.html

[72] https://www.wired.com/story/ukraine-russia-wiper-malware/

Proof of concepts like BlackMamba have shown how AI can power malware that dynamically evolves in the memory.[73] In that case, a benign-looking app fetches a fresh keylogger code via OpenAI's API and exfiltrates data over Microsoft Teams without writing to disk. While there is no confirmed Russian deployment of such tools, their known use of AI for malware refinement indicates a growing interest in AI-driven polymorphism.

Russian groups have adopted these techniques at different sophistication levels. GRU-linked UAC-0184 demonstrated advanced evasion using steganography, DLL sideloading, and process injection.[74] In 2023, it hid payloads in PNG files, deployed fake DLLs alongside legitimate executables, and used multi-stage chains, from LNKs to RATs, designed to bypass detection and delay containment or attribution.

Over the discussed period, Gamaredon (FSB-linked UAC-0010) has evolved from basic phishing to sophisticated delivery tactics involving geofencing, HTML smuggling, and cloud-based C2 channels, like Telegram bots and Cloudflare Tunnels.[75] [76] By 2025, it has adopted fast-flux DNS, HTTPS communications, and exploited a Windows LNK 0-day for stealthy execution – showing a marked technical growth.[77]

Russia has also blurred the lines between espionage and cybercrime. APT28 repurposed such tools as Mirai and adopted commodity malware, such as XWorm, a flexible RAT used for espionage, ransomware, and credential theft. In 2024, UAC-0184 deployed XWorm through a hybrid chain of PowerShell, Python, and Shadowloader, exemplifying a modular strategy that complicates attribution.[78]

To summarize, the Russian malware capabilities became highly evasive, rapidly adaptable, and increasingly polymorphic between 2022 and 2025. With AI now aiding iteration, future campaigns will likely feature malware that self-adjusts, abuses trusted infrastructure, and evades even AI-based detection. This adaptive cycle will demand a shift toward an equally agile, AI-assisted defenses capable of outpacing future malware evolution.

Multi-Vector Campaigns and Blended Threat Operations

The Russian cyber warfare between 2022 and 2025 featured multi-vector campaigns: coordinated operations that combined technical intrusions, information warfare, and kinetic actions at times. Rather than relying on a single attack vector, Russian state and proxy actors increasingly blended cyber espionage, disruptive attacks, data leaks, psychological operations, and military strikes into integrated efforts designed to amplify each other's impact. Rooted in Russia's hybrid warfare doctrine, this approach reached an unprecedented scale during the war in Ukraine.

The Russian intelligence agencies coordinated across cyber units to achieve multi-domain effects. APT28 (Fancy Bear), known for high-profile operations, like the 2016 DNC breach, continued enacting this strategy stealing sensitive data suitable to be repurposed for propaganda. In 2023, the breach of a Ukrainian satellite provider raised concern over strategic leaks, which groups like GhostWriter/UNC1151 later amplified, thus pointing to deliberate coordination with GRU operations. The campaigns often combined espionage, staged leaks, and disruptive actions, such as DDoS attacks, illustrating Russia's emphasis on synchronized tactics across cyber and information domains.

[73] https://www.esecurityplanet.com/threats/blackmamba-malware-edr-bypass/
[74] https://cyble.com/blog/uac-0184-abuses-python-in-dll-sideloading-for-xworm-distribution/
[75] https://www.recordedfuture.com/research/bluealpha-abuses-cloudflare-tunneling-service
[76] https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html
[77] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a
[78] https://cyble.com/blog/uac-0184-abuses-python-in-dll-sideloading-for-xworm-distribution/

Moscow also extended its reach through proxy groups and cybercriminal affiliates, such as KillNet, which emerged prominently in 2022. These actors launched broad DDoS attacks against Western governments, healthcare, and transportation infrastructure – often timed with diplomatic tensions or battlefield events.[79] Despite their limited technical sophistication, the attacks generated disruption, psychological pressure, and resource strain. Their alignment with Kremlin narratives and potential links to state support created a layered threat model: elite APTs executed targeted intrusions, while proxies added scale, noise, and deniability.

The mentioned operations were not isolated incidents but rather components of broader strategic campaigns consistent with Russia's information confrontation doctrine. Ukraine became a testing ground for the model also detectable in global ransomware, espionage, and influence operations. Future conflicts involving Russia are likely to feature synchronized cyber and information strikes designed to confuse, degrade, and destabilize.

In summary, the Russian offensive cyber operations in 2022 to 2025 evolved into flexible, multi-pronged campaigns that fused technical and informational tactics. The adoption of AI-driven tools, polymorphic malware, and hybrid coordination reflects a deliberate evolution of the Russian cyber doctrine. From the standpoint of defenders, it has created a more agile, ambiguous, and persistent threat environment – one that demands integrated cross-domain strategies, faster attribution, and continual monitoring of the Russian capabilities and tradecraft.

6.3. Targeting Trends: Broader Attack Surfaces – OT, AI Systems, IoT, Critical Civic Tech

Since 2022, the Russian state-backed and proxy cyber actors have broadened their focus beyond traditional IT networks, increasingly targeting operational technology (OT), AI systems, IoT devices, and critical civilian infrastructure. Driven by the war in Ukraine and rising global tensions, this shift reflects Moscow's strategy to maximize disruption across cyber-physical domains. Coordinated by Russian security services, a mix of APTs, cybercriminals, and hacktivists have carried out both destructive and covert attacks, often paired with information warfare and military actions, to strike at the heart of civilian and strategic systems.

Operational Technology (OT) and Critical Infrastructure

Russia's increasing focus on operational technology (OT) systems tied to critical infrastructure has been a key trend since 2022. The GRU-linked Sandworm group has led these efforts, most notably with the deployment of Industroyer2 in April 2022, which targeted Ukraine's power grid by manipulating substation controls using the IEC-104 protocol. The attack was timed to coincide with missile strikes, demonstrating a clear cyber-kinetic coordination strategy. Although Ukrainian defenders largely mitigated the impact, the post-incident analysis revealed that Sandworm had maintained covert access to SCADA systems for months prior, using living-off-the-land techniques to stage the operation. This exemplifies Russia's growing OT attack proficiency and its integration of cyber operations with conventional military campaigns.

Between 2022 and 2025, Russian threat actors have also tested and developed new ICS-specific malware, reinforcing their long-term investment in OT disruption. COSMICENERGY, discovered in 2023, was designed to issue rogue commands to remote terminal units (RTUs), potentially causing power outages.[80] Likely built by a Russian defense contractor, it resembled Industroyer in both design and protocol targeting. However, COSMICENERGY lacked key capabilities of reliable execution, suggesting it was a prototype or a testbed. Its limited functionality signals that Russia is still refining its approach – and is likely to produce more specialized, destructive OT malware tailored to real-world infrastructure environments in future campaigns.

[79] https://www.reuters.com/world/europe/russian-hackers-targeting-western-critical-infrastructure-uk-says-2023-04-18/

[80] https://cloud.google.com/blog/topics/threat-intelligence/cosmicenergy-ot-malware-russian-response/

Russia's focus on critical infrastructure has also extended beyond Ukraine, increasingly targeting Western systems in the countries backing Kyiv. APT28, a GRU-linked group, conducted campaigns in 2022–2023 against energy, transportation, and pipeline networks across NATO member states. One of the campaigns included infiltration of a satellite communications provider to critical infrastructure operators, raising concerns about threats to both civilian and military space-based assets.[81] In May 2023, Sandworm was suspected of an attack on 22 Danish energy firms which featured exploitation of a firewall vulnerability (CVE-2023-28771) in Zyxel devices to gain root access.[82] Although no major outages occurred, the breach forced multiple providers offline, showing Russia's readiness to project cyber power against adversary infrastructure.

Beyond short-term sabotage, Russian actors are also pursuing long-term access to critical systems for strategic advantage. In 2023, Sandworm-linked actors, like Solntsepek, breached Ukrainian telecom providers and executed a destructive attack on Kyivstar after a while, wiping out thousands of servers and disrupting service for 24 million users.[83] Although military communications remained unaffected, the goal appeared to have been to degrade civilian and command-and-control infrastructure. Elsewhere, APT29 targeted OT-adjacent systems, exploiting a JetBrains TeamCity vulnerability potentially offering pathways from IT networks into industrial control layers at manufacturing firms.[84] These activities confirm that critical infrastructure is now a sustained target in Russia's cyber doctrine, combining immediate disruption with persistent espionage.

AI Systems and AI-Driven Platforms

From 2023 to 2025, both Russian state-linked threat actors and affiliated cybercriminals increasingly incorporated artificial intelligence in their operations. By early 2025, reports from Dark Reading and Wired confirmed that Russian groups had begun experimenting with generative AI platforms, like ChatGPT, to enhance malware development, evade defenses, and scale offensive cyber operations.[85] This included tasks such as debugging payloads, scripting initial access tools, and crafting more deceptive phishing lures. These developments placed Russian operatives alongside peers from China, Iran, and North Korea in the global adoption of AI-enabled offensive tooling.

At cybercrime level, actors tied to the Russian-speaking underground began integrating AI into Malware-as-a-Service (MaaS) offerings. Analyses from Trellix, Microsoft, and Recorded Future in early 2025 identified Lumma (also known as LummaC2), an infostealer toolkit, likely developed by Russian operators, which had been enhanced with AI-driven features.[86] These included automated filtering of harvested credentials and intelligent bot triage systems: streamlining monetization and operationalization of the stolen data. This points to a maturing MaaS ecosystem where AI is embedded to improve scalability and efficiency.

Integration of AI boosted a rapid evolution in social engineering as well. According to the Financial Times, Russian-speaking ransomware and phishing groups achieved a 442% increase in voice phishing ("vishing") campaigns by late 2024, fueled by the growing use of AI voice cloning.[87] Generative models are also used to mass-produce phishing emails that mimic human language and tone with high fidelity. These techniques enhance both the credibility and success rate of social engineering operations, lowering the barrier for non-technical actors to participate in sophisticated cybercrime.

[81] https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/

[82] https://industrialcyber.co/reports/sektorcert-reports-cyber-attack-against-danish-critical-infrastructure-raises-concerns-of-state-involvement/

[83] https://cyberscoop.com/russia-ukraine-kyivstar-vitiuk/

[84] https://www.techtarget.com/searchsecurity/news/366563365/Russian-APT-exploiting-JetBrains-TeamCity-vulnerability

[85] https://www.darkreading.com/threat-intelligence/openai-bans-chatgpt-accounts-nation-state-threat-actors

[86] https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

[87] https://www.cybersecuritydive.com/news/fbi-us-officials-impersonated-text-ai-voice/748334/

While not all AI-assisted tactics have been directly attributed to Russian groups, academic research confirms that tools like large language models can automate phishing, generate malware variants, and manage synthetic social botnets. The applicability of these methods, combined with Russia's known history of adopting foreign innovations tactically, suggests that AI will increasingly underpin both state-aligned and criminal cyber operations moving forward. This convergence of AI and cybercrime marks a significant escalation in the complexity and reach of Russian cyber threats.

Internet of Things (IoT) and Network Device Compromise

Since 2022, Russia has increasingly expanded its cyber operations into the Internet of Things (IoT), targeting vulnerable devices, like routers, firewalls, and industrial sensors. A key example is *Cyclops Blink*, a botnet attributed to Sandworm (GRU) and seen as the successor to *VPNFilter*. Discovered in early 2022, it infected thousands of WatchGuard and ASUS network appliances worldwide, establishing a layered command-and-control infrastructure. U.S. and UK agencies disrupted the botnet by remotely removing the malware but the incident underscored how aggressively Russian actors we the were exploiting IoT hardware for persistent access, stealth, and potential lateral movement. APT28 (Fancy Bear) has been pursuing similar methods; in 2023, it was found exploiting unpatched Cisco routers to deploy implants and conduct surveillance across Europe and North America. Firmware-level compromises on edge devices enable long-term access that often bypasses traditional endpoint defenses – making IoT exploitation a strategic asset in Russian cyber campaigns.[88]

Russian groups have also weaponized IoT for battlefield and sabotage purposes. Sandworm deployed *Infamous Chisel*, an Android malware for targeting rugged tablets used by Ukrainian troops, turning them into mobile surveillance platforms. Civilian IoT, including smart cameras in Kyiv, has been leveraged to monitor strategic areas.[89] Hacktivist fronts, like KillNet, used IoT-powered botnets for DDoS attacks against Western and Ukrainian targets, further blurring the line between criminal and state-linked operations.[90] Analysts warn of a growing convergence, as ransomware gangs piggyback on IoT botnets to hit industrial systems under the guise of financial motives. This mirrors the trends seen in other authoritarian states and confirms IoT is a key domain in Russia's evolving cyber warfare strategy.

Critical Civic Technology and Civilian Systems

Since 2022, the Russian cyber campaigns have increasingly targeted critical civic technologies: systems supporting public safety, governance, and societal infrastructure. It includes attacks on local governments, healthcare providers, public broadcasting, and smart city platforms. Proxy groups, like KillNet, launched DDoS attacks on hospitals across more than 25 U.S. states in early 2023 and periodically disrupted European civic systems.[91] While the functional damage was limited, the attacks served to intimidate and signal of their reach. Officials caution that such activity may precede deeper intrusions, as was seen when Russian-speaking ransomware groups, like Black Basta, targeted Western utilities and municipal networks for both financial gain and potential espionage.

In Ukraine, Russian actors were persistently striking civilian government and media systems to erode morale. Dozens of city and state websites were defaced or disabled bearing pro-Russian messages. In July 2022, hackers hijacked Ukrainian radio to falsely report President Zelenskyy's critical illness in a psychological operation

[88] https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers.pdf

[89] https://www.cisa.gov/news-events/analysis-reports/ar23-243a

[90] https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

[91] https://therecord.media/ddos-hospitals-cisa-killnet-limited-effects

that was quickly exposed but stood emblematic of civic tech weaponization.[92] Russia also was triggering false air-raid sirens through hacked emergency alert systems and continues to probe smart infrastructure, like transit, traffic control, and election platforms.[93] While no major attack on NATO municipal systems had occurred, officials remain on alert in case of a potential escalation.

To sum up, Russia's cyber strategy now extends far beyond military networks, targeting the full spectrum of technologies that underpin modern society. The expansive, integrated Russian approach blurs the boundary between civilian and combatant systems, reshaping global cyber conflict and forcing defenders to adopt holistic protection strategies across civic, critical, and emerging technologies.

6.4. Lessons from High-Profile Campaigns: Case Studies Ranging 2023–2025

Russian offensive cyber operations expanded in scale and improved in coordination, cyber efforts being increasingly aligned with military and strategic goals, between 2022 and 2025. While core tactics remained consistent, threat actors refined their techniques adopting new technologies like cloud services and AI-enabled tools and employed more advanced tradecraft to bypass the evolving defenses. The 2023–2025 period featured a series of high-profile campaigns by the Russian state and proxy actors, each reflecting shifts in tactics, targeting, or technical sophistication. Below is a summary of key case studies and the operational lessons drawn from each.

Hybrid Warfare – Coordinated Cyber, Kinetic, and Influence Attacks (2022–2023): In Ukraine, Russia blended cyberattacks with missile strikes and disinformation to maximize disruption. Late 2022 cyberattacks on the energy grid often preceded bombardments, while propaganda blamed Ukraine for resulting outages.[94] This pattern repeated in cities like Lviv in May 2022. Over time, targeting expanded to civilian infrastructure, reinforcing the Russian use of cyber as a force multiplier –merging digital, physical, and psychological attacks – and highlighting the need for integrated, rapid-response defenses.

Ghostwriter Influence Operations in Poland (2023): In April 2023, the Ghostwriter campaign, linked to UNC1151, targeted Poland with disinformation falsely claiming there was a secret conscription to Ukraine's advantage. Messages spread via SMS, email, and Telegram aimed to spark unrest and erode NATO support. Polish authorities swiftly attributed the attack and debunked the claims limiting the impact. The incident underscored two key points: cyber tools are increasingly used to amplify influence operations, and a rapid, transparent attribution is essential for neutralizing such threats.[95]

Gamaredon's Evolving Espionage Tactics (2023–2025): By 2025, the FSB-linked Gamaredon group has transformed from a noisy phishing actor into a more agile and technically capable threat. It adopted tools like Telegram channels, Cloudflare Tunnels, HTML smuggling, and geofenced payloads for stealthy C2 operations. In 2023, it attempted a phishing attack on Latvia's defense ministry.[96] By 2025, it has exploited a 0-day LNK vulnerability (ZDI-CAN-25373), using trusted Windows tools (LOLbins) to deliver oversized malicious shortcut files.[97] With faster operations (exfiltrating data within 30–50 minutes) and expanded targeting of officials' personal accounts and home devices, Gamaredon illustrated how even lower-tier actors can rapidly evolve (see Reference 2). The lesson here is to be aware of persistent threats adapting quickly, and requiring defenders to remain equally agile.

[92] https://cyberscoop.com/hackers-infiltrate-ukrainian-radio-network-broadcast-fake-message-about-zelenskys-health/
[93] https://www.bleepingcomputer.com/news/security/russian-hackers-breach-orgs-to-track-aid-routes-to-ukraine/
[94] www.wired.com/story/russia-cyberwar-ukraine-target-civilians
[95] https://therecord.media/ghostwriter-belarus-hacking-group-targets-poland-disinformation
[96] https://www.cybersecurityintelligence.com/blog/latvias-defence-ministry-targeted--6765.html
[97] https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zero-day-exploit.html

APT28 (Fancy Bear) Exploiting Network Infrastructure (2023): In 2023, the GRU-linked APT28 shifted its focus to targeting network hardware for persistent access. A joint US-UK advisory exposed exploitation of a long-standing Cisco SNMP vulnerability (CVE-2017-6742) in order to deploy custom malware (Jaguar Tooth) on unpatched routers.[98] The campaign, active since at least 2021, impacted routers in Europe, the U.S., and around 250 Ukrainian targets. This strategy enabled stealthy data interception beyond traditional endpoint defenses. The key takeaway is that network edge and IoT infrastructure must be secured alongside IT systems.

NOBELIUM (APT29) Phishing via Microsoft Teams (2023): In mid-2023, APT29 (Midnight Blizzard) exploited Microsoft Teams to bypass MFA protections.[99] Using compromised Microsoft 365 accounts the group posed as IT support, targeting employees at about 40 organizations. Victims were tricked into accepting malicious MFA prompts or clicking phishing links. The campaign, aligned with SVR espionage goals, targeted government agencies, NGOs, and media outlets. The case highlights the risk of trusted collaboration tools being weaponized and the need for increased user training and monitoring beyond email.

Turla's Snake Malware Disrupted (2023): In a major 2023 operation, the FBI and international partners dismantled Turla's long-standing Snake malware platform. Snake, a covert FSB tool used against NATO and government networks for years, was known for its stealth and resilience.[100] Operation MEDUSA remotely disabled Snake across infected systems, forcing Russia to rethink its infrastructure. The case demonstrated the power of a coordinated cyber defense in disrupting even elite nation-state tools.

Pro-Russian Hacktivist DDoS Campaigns (2023–2024): Kremlin-aligned hacktivist groups, like KillNet and NoName057(16), launched ongoing DDoS attacks on government, media, and healthcare targets in pro-Ukraine countries. On January 28, 2023, KillNet launched a coordinated DDoS campaign targeting more than 90 U.S. healthcare organizations across 48 states, with over half being hospitals, causing service outages ranging from hours to days.[101] Though unsophisticated, these attacks had outsized media impact and strained resources. Increasingly crowdsourced and deniable, they serve as low-cost harassment tools. The lesson here is that even basic DDoS campaigns can have strategic effects, highlighting that resilience and public communication are essential.

From Destructive Attacks to Stealthy Intrusions (2023–2025): A defining trend of the Russian cyber strategy was the shift from loud, destructive attacks to stealthy, long-term intrusions. Early in the war, wipers like Industroyer2 and HermeticWiper were causing visible damage. But by 2023–2024, Russia had already increasingly favored low-and-slow tactics, emphasizing supply-chain compromises and persistent access. The 2025 PathWiper attack, for example, struck only after extensive reconnaissance was done.[102] Ukraine also reported a growing use of upstream vendor compromises over direct assaults. The trend reflects a strategic pivot toward covert infiltration and highlights the importance of sustained defensive vigilance, especially across supply chains.

[98] https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jaguar-tooth/NCSC-MAR-Jaguar-Tooth.pdf

[99] https://www.hhs.gov/sites/default/files/new-midnight-blizzard-campaign-analyst-note-tlpclear.pdf

[100] https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled

[101] https://www.hipaajournal.com/killnet-hacktivist-group-continues-to-target-healthcare-organizations

[102] https://industrialcyber.co/ransomware/pathwiper-malware-targets-ukrainian-critical-infrastructure-in-russia-linked-apt-attack-using-legitimate-admin-tools

Expansion into NATO Territory (2022–2025): The reach of the Russian cyber operations started stretching beyond Ukraine into NATO states. APT28 carried out espionage against diplomatic, defense, and logistics entities, compromising routers and launching phishing tied to military aid.[103] Simultaneously, groups like NoName057(16) and KillNet disrupted NATO government and transport systems, especially during key summits or aid milestones, aiming to divide Allies and apply pressure on Kyiv's supporters.[104]

Taken together, the campaigns show how Russian cyber actors, state-backed and proxy, have evolved into adopting more advanced tactics, integrating cyber with kinetic and influence operations, and broadening their target scope. The clear lesson for defenders is to anticipate both overt and covert threats, secure infrastructure across all domains, and prepare for hybrid operations that blend disruption, espionage and psychological impact. Studying the Russian cyber operations is essential for building resilience against Russia's full-spectrum cyber strategy.

[103] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

[104] https://apnews.com/article/nato-summit-cybersecurity-hack-russia-netherlands-fa97bbf8797a51c2885d47f5f83691be

7. Comparative Analysis: 2022 vs. 2025

7.1. Tactical Evolution

Russian cyber threat actors have markedly refined their tactics, techniques, and procedures (TTPs) over 2022–2025, adapting to the evolving conflict in Ukraine and improvements in defensive measures. While their core objectives (espionage, disruption, and influence) remained consistent, execution of cyber operations grew more sophisticated and diverse. State-sponsored groups, including APT28 (Fancy Bear), APT29 (Cozy Bear), Turla, Gamaredon, and Sandworm, as well as proxy actors, like UAC-0050, and hacktivist collectives, such as NoName057(16) – all demonstrated a significant tactical evolution. Next section compares their tactics over time, with a focus on Ukraine-targeted operations and notable global incidents that exemplify innovation.

Key Shifts in Tactics: 2022 vs 2025 Overview

The table below highlights how key attack components evolved between 2022 and 2025 across different Russian threat actors:

Aspect	Typical Tactics in 2022	Evolved Tactics by 2025
Initial Access & Phishing	▪ Heavy use of spear-phishing emails with malicious Office documents (macros or exploits). ▪ War-themed lures exploiting fears (e.g. APT28's 2022 "Nuclear Terrorism" document using the Follina exploit for one-click compromise). ▪ Hacktivists relied on mass phishing and simple credential theft for account compromises.	▪ Multi-vector phishing leveraging cloud services and MFA fatigue techniques. For example, APT29 had targeted Microsoft 365 users via Teams chat messages to trick users into approving MFA prompts by 2023. ▪ HTML smuggling and one-click exploits replaced macros; threat actors weaponized 0-days (e.g. Outlook and Web vulnerabilities) for initial access. ▪ AI-driven content creation began enhancing phishing realism (using LLMs to craft convincing lures).
Malware & Payloads	▪ Deployment of well-known malware families and wipers. Sandworm launched destructive wipers (e.g. *HermeticWiper, CaddyWiper*) during the invasion onset. ▪ Predominantly Windows-focused custom implants (e.g. Turla's Snake backdoor) and basic Trojans. ▪ Limited use of mobile or cloud-specific malware.	▪ Introduction of modular, fileless malware and multi-stage payloads to evade detection. APT28 diversified into router malware and multi-stage backdoors, encrypting C2 traffic and mimicking benign processes. ▪ Custom malware targeting cloud and identity systems emerged. APT29 stealthily backdoored identity platforms (e.g. deploying *MagicWeb* malware in AD FS to maintain cloud access). ▪ Broader platform reach: use of mobile malware and cross-platform tools (e.g. Gamaredon's Android spyware in Central Asia) and malware for abusing browser APIs and Office add-ins by 2025.

Aspect	Typical Tactics in 2022	Evolved Tactics by 2025
C2 Infrastructure	▪ Reliance on self-owned or static infrastructure (compromised servers,.ru domains, bulletproof hosts). Frequent manual rotation of IPs/ domains to avoid static detection. ▪ Some use of simple techniques, like DNS tunneling and open web storage, for drop sites.	▪ Widespread abuse of legitimate cloud services and "hybrid" infrastructure. Threat groups leveraged platforms like Telegram, OneDrive, Google Drive, Cloudflare and even other APTs' servers for C2. In 2023 Gamaredon (FSB) started using multi-stage Telegram-based C2 channels that deliver payloads only to targets with Ukrainian IPs. ▪ Use of fast-flux DNS, geo-fenced C2, and stealthy channels (e.g. DNS-over-HTTPS, community forums, API traffic) became common. ▪ Compromised network devices (routers, IoT) are now integrated into C2 meshes, serving as proxies to mask attribution.
Lateral Movement & Evasion	▪ Threat actors utilized standard post-exploitation toolkits (Mimikatz for credential theft, PsExec/RDP for lateral movement) and living-off–the-land to some extent. ▪ Basic obfuscation and DLL hijacking were used but many of the attacks (esp. 2022 wipers) were noisy and detected quickly.	▪ Living-off-the-land techniques became pervasive: APT28 and others now routinely execute malicious code via legitimate binaries (PowerShell, WMI, MSHTA) to blend in. ▪ Enhanced persistence: use of stolen credentials and OTP tokens to maintain cloud access (APT29), and deployment of commercially available remote admin tools (RMS, AnyDesk) by groups like UAC-0050 to maintain stealth on victim networks. ▪ Sophisticated defense evasion: code-signing malware, geolocation checks (payload only executed on intended network), multi-stage loaders that defeat sandbox analysis, and backdooring software updates. By 2025, some campaigns have even mimicked user behavior within victim clouds (creating fake accounts and authentic sessions) to avoid anomaly detection.
Targeting & Objectives	▪ Ukraine was the focal point in early 2022: destructive attacks on government networks, critical infrastructure, and media to support kinetic operations. Espionage prioritized military and government intel. ▪ Global targets were secondary but included NATO governments and organizations supporting Ukraine (e.g. APT28 attacks on European government servers, some spillover like the Viasat satellite sabotage in Feb 2022). ▪ Hacktivist and criminal groups launched opportunistic attacks (DDoS, defacements), largely to harass Ukraine and its allies, with propaganda goals.	▪ Broadened scope: State-backed groups expanded target lists to Ukraine's partner countries and international bodies. By 2023, Turla and APT28 shifted heavily towards NATO and European networks aiding Ukraine. Simultaneously, they continued global espionage (e.g. APT29 persistently targeting Western diplomats and organizations for strategic intelligence). ▪ Integrated objectives: Cyber operations were increasingly conducted in support of influence campaigns. Stolen data was leaked or used to fuel disinformation, blurring lines between hacking and information warfare. Hacktivist attacks (NoName057(16) DDoS barrages, KillNet campaigns) were synchronized with Russian narratives, aiming to erode foreign support for Ukraine. ▪ Financial and disruptive motives grew among proxy actors. UAC-0050, for instance, added massive financial phishing campaigns and ransomware-like extortion to its repertoire post-2022. Some hacktivist units even pursued profit, as seen in groups like KillNet reorganizing to accept "commercial" attack contracts in 2024.

Table 1. A Highlight of Evolving Key Attack Components (2022–2025)

Heatmap of Russian Offensive Cyber Operations 2022–2025

TTP \ Year	2022	2023	2024	2025
DDoS Attacks	🔴	🔴	🔴	🔴
Phishing & Spear-Phishing	🔴	🔴	🔴	🔴
Credential Theft & Abuse	🔴	🔴	🔴	🔴
Exploitation of Public-Facing Applications	🔴	🔴	🟡	🟡
Use of Wiper Malware	🔴	🟡	⚪	⚪
Living-off-the-Land (LotL) Techniques	🟡	🔴	🔴	🔴
Cloud Infrastructure & OAuth Abuse	⚪	🔴	🔴	🔴
Polymorphic & Fileless Malware	⚪	🟡	🔴	🔴
Remote Access Trojans (RATs)	🟡	🔴	🔴	🔴
Supply Chain Intrusions	⚪	⚪	🔴	🟡
Zero-Day Exploitation	🟡	🔴	🔴	🔴
Use of AI in Malware Development	⚪	⚪	🟡	🔴
Fast-Flux DNS & Evasive C2 Infrastructure	⚪	🟡	🔴	🔴
Hack-and-Leak Operations	🟡	🔴	🟡	🟡
Psychological Operations & Disinformation	🔴	🔴	🟡	🟡
Mobile & IoT Malvare	🟡	🔴	🟡	🔴
Satellite or Out-of-Band C2 Channels	🟡	🔴	🟡	🟡
Use of Proxy Actors & Hacktivist DDoS Campaigns	🟡	🔴	🔴	🔴

🔴 High activity / frequent use; 🟡 Emerging or moderate use; ⚪ Not observed / not prominent

Table 2. Heatmap of Russian Offensive Cyber Operations 2022–2025

State APT Adaptation: Russia's top state-backed threat groups have continually refined their tactics to enhance impact and stealth. APT28 (GRU) intensified operations against Ukraine and NATO, combining war-themed phishing, such as the "Nuclear Terrorism" lure in 2022 exploiting the Follina zero-day, with living-off-the-land techniques to evade detection. By 2023–2024, the group had shifted beyond typical malware, compromising routers like Mikrotik and Cisco for covert proxies and phishing infrastructure while enhancing implants with encrypted communications and stealth modules.

Meanwhile, APT29 (SVR) pivoted toward cloud-centric espionage. Traditionally focused on on-premises targets, it began exploiting cloud services and identity platforms by 2022, abusing trusted supply chains

and federated authentication. The group embedded persistent backdoors in Microsoft identity systems (e.g., FoggyWeb, MagicWeb) to silently access Azure AD tenants. In 2023, dubbed Midnight Blizzard, APT29 launched a novel campaign via Microsoft Teams, using social engineering to bypass MFA and steal session tokens. These developments reflect a strategic shift: Russia's premier cyber units now blend technical exploits with creative targeting of cloud and SaaS environments to maintain long-term access.

By 2025, Gamaredon (FSB Centre 18) has evolved into a more adaptive and persistent threat actor. While it initially relied on basic phishing and PowerShell scripts in 2022, the group later integrated Cloudflare Tunnels, Telegram bots, and Living-off-the-Land Binaries for stealthier operations. It shifted toward fileless malware delivery and exploited zero-day vulnerabilities, like the Windows LNK flaw, to deploy tools such as Remcos. These changes reflect Gamaredon's growing technical maturity and its entrenched role in supporting Russian espionage efforts against Ukraine.

Russia's Turla and Sandworm groups demonstrated notable tactical evolution between 2022 and 2024. Turla, known for stealthy FSB-linked espionage, had shifted from its traditional toolkit, like the Snake rootkit and Carbon backdoors, to more covert, fileless malware by 2023. It also began hijacking infrastructure from other threat actors, including Iran's OilRig, to obscure attribution through false-flag operations, complicating detection and response.

Sandworm, the GRU's destructive cyber arm, adapted its tactics to wartime conditions. In early 2022, it launched high-impact operations, like the attempted Industroyer2 attack on Ukraine's power grid, and multiple wiper deployments. As the war progressed, Sandworm transitioned to a more sustainable sabotage tempo. By late 2022 and into 2023, it had deployed new tools, like SwiftSlicer, a Go-based wiper spread via Active Directory group policies, and disguised other destructive malware as ransomware (e.g., "RansomBoggs") to create plausible deniability. In 2024, the group escalated its hybrid approach, combining IT compromise, OT disruption, and ICS-specific payloads in attacks on Ukraine's energy sector. These shifts reflect a broader Russian strategy: integrating cyber capabilities into military and psychological campaigns for sustained, multi-domain impact.

Proxy Actors and Hacktivists: Beyond formal APTs, Russia has increasingly leveraged cybercriminal and hacktivist groups as force multipliers. UAC-0050 is one of the prominent examples, a threat group tracked by CERT-UA that has become highly active after 2022. Initially focused on government espionage, the group expanded rapidly following the invasion, adopting a volume-based strategy centered on commodity malware and mass phishing. UAC-0050 impersonated Ukrainian government agencies to distribute Remote Access Trojans (e.g., Remcos, Quasar) and infostealers, like Meduza and RedLine, through staged downloaders and decoy documents. By 2024, it had incorporated legitimate remote administration tools, such as Remote Utilities, LiteManager, Netsupport, and AnyDesk, to maintain persistence and move laterally while blending into normal network traffic. Unlike stealth-focused APTs, UAC-0050's broad, pragmatic approach enabled it to cast a wide net – reaching hundreds of targets, including private sector and financial entities typically outside the scope of state operations.

Pro-Russian Hacktivists and Cyber Guerrilla Tactics: Alongside formal APTs, pro-Russian hacktivist groups, like NoName057(16), KillNet and Anonymous Russia, added a disruptive cyber guerrilla element starting early 2022. These groups conducted widespread DDoS attacks and website defacements targeting Ukraine and its allies. Over time, they became more organized and capable: NoName057(16), for example, developed its own DDoS toolkit, *DDOSIA*, enabling crowd-sourced attacks coordinated via Telegram. In 2023, during the #OpIndia campaign, they targeted over 2,000 websites in collaboration with other actors. By 2024, their scope had expanded to include government, financial, and election-related websites across Europe and North America.

Though their tools remained basic, these groups improved in scale and targeting, leveraging botnets, rented infrastructure, and politically timed campaigns to amplify impact. Some blurred the line between activism and cybercrime, issuing ransom demands, while others appeared to function as fronts for state actors – such as the People's Cyber Army, reportedly linked to APT28. By 2025, this convergence of hacktivist, criminal, and state-aligned operations reflects a broader trend: fusion of proxy cyber actors into Russia's strategic cyber apparatus.

Evolution of Objectives and Technology: Between 2022 and 2025, Russian cyber operations shifted from immediate disruption to longer-term strategic goals. During the initial invasion, attacks focused on rapid impact using wipers, DDoS, and sabotage to paralyze Ukrainian communications and services in sync with military actions. As Ukraine's cyber defenses improved, Russian efforts pivoted back toward espionage and persistent access. Groups like APT28 and Gamaredon increasingly targeted Ukrainian government, military, and infrastructure networks to monitor battlefield communications, logistics, and foreign support. Influence operations also grew more sophisticated, with stolen data leaked or altered to spread distrust, and DDoS or defacement attacks timed for psychological impact results – such as disrupting NATO websites during key summits or hitting foreign banks to discourage support for Ukraine. By 2025, Russian cyber campaigns have showcased hybrid warfare: a fusion of hacking, propaganda, and military pressure aimed at achieving broader strategic objectives.

Adoption of Emerging Technologies: Russian threat actors have increasingly integrated emerging technologies into their operations, enhancing both agility and stealth. Cloud infrastructure is now routinely exploited – APT29, for instance, have abused Azure AD trust relationships, while various groups have leveraged platforms like OneDrive, Cloudflare, and Telegram for covert data exfiltration and command-and-control. There is also growing evidence of experimentation with Artificial Intelligence (AI). Intelligence reports suggest Russian operators have used Large Language Models to craft more convincing phishing content and analyze stolen data at scale. The FBI has further warned that cybercriminals, including Eastern European actors, are using AI for highly targeted phishing and deepfake audio/video impersonation, tools that state-aligned groups could readily adopt for advanced social engineering and disinformation. By 2025, the integration of AI and cloud-based tactics reflects a marked evolution in Russia's cyber arsenal. Overall, the 2022–2025 period has transformed Moscow's approach model into a more sophisticated blend combining traditional cyber capabilities with new technologies and aligning state, criminal, and proxy efforts to serve its strategic objectives.

7.2. Operational Changes

Between 2022 and 2025, Russian state-aligned cyber operations underwent significant transformation in structure, tempo, and coordination. Key actors, including APT28 (Fancy Bear), APT29 (Cozy Bear), Turla, Sandworm, and Gamaredon, adapted their tactics to meet shifting battlefield demands, while pro-Russian hacktivist and criminal proxies, like NoName057(16) and UAC-0050, became increasingly embedded within a broader, state-aligned cyber ecosystem. What began as a fragmented activity in 2022, has evolved into a more cohesive, multi-layered campaign by 2025. The next section compares cyber operations conducted across the two periods, with an emphasis on shifts in operational coordination, campaign tempo, integration with military and influence efforts, shared infrastructure, and targeting strategies.

Evolving Operational Structure and Coordination

In 2022, the Russian cyber operations were largely siloed across agencies like the GRU, FSB, and SVR, alongside a patchwork of proxy actors. As the war progressed, a more integrated command structure emerged. By 2025, cyber campaigns have shown clear signs of a tighter coordination, with Russia's intelligence services outsourcing tasks to private contractors, cybercriminal gangs, and hacktivist collectives. This approach created a sprawling, hybrid ecosystem that blurs the line between state and non-state actors while enabling plausible deniability. For example, groups like CyberArmyofRussia_Reborn have coordinated with the GRU's Sandworm unit (APT44), and ransomware crews, such as Conti, have cooperated with the Russian intelligence, motivated by protection or patriotic alignment. This decentralized model has enhanced operational flexibility and reach but introduced complexity and reduced centralized control, reflecting a maturing – even if messy – hybrid warfare architecture.

Tightening Coordination Across Threat Actors: In early 2022, pro-Russian hacktivist groups, like NoName057(16), emerged in a loosely organized, ad-hoc fashion, launching DDoS attacks on Ukrainian targets. Over time, these proxy actors became increasingly aligned with state objectives. The Russian military intelligence began using hacktivist personas as fronts – most notably, Sandworm (GRU) operated through fake collectives, like Xaknet, to claim credit for cyberattacks and leaks, that way obscuring a direct state involvement. In one case, Xaknet took responsibility for disrupting Ukrainian government registries and leaking data, though evidence later linked the operation to Sandworm. By 2023–2024, such coordination had evolved into a deliberate strategy, merging influence operations with technical intrusions. Russian authorities also encouraged alliances among hacktivist groups; by 2024, collectives like NoName057(16) were conducting joint campaigns with others, such as the #OpIndia DDoS attacks during the 2023 G20 Summit. This marked a shift from an isolated, opportunistic activity to coordinated, coalition-based operations supporting broader strategic goals.

Changes in Tempo and Campaign Sustenance

From 2022 to 2025, the Russian cyber operations shifted from short bursts of disruption to continuous, high-tempo campaigns. At the onset, the war saw a wave of intense attacks – such as wipers, like HermeticWiper, and the Viasat satellite outage – launched in February 2022 in support of kinetic strikes. However, after the earliest offensives, state actors transitioned to sustained espionage and longer-term access. By 2025, groups like Sandworm have evolved their modus operandi from brute-force disruptions to multi-phase intrusions marked by long dwell times, staged payloads, and ongoing intelligence collection.

Campaign frequency and duration increased across all major actors. CERT-UA reported that UAC-0050 had become one of the top three most active threat groups by 2024, with 99 confirmed incidents that year alone. Gamaredon adopted a high-volume, low-success-rate approach, continuously bombarding Ukrainian targets with phishing and malware in the hope of statistical gains. This marked a shift from isolated pre-war operations to overlapping, near-constant campaigns. Even APT29, known for stealth and restraint, had accelerated its activity expanding operations against NATO and European targets, as well as steadily upgrading its toolkit with cloud-focused techniques to sustain persistent access – resulting in an offensive cyber posture defined by scale, endurance, and operational persistence.

Integration with Military and Influence Operations

Between 2022 and 2025, Russian cyber campaigns became increasingly integrated with conventional military actions and psychological warfare. Early coordination was evident in high-impact incidents, such as Sandworm's April 2022 deployment of Industroyer2 against Ukraine's power grid, timed with missile and air strikes to amplify disruption. It marked a new level of joint operational planning between cyber and kinetic forces. The pattern continued in later years; in 2024, Sandworm combined cyber intrusions using Active Directory compromises and custom malware with presumed physical operations against Ukraine's energy infrastructure. By 2025, this integration has extended beyond Ukraine towards Western support networks. The 26165 (APT28) GRU unit shifted its focus to NATO transportation and logistics systems targeting aid delivery pipelines. Joint advisories reported that APT28 had expanded efforts to infiltrate logistics firms, technology vendors, and even border surveillance systems, to track arms shipments. The shift reflects a strategic pivot toward using cyber capabilities to support battlefield objectives by targeting military supply chain and intelligence infrastructure.

From 2022 to 2025, the Russian cyber actors increasingly synchronized their operations with information-psychological campaigns. A notable early example was the March 2022 hack of Ukraine 24 TV, in which the attackers injected into the broadcast a deepfake video of President Zelenskyy urging Ukrainian troops to surrender. The video, amplified through defaced news tickers and social media, aimed to undermine the morale and sow confusion in a clear fusion of cyber intrusion and disinformation. This tactic became a recurring element in Russia's strategy. By 2023–2024, leaks perpetrated by APT groups and hacktivist fronts had been routinely used to support Kremlin narratives – with stolen emails and documents released to discredit the Ukrainian leadership or sway foreign opinion. Sandworm-linked personas, in particular, played a central role in these operations. Over time, the integration of cyberattacks and influence campaigns became more structured, reflecting Russia's indoctrinated treatment of cyber and information operations as inseparable components of modern conflict. By 2025 such convergence has become a defining feature of Russia's digital warfare playbook.

Joint Infrastructure and Resource Shifts

By 2025, Russian cyber operations increasingly feature shared infrastructure and tools across state and proxy actors – marking a shift from the more siloed approach seen in 2022. Early overlaps, such as GRU malware delivered via criminal botnets, were relatively limited. But over time, actors began routinely leveraging each other's infrastructure and third-party assets to enhance reach and complicate attribution. Turla (FSB), for example, was tracked hijacking servers used by Iranian and criminal groups, like OilRig and Amadey, to mask its activity by 2024. This practice of piggybacking illustrates both increased coordination and pragmatic resource sharing.

Common platforms also became widely used for command-and-control. Multiple groups, including Gamaredon and APT29, converged on using cloud services (e.g., Cloudflare, Telegram, OneDrive) and fast-flux DNS to evade detection and blend with legitimate traffic. Adoption of public infrastructure, API-based C2 channels and shared tradecraft enabled faster, more flexible operations. State and proxy actors alike increasingly relied on off-the-shelf RATs (like Remcos) and open-source loaders, with groups such as UAC-0050 using the tool for rapid deployment. The discussed convergence reflects a shift toward a modular, plug-and-play approach to cyber operations – streamlining execution while obscuring attribution and reducing operational overhead.

Operational Aspect	2022 (Invasion Onset)	2025 (Ongoing War)
Coordination & Structure	Agencies (FSB/GRU/SVR) ran largely separate cyber ops; ad-hoc use of proxy hackers. Little formal integration between state and criminal actors.	Centralized strategy with integrated state–proxy ecosystem. Intelligence units regularly task or collaborate with hacktivist and eCrime groups under a unified cyber campaign.
Operational Tempo	Intense bursts of attacks (e.g. wiper waves) around Feb 2022, followed by pauses. Campaigns often one-off or short-term.	Sustained high-tempo operations year-round. Multiple concurrent campaigns (espionage, DDoS, influence) maintained continuously, reflecting a protracted cyber conflict.
Target Prioritization	Focused on Ukrainian government networks, critical infrastructure, and immediate battlefield comms. Limited initial focus on Western targets beyond Ukraine.	Broadened target scope: continued focus on Ukraine's military, government, and energy sectors, plus expanded operations against NATO logistics, European governments, and global strategic targets supporting Ukraine. Priorities adjusted to war needs (e.g. arms supply lines, allied public opinion).
Military Integration	Nascent coordination; a few cases of synchronized cyber strikes with military action (e.g. energy grid attack timed with kinetic strikes). Not yet routine.	Integrated cyber-kinetic planning: cyber operations commonly support or precede military moves. Examples include sustained hacking of air/rail logistics to assist targeting of aid deliveries. Cyber units function as an arm of battlefield intelligence and sabotage.
PsyOps Integration	Opportunistic use of cyber for propaganda (e.g. defacements, one-time hacks to spread fake news, like the Zelenskyy deepfake incident).	Cyber-enabled influence ops are a regular tactic. Hack-and-leak operations, data dumps, and DDoS disruptions are closely timed with disinformation narratives, aimed at eroding enemy morale and shaping international perceptions.
Infrastructure & Tools	Groups largely used distinct infrastructure and custom malware (e.g. APT28's own servers, Sandworm's specialized wipers). Limited tool sharing; some basic reuse of known malware.	Joint and outsourced infrastructure usage is common. Actors leverage third-party botnets, cloud services, and even each other's malware/toolsets. Greater adoption of shared tactics (Cloudflare Tunnels, Telegram C2, common RATs) across different groups.
Resource Allocation	Rapid, *"surge"* deployment of cyber weapons to achieve shock effect (e.g. mass phishing + wipers to soften defenses). Relatively short campaign planning cycle.	Planned, resource-efficient campaigns with iterative cycles. Emphasis on persistence and maximizing impact per asset: long-term infiltrations (APT29, Turla) and repeated mass phishing waves (Gamaredon, UAC-0050) show more calculated use of manpower and malware over time.

Table 3. Operational Evolution of Russian Cyber Campaigns (2022–2025)

Illustrative Campaign Shifts

Concrete examples highlight the evolution in the Russian cyber operations between 2022 and 2025. Sandworm's trajectory is especially telling: in 2022, it operated as a destructive saboteur, deploying wipers and Industroyer2 to cause immediate damage without maintaining access. By 2023–2024, the same GRU unit had shifted to more sophisticated, blended campaigns. In one 2024 operation, Sandworm infiltrated Ukraine's energy grid, established covert backdoors via Active Directory compromise, and delayed activation of destructive payloads, which signals a move toward multi-phase operations that support both espionage and disruption depending on strategic needs.

APT28 developed a similar pattern. Initially focused on traditional espionage against Ukrainian and NATO entities, the group broadened its role after the early Russian military setbacks. By late 2022, APT28 was actively targeting Western logistics networks and municipal surveillance systems to support battlefield planning and arms interdiction. This operational expansion underscores a strategic shift from isolated intelligence gathering to integrated support for military campaigns, reflecting Russia's increasingly coordinated and adaptable approach to cyber warfare.

The trajectories of NoName057(16) and UAC-0050 demonstrate the evolution of proxy actors from loosely organized or criminal origins into aligned instruments in the Russian state cyber strategy. In 2022, NoName057(16) operated as a spontaneous hacktivist group, launching crude DDoS attacks to deface or disrupt Ukrainian websites. By 2023–2025, it had grown significantly in coordination and reach, executing thousands of attacks across Europe, including attempts to influence elections – such as targeting the Czech presidential candidates in 2023. Its focus increasingly mirrored Kremlin priorities, consistently hitting government and financial sites in the pro-Ukraine nations, like Poland, the Nordics, and Canada. This reflects a broader trend of the Russian hacktivist fronts acting as an "online auxiliary," sustaining constant low-level pressure on adversaries' public services.

Similarly, UAC-0050 transitioned from a financially driven phishing group into a more aggressive actor with clear military alignment. After 2022, it expanded its targeting to include Ukrainian financial institutions, government agencies, military personnel, and even engagement in psychological operations, such as bomb threat hoaxes to cause panic in the public. This shift highlights the criminal capabilities co-opted to serve broader state objectives, blending espionage, disruption, and psychological impact. Together, the cases underscore an increasing convergence of state, criminal, and hacktivist resources in Russia's hybrid cyber warfare ecosystem.

By 2025 the Russian offensive cyber operations have become better structured, faster-paced, and strategically integrated. What began as loosely coordinated, sporadic hacks, evolved into sustained campaigns closely aligned with military and influence objectives over the discussed period of time. State APTs and proxy actors progressed to operate in tandem, sharing infrastructure and tradecraft while conducting espionage, sabotage, DDoS, and disinformation, in parallel. This transformation reflects Russia's adaptation to a prolonged conflict: merging cyber, kinetic, and psychological warfare, and expanding its operational base through cybercriminal and hacktivist surrogates. The result is a more agile, resilient, and deeply embedded cyber apparatus central to Moscow's broader warfighting strategy.

7.3. Strategic Objectives

At the onset of the full-scale invasion in 2022, Russia's offensive cyber operations were tightly coupled with its military strategy, aimed at achieving a swift collapse of Ukraine's defensive capacity. The goal was to use cyberattacks as force multipliers for crippling government services, military communications and

public infrastructure in the critical hours and days surrounding the kinetic assault. This was evident in the deployment of wiper malware, such as HermeticWiper and WhisperGate, which struck Ukrainian government and financial networks on February 23–24 in coordination with the ground invasion. The Viasat KA-SAT attack, which disabled both military and civilian satellite connectivity across Ukraine and parts of Europe, further underscored Russia's intent to disable communications and command-and-control capabilities in real time. Malware, like Industroyer2, deployed against Ukraine's energy grid, and AcidRain, used against satellite modems, characterized a cyber-campaign designed to paralyze national functions and break resistance through coordinated digital and physical strikes.

However, by 2023 it had become clear that the objective were failing. Ukraine's defenses held, and Russian cyber units shifted from shock-focused sabotage to sustained disruption, influence, and pressure. Cyber operations began to target not only Ukraine but also its diplomatic and military supporters. APT28 and Sandworm reprioritized espionage and disruption campaigns targeting NATO-aligned countries, while Russian-aligned hacktivist groups launched politically-timed DDoS attacks in response to visible support for Ukraine.[105] In June 2022, folowing Lithuania's blockade on the sanctioned goods transited to Kaliningrad, the Russian actors launched widespread DDoS attacks against Lithuanian government, transport, and financial systems.[106] Later, Japan's expression of support for Ukraine and delivery of non-lethal aid prompted pro-Russian groups to launch cyberattacks against Japanese Ministries and businesses.[107] Canada faced similar retaliation after expanding military assistance and training for Ukrainian forces, with KillNet and affiliated groups disrupting Canadian government sites.[108]

These attacks, while often unsophisticated, reflected a strategic shift: from battlefield support to retaliatory pressure aimed at deterring foreign aid and punishing political decisions. Cyber operations became instruments of coercion and messaging, especially when paired with disinformation or propaganda campaigns. Defacements, fake news injections, and social media amplification campaigns often accompanied these attacks suggesting a hybrid objective: to strain public trust, destabilize foreign political environments, and raise the costs of supporting Ukraine.

By 2025, Russia's cyber objectives have evolved into a persistent, multi-front campaign – still focused on Ukraine but increasingly projecting outward to its supporters and partners. Ukrainian civilian infrastructure remained under constant digital pressure, while NATO states, EU governments, and regional neighbors were drawn into the cyber battlespace through attacks on parliaments, logistics systems, and energy firms. What began as a war-specific cyber effort transformed into a broader geopolitical pressure strategy, with Russia using cyber operations not only to influence the battlefield but to reshape the strategic environment surrounding it.

7.4. Technological Leverage

Between 2022 and 2025 the Russian cyber operations have been demonstrating increasing technological flexibility, combining legacy malware techniques with new platforms, evasion tactics, and emerging technologies. As the conflict evolved, threat actors selectively adopted technologies that enhanced speed, persistence, and operational ambiguity. This included creative use of red-team frameworks, cloud platforms, AI models, and even Internet of Things (IoT) – all integrated into a rapidly adaptable threat ecosystem.

[105] https://socradar.io/gru-backed-apt28-cyber-war-on-nato/

[106] https://www.euronews.com/next/2022/06/27/ukraine-crisis-lithuania-cyber

[107] www.darkreading.com/cyberattacks-data-breaches/russia-linked-hackers-attack-japan-govt-ports

[108] https://www.radware.com/security/threat-advisories-and-attack-reports/pro-russian-hacktivists-targeting-canadian-organizations

In early 2022 threat actors relied heavily on well-established tooling and malware families. Sandworm and APT28 used frameworks like Cobalt Strike and later Brute Ratel C4 to enable post-exploitation operations, including lateral movement, credential theft, and command execution. These commercial red-team kits, designed for penetration testing, became key enablers for stealthy intrusions when paired with custom implants or commodity loaders, such as Sliver and ShadowLoader. Russian operators routinely modified beacon profiles and encrypted communications to evade signature-based detection.

By 2023, Russian APTs had shifted toward abusing cloud infrastructure and legitimate software-as-a-service (SaaS) platforms. Groups like APT29 and Gamaredon tunneled C2 traffic through Telegram bots, Cloudflare Tunnel, hiding malware traffic within trusted services. The instrumentalization of fast-flux DNS and cloud-based dynamic C2 infrastructure allowed attackers to rotate command servers frequently, making them difficult to block or trace. These methods also leveraged the defenders' reluctance to blacklist widely used legitimate services.

In parallel, Russian groups increasingly abused Living-off-the-Land Binaries (LOLBins) – trusted system utilities, like PowerShell, WMI, and mshta.exe – to perform malicious actions without dropping detectable binaries. These fileless techniques became foundational for groups like Gamaredon and UAC-0184, especially for espionage campaigns in Ukrainian government systems. Malware was often delivered through complex loader chains involving .LNK files, HTA files, DLL sideloading, and steganographically embedded payloads (e.g., malware hidden in PNG images with unique byte markers).

In terms of destructive capability, tools like Industroyer2 and AcidRain represented Russia's evolving OT threat posture. Industroyer2 specifically targeted the IEC-104 protocol used in electrical substations to issue rogue commands and trigger blackouts. AcidRain's modular design enabled mass disruption of satellite modems in both Ukraine and Germany. The used tools emphasized Russia's focus on cross-domain attacks: hitting IT, OT, and telecommunications infrastructure in tandem with military action.

By 2024–2025, the Russian actors have begun experimenting with artificial intelligence (AI) to improve operational tempo and realism. OpenAI reported that state-linked groups, including the Russian actors, used generative tools, like ChatGPT, to debug malware, generate phishing lures, and refine payloads. In some cases, AI-assisted info-stealers were deployed against gaming communities for operations featuring credential theft, privilege escalation, and encrypted exfiltration. Although no large-scale AI-powered campaign has been attributed to Russia yet, the incidents suggest early phases of a shift toward AI-assisted cyberattack development. The Russian-aligned actors have also likely leveraged jailbroken LLM models, such as WormGPT and FraudGPT, which are trained without content restrictions. These tools that facilitate automated phishing, fake news generation, and persona development at scale are useful for both psychological operations and social engineering. Given Russia's long-standing focus on disinformation, the mentioned AI platforms may soon form a central part of cyber-influence campaigns targeting civilian populations or military morale.

Finally, the Russian APTs continued to exploit IoT and edge devices – notably routers and firewalls – to build durable, decentralized infrastructure. Cyclops Blink, Sandworm's successor to VPNFilter, was infecting WatchGuard and ASUS devices by embedding itself in the firmware. APT28 exploited old SNMP vulnerabilities in Cisco routers to install implants like Jaguar Tooth, gaining stealth access to mid-network infrastructure across NATO countries.

Altogether, the period between 2022 and 2025 shows how Russia's cyber capabilities were evolving toward greater stealth, automation, and integration. By combining traditional malware with cloud tools, physical access and emerging technologies, like AI, the Russian cyber operations have become more difficult to detect and defend against – especially in the context of modern hybrid warfare.

8. Mitigation recommendations

Strengthening the defenses against the advanced Russian cyber tactics requires a multi-layered approach. These recommendations are structured to support both civilian and critical infrastructure organizations, with an additional focus on frontline resilience.

Access Control and Credential Hygiene

Russian operations quite typically are initiated using stolen credentials obtained via phishing or reuse. Implementation of strong password policies, enforced rotation, and comprehensive multi-factor authentication (MFA) across VPNs, administrative accounts, and cloud platforms is essential. Monitoring of unusual login patterns, such as remote access or logins during off-hours, can identify compromised credentials before the damage occurs. Ukraine's experience shows early credential-based intrusions can overwhelm defenses before the traditional exploits are even used.

Detection of Native Tools and Cloud Abuse

The attackers increasingly rely on legitimate utilities and cloud services (e.g., PowerShell, WMI, Telegram, Cloudflare Tunnels) to hide malware activity in plain sight. Organizations must enhance the visibility into these tools with behavior monitoring, anomaly detection, and stronger logging controls. Public sector agencies should treat messaging platforms like cloud services – in effect, extending existing endpoint detection capabilities into the cloud. This dramatically improves detection of stealth campaigns using trusted services for control or data exfiltration.

OT and IoT Device Security

The Russian actors have demonstrated a clear intent to compromise the industrial systems via routers, firewalls, and ICS/SCADA networks. To counter this trend, agencies must deploy strict segmentation between IT, OT, and IoT networks, enforce regular firmware updates, and monitor network traffic for unusual protocol or configuration changes. These controls help prevent persistent footholds and preempt cyber-kinetic integration in sensitive industries, like energy and transportation.

Resilience Through Prepared Planning

Ukraine's challenges highlight the importance of a pre-scripted incident response plans and cross-sector collaboration. Organizations should design and practice multi-domain incident exercises that combine network defense with crisis communication, public messaging, and infrastructure continuity. Dedicated teams should include cybersecurity leads, communications experts, infrastructure operators, and emergency services to ensure cohesive responses during combined cyber and physical threats.

Countering Psychological Operations

Cyber campaigns are increasingly paired with disinformation tools (fake alerts, deepfake audio, or propaganda dumps) designed to induce chaos and distrust. Defenders need integrated response plans that coordinate technical containment with media and community outreach. Partnership with trusted messengers (e.g., civil defense, media, NGOs) can mitigate panic-driven fallouts. Ukraine's rapid public debunking of bomb scares and fake air-raid sirens underscores how timely messaging can blunt the impact of hybrid threats.

Proactive Threat Hunting and Threat Intelligence

Given the layered threat that includes hacktivist proxies, like KillNet and NoName057(16), the defenders should conduct ongoing threat hunting looking for emerging infrastructure – such as booter services, Telegram channels, or dynamic domains linked to known actor groups. A public-private intelligence-sharing is critical for identifying coordinated campaigns and improving collective detection capability.

Preparing for AI-Enhanced Threats

Early signs of AI use, especially for phishing, propaganda, and code generation, suggest a future where attacks will be faster, more targeted, and harder to parse. Organizations should begin integrating AI-enhanced defense tools able to detect deepfake content or anomalous messaging patterns. Equally important is conducting tabletop exercises that simulate AI-driven disinformation or spear-phishing scenarios, preparing both technical and human systems for next-generation threats.

9. Conclusions

9.1. Summary of Findings

Between 2022 and 2025, the Russian offensive cyber operations evolved from a short-term tactical disruption to a long-term strategic component of the hybrid warfare. At the onset of the Ukraine invasion in 2022, the cyber campaigns were tightly coordinated with kinetic operations: wipers, like HermeticWiper and CaddyWiper, were launched hours before missile strikes, and satellite communications were disabled to cripple the response capabilities. Threat groups like Sandworm, APT28, and Gamaredon executed the attacks with high frequency, speed, and intensity, aiming to rapidly destabilize Ukraine's defenses and communication networks.

As the war dragged into 2023 and beyond, the failure to swiftly defeat Ukraine prompted a strategic shift. The Russian cyber forces transitioned from immediate disruption to sustained, adaptive operations. Groups like APT29 and Turla expanded espionage activity across Europe and NATO countries, using advanced cloud-focused intrusion techniques, supply chain compromises, and stealthy malware. At the same time, actors such as Gamaredon refined access persistence techniques using cloud infrastructure, Living-off-the-Land binaries, and fast-flux DNS. Russia's approach became more about distribution, modularity, and resilience: integrating commodity malware, legitimate cloud tools, and new AI-assisted capabilities.

By 2024 and 2025, the targeting extended beyond Ukraine's borders to include the nations offering military, economic, or diplomatic support to Kyiv. Lithuania, Japan, Canada, and others were hit with DDoS campaigns or espionage operations following their public announcements of aid. This marked the widening of the conflict's cyber theater, as Russian actors combined military-aligned APTs and proxy hacktivists (e.g., KillNet, NoName057(16)) to conduct punitive operations while maintaining deniability. These groups often coordinated or followed the lead of GRU-linked actors, echoing state priorities while employing cheaper, noisier tactics.

The analyzed evolution reflects a maturing offensive ecosystem where destructive attacks, espionage, psychological operations, and AI-augmented tooling converge to support Russia's geopolitical goals. The integration of cyber operations into both military planning and retaliatory foreign policy responses demonstrates a long-term, state-backed investment in offensive cyber as a primary instrument of power projection.

9.2. Way forward

As Russia's cyber operations continue to evolve, several emerging trends are expected to shape the threat landscape beyond 2025. First, the integration of artificial intelligence into malware development, reconnaissance, and influence operations is likely to accelerate. Russian groups have already begun experimenting with AI to automate phishing, develop polymorphic code, and generate propaganda – capabilities that will likely be enhanced through domestic LLMs or custom offensive frameworks.

Second, critical infrastructure, both civilian and military, will remain a primary target. While Ukraine has borne the brunt of destructive attacks, the expansion of campaigns into NATO countries suggests that Russia will continue to use cyber means to punish or deter geopolitical adversaries. Telecommunications, energy, and satellite systems are especially at risk, as shown by the attacks on Viasat and regional power grids.

Third, the ecosystem of proxy groups, hacktivist fronts, and cybercriminal affiliates will likely grow in scale and complexity. These actors provide plausible deniability while conducting DDoS, ransomware, and hack-and-leak operations aligned with state objectives. As seen with KillNet and XakNet, such groups blur the lines between patriotism, cybercrime, and state control.

The defensive strategies must adapt accordingly. Governments and organizations should prioritize threat intelligence-sharing, cross-border coordination, and resilient infrastructure design – especially in sectors most vulnerable to espionage and sabotage. Detection mechanisms must evolve to account for fileless malware, cloud-native threats, and AI-generated content. Above all, analysts should recognize that Russia's cyber campaigns are not isolated events but persistent, state-aligned strategies designed to shape both tactical and geopolitical outcomes.

10. List of references, annexes

Gamaredon (FSB Centre 18)

Gamaredon remained one of the most active Russian cyber units targeting Ukrainian government and military networks. Between 2022 and 2025, the group has conducted sustained, large-scale phishing campaigns demonstrating a marked increase in technical sophistication. Their operational infrastructure evolved to include Cloudflare Tunnels, Cloudflare Serverless Workers, and Telegram for command-and-control communications, enabling the group to bypass conventional detection methods and maintain persistence in target environments.

Turla (FSB Centre 16)

Turla continued to specialize in long-term espionage operations against diplomatic, defense, and government institutions within NATO and affiliated states. The group employed highly advanced stealth techniques, including satellite-based communication relays and multi-stage malware frameworks. Known toolsets, such as Kazuar, ComRAT, and Snake, were deployed with precision, often through compromised third-party infrastructure to obfuscate attribution and entry vectors.

APT29 (SVR)

APT29, also known as Cozy Bear, maintained its focus on intelligence collection across diplomatic and strategic sectors in NATO countries. The group's tactics emphasized cloud infrastructure exploitation, particularly through abuse of OAuth tokens and Azure Active Directory. APT29 deployed evasive malware, such as SUNBURST and MagicWeb, leveraging the tools to compromise networks without triggering standard endpoint defenses.

APT28 and Sandworm (GRU)

APT28 continued the operations targeting military, political, and critical infrastructure sectors with advanced phishing, exploitation of zero-day vulnerabilities, and deployment of customized Remote Access Trojans. LNK file abuse and social engineering were central to many campaigns. Sandworm, operating in parallel, focused on destructive attacks aligned with the Russian kinetic military actions. The group was responsible for the 2022 Industroyer2 malware deployment against Ukraine's power grid, which coincided with missile strikes and demonstrated a coordinated cyber-physical attack capability.

Reference List:

1. **The State Service for Special Communication and Information Protection of Ukraine (SSSCIP).** Russia's *Cyber Tactics: Lessons Learned 2022.* (2023) Available at: https://nsarchive.gwu.edu/sites/default/files/documents/s9zfme-rssdn/2023-03-08-SSSCIP-Russia's-Cyber-Tactics-Lessons-Learned-2022-via-website.pdf

2. **National Security and Defense Council of Ukraine.** *Review of Cybersecurity News in Ukraine, Tendencies, and World Events Related to the First World Cyber War.* (2023). Available at: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023%28EN%29.pdf

3. **National Security and Defense Council of Ukraine.** *Review of Cybersecurity News in Ukraine, Tendencies, and World Events Related to the First World Cyber War.* (2023). Available at: https://www.rnbo.gov.ua/files/НКЦК/2023/Cyber%20digest_August_2023_EN.pdf

4. **Janne Hakala, Jazlyn Melnychuk.** *Russia's Strategy in Cyberspace.* (2021). Available at: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf



Regional Cyber Defence Centre

A Comparative Study of Russian Offensive Cyber Capabilities from 2022 to 2025