CybelAngel

Cyber Threat Landscape of the Russia-Ukraine War (Jan 2022 – Jan 2026)

Targeting, Tradecraft, Trajectories and Defensive Implications

TABLE OF CONTENTS

Date: April 28, 2026

Version: 1.0

Author:
Louis-Charles Beyeler | Pre Sales
Anne-Claire Chaugny | Cyber Operations
CybelAngel REACT | react@cybelangel.com | Research and Analysis of Cyber Threats

Classification: TLP: GREEN

KEY TAKEAWAYS

- **The volume of claimed attacks is markedly uneven between the two sides.** For example, roughly 1,650 incidents targeting Ukrainian entities were recorded between January 2025 and January 2026, compared to fewer than 600 targeting Russian entities over the same period.

- **Operations against Ukraine are driven by high-volume DDoS traffic**, which seeks to deny access to online services, **whereas attacks against Russia reflect a more deliberate effort to breach targets, exfiltrate data, and subsequently exploit or publicly expose it.**

- **Government administration is the leading target on both sides.** Beyond this, targeting patterns differ: **in Ukraine, critical infrastructure is especially exposed**, with telecoms, energy and utilities, and manufacturing among the most affected, while **Russia is more often hit in sectors of civilian daily life** such as e-commerce, education, and retail.

- The two sides also differ sharply in actor concentration. **The offensive effort against Ukraine is driven by a small number of prominent pro-Russian groups, while operations against Russia are distributed across a broader, more heterogeneous set of actors.**

- **Cyber operations extend beyond the Ukrainian front** into NATO members and other countries supporting Ukraine, with NoName057(16) being the most active cross-border actor.

Framing note

February 24, 2026 marks four years since the start of Russia's full-scale invasion of Ukraine.

While cyber operations were already an established component of Russia-Ukraine tensions prior to 2022, the transition to open interstate warfare has led to their deeper integration into military and geopolitical dynamics.

This note examines the cyber dimension of the conflict and its trajectory. It analyzes the objectives pursued, the capabilities deployed, the tradecraft and targeting of threat actors, and the observed effects on their targets as operational patterns evolve throughout a prolonged war.

Scope and methodology

Attack counts in this report aggregate both publicly claimed incidents (e.g., via Telegram) and independently verified intrusions. They should therefore be interpreted as indicators of operational patterns rather than as a measure of confirmed impact.

The qualitative analysis in this note spans the entire war, from its onset to the present. Quantitative figures, by contrast, primarily cover the January 2025 – January 2026 period and are compared with the preceding twelve months (January 2024 – January 2025) to provide a recent year-on-year baseline.

This note does not aim to provide a systematically symmetrical analysis of the two parties' actions with respect to specific attack types or modi operandi. Rather, its purpose is to highlight the distinctive characteristics, capabilities, and behaviors of each of the actors under study.

I. Threat Landscape

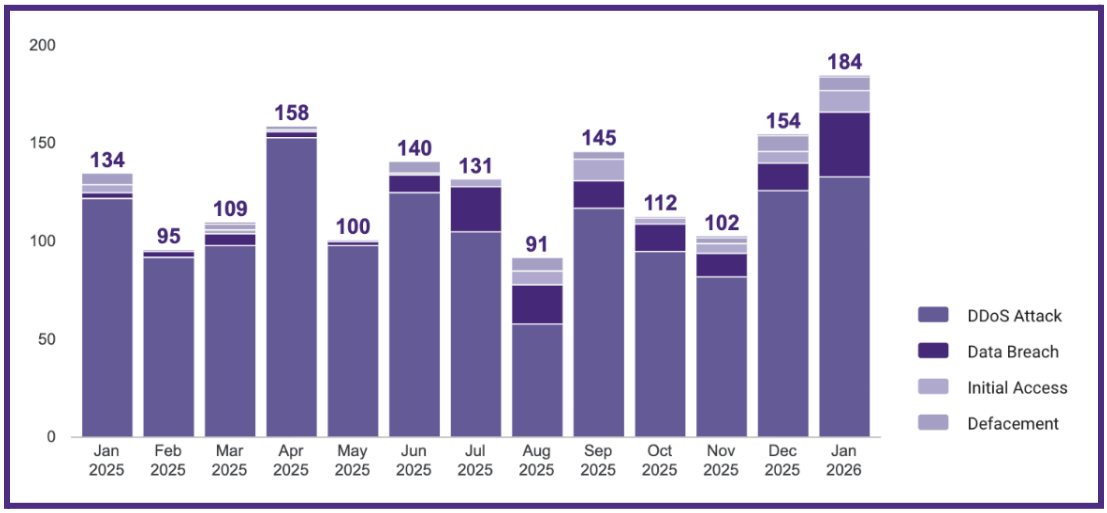
1.1 Attack Typology, Volumes and Trends

Between January 2025 and January 2026, the dataset shows a **continued asymmetry in cyber activity affecting Ukraine and Russia, both in volume and in the type of operations observed.**

Ukraine accounted for a significantly **higher number of recorded incidents**, with 1,651 incidents, compared with 575 incidents targeting Russian entities over the same period. This imbalance reflects the sustained focus of pro-Russian activity on Ukrainian targets, particularly through high-volume and in depth disruptive operations.

Attacks targeting Ukraine (January 2025 – January 2026)

Cyber activity targeting **Ukraine** is heavily dominated by **DDoS operations**, which account for approximately 84% of all recorded incidents (1,391 claims).



Distribution of Observed Cyber Activity Targeting Ukraine (Jan 2025–Jan 2026)

Activity is highly concentrated among a **small number of actors**, notably:

- NoName057(16) (919 incidents)
- OverFlame (106)
- Z-ALLIANCE (45)

Of note, **NoName057(16) alone accounts for the majority of DDoS incidents** recorded against Ukrainian targets, confirming its central role.

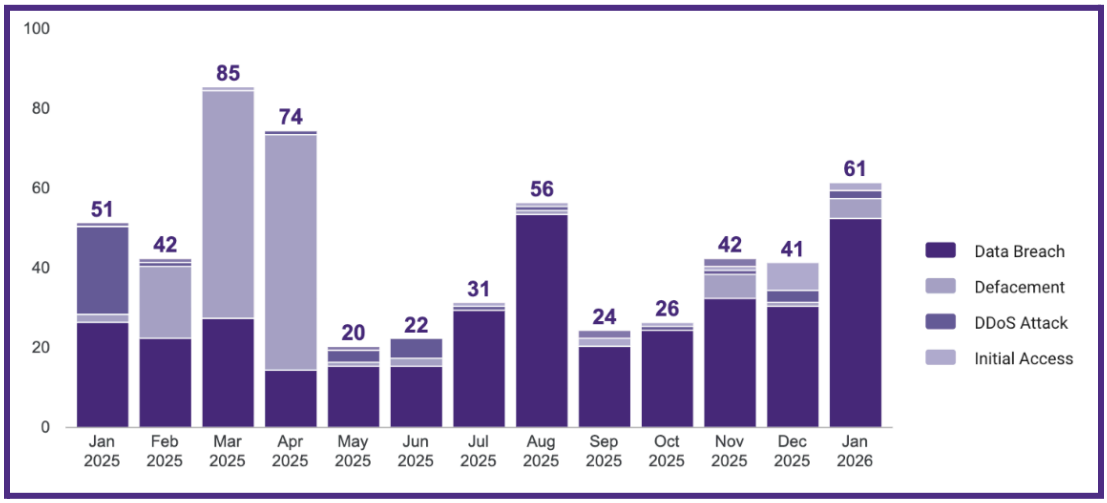
Other observed activity includes:

- **Data breach claims:** ~9% (156 incidents)
- **Initial access claims:** ~3% (57 incidents)
- **Defacement:** ~2% (47 incidents)

Although marginal in volume, **intrusion and data-compromise activity remains persistent** across the period, signaling sustained breach and exfiltration objectives behind the dominant DDoS effort.

Attacks targeting Russia (January 2025 – January 2026)

In contrast, cyber activity targeting **Russian entities** is lower in volume and differs in composition, with a stronger representation of **data breach and defacement activity** and a comparatively limited DDoS presence.



Distribution of Observed Cyber Activity Targeting Russia (Jan 2025 – Jan 2026)

Of the 575 recorded incidents:

- **Data breach claims** account for the majority (359 incidents)
- **Defacement** accounts for a significant share (152 incidents)
- **DDoS** activity is comparatively limited (41 incidents)

The most active actors targeting Russian entities include:

- **Anonymous Italia** (133 incidents)
- **HIMARS DDOS** (21)
- **BreachLaboratory** (21)

Compared with activity targeting Ukraine, operations against Russia are more distributed across a wider set of actors and lower in scale.

Year-on-year comparison (2024-2025 vs 2025-2026)

The January 2025 – January 2026 window indicates continuity rather than rupture in the cyber dimension of the conflict. The operational **asymmetry** between activity targeting Ukraine and Russia observed during the prior January 2024 – January 2025 period is maintained across three structural axes.

- **Volume:** activity targeting Ukraine remains significantly higher than activity targeting Russia, with no rebalancing across the two periods.
- **Type:** Ukraine continues to absorb large-scale disruptive operations, while activity against Russia remains oriented toward data exposure and defacement.
- **Actor concentration:** activity targeting Ukraine remains driven by a small set of high-volume actors, while activity targeting Russia stays more distributed across a wider set of collectives.

The only notable **shift** in the current window is the **reduced relative weight of DDoS within activity targeting Russia**, consistent with an operational model centered on leak and public exposure objectives rather than disruption.

Taken together, these patterns confirm two stable and distinct **operational approaches: disruption-focused operations against Ukraine, and data-theft-focused operations against Russia.**

1.2 Most Targeted Sectors: Divergent Strategic Goals

The sectoral distribution highlights a clear difference in targeting approaches.

Sectors targeted in Ukraine (January 2025 - January 2026)

Cyber activity targeting **Ukraine** between January 2025 and January 2026 shows a strong concentration on **government, defense, and critical infrastructure sectors**, which together form the operational backbone of Ukraine's wartime governance and military logistics. This pattern is reflected in the sectoral distribution of incidents, led by:

- Government and public sector (432 incidents)
- Network and telecommunications (134)
- Aerospace and defense (115)
- Insurance (85)
- Manufacturing (73)
- Energy and utilities (70)

Telecommunications infrastructure ranks as a priority target. Its disruption can affect both military command-and-control and civilian communications.

Telecommunications as a High-Leverage Target: The Viasat / KA-SAT Case

On 24 February 2022, at the onset of the Russian ground invasion, a destructive cyber operation targeted Viasat's KA-SAT satellite network.[1] The attackers gained access through a misconfigured VPN appliance on the management segment, then deployed AcidRain, a wiper that overwrote the firmware of tens of thousands of modems and rendered them inoperable.[2] The operation disrupted satellite communications used by Ukrainian government, military and civilian users, and produced spillover effects across parts of Europe, notably affecting the remote-management of approximately 5,800 wind turbines in Germany. The operation was publicly attributed to the Russian state (GRU) by the United States, the European Union and the United Kingdom in May 2022.

[1] https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/
[2] https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Targeting of **aerospace and defense, manufacturing, and energy sectors** suggests an additional focus on the defense industrial base and on the critical services underpinning national resilience,

Energy Infrastructure and Cyber-Enabled Disruption

Cyber operations aimed at degrading grid operator visibility and delaying restoration typically follow kinetic strikes, through IT-to-OT intrusion chains pivoting from corporate IT environments into ICS/SCADA systems. Notable examples include the attempted deployment of Industroyer2 in April 2022 against a Ukrainian electricity provider's high-voltage substations,[3] attributed to Sandworm (GRU), and the use of FrostyGoop in January 2024, which disrupted district heating services in Lviv for approximately 48 hours and affected more than 600 residential buildings[4] during sub-zero temperatures. These operations illustrate how cyber activity can be used to extend and compound the effects of kinetic strikes.

Overall, the distribution of targets indicates a prioritization of sectors with high operational impact.

Sectors targeted in Russia (January 2025 - January 2026)

In contrast, cyber activity targeting **Russia** is more evenly distributed across sectors, with a stronger presence of commercial and consumer-facing services.

The most targeted sectors include:

- **E-commerce and retail** (58)
- **Government administration** (33 incidents)
- **Network and telecommunications** (30)
- **Education** (27)

Other sectors, including building and construction (22), IT services (22), and financial services (22), are also regularly targeted, though at lower volumes.

[3] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
[4] https://attack.mitre.org/campaigns/C0041/

The prominence of e-commerce, retail, and education is consistent with **a preference for publicly exposed platforms**, which maximize the visibility of defacement and data-exposure operations.

Year-on-year comparison (2024-2025 vs 2025-2026)

Relative to the prior January 2024 – January 2025 period, the sectoral distribution shows broad continuity, with one **notable shift on each side:**

- **Ukraine:** government administration and telecommunications remain the top sectors. **Insurance rises more prominently**, while energy stays present but less dominant by incident volume than in 2024-2025.
- **Russia: government administration** moves from sixth position in 2024-2025 to the **most targeted sector** in the current dataset. Publicly exposed sectors (e-commerce, retail, education) remain prominent.

The two datasets converge on government administration as the most targeted sector, through continuity in Ukraine and a recent rise in Russia. Attack typologies and actor compositions remain unchanged across both periods.

1.3 Major actors: Hacktivism and APTs

This section focuses on the two categories of threat actors with the highest activity and operational impact during the conflict: hacktivist collectives and state-aligned Advanced Persistent Threat (APT) groups.

The **hacktivism** subsection focuses on **pro-Ukrainian activity.** This **ecosystem** took shape soon after the February 2022 invasion, **bringing together pre-existing groups and newly formed collectives** operating in support of Ukraine. Their cumulative volume remains well below that of NoName057(16), the most prominent pro-Russian collective, which is examined in detail further in this note. Pro-Ukrainian hacktivism is nonetheless treated separately, as it

reflects a **dynamic specific to this conflict.** The APT subsection focuses on threat actors aligned with the Russian state.

Hacktivist Activity

Hacktivist activity conducted from the Ukrainian side against Russia is diverse in its modes of operation. A significant portion of it is oriented towards **data exfiltration and public release** rather than service disruption. Groups such as Cyber Anarchy Squad and the Ukrainian Cyber Alliance have claimed intrusions into Russian **internet service providers, regional administrations, financial institutions and contractors serving the Russian state**, followed by the publication of large volumes of internal documents, customer databases and corporate emails. Part of this material is relayed through publication platforms such as DDoSecrets and sometimes picked up by investigative journalists, giving pro-Ukrainian operations a documentary and media dimension that goes beyond symbolic defacement. Other groups, including Anonymous Italia and BreachLaboratory, combine **website defacements** with the **release of data allegedly stolen from Russian entities**, while the IT Army of Ukraine is primarily associated with **denial-of-service** and HIMARS DDOS specialises in it.

Russian State-Linked APT Activity

Advanced Persistent Threats (APTs) play a key role in the Russia-Ukraine cyber activity, particularly in operations targeting **high-value entities such as government institutions, defense infrastructure, and logistics networks.** These actors are assessed as **state-linked**, operating in line with broader **strategic and intelligence objectives.** The most notable Russian state-linked actors are APT28 and Gamaredon.

APT28

Aliases	Fancy Bear, Forest Blizzard (Microsoft), STRONTIUM, Pawn Storm, Sednit...
Identity	Attributed to Unit 26165 of the GRU (Russian Military Intelligence).
Operational Logic	Follows "Support-to-Operations" (S2O) model, prioritizing high-value collection that enhances military and political decision-making, with an emphasis on sustained access and operational relevance.
Modus Operandi	Exploits infrastructure vulnerabilities (e.g., webmail servers) and edge devices (IoT), favoring stealthy persistence. Often leverages legitimate cloud services or APIs to mask activity and maintain access.
Attributed operation	Tactical IP Camera Reconnaissance (publicly disclosed May 2025). Public reporting describes Unit 26165/APT28 conducting large-scale targeting of internet-facing RTSP camera servers using RTSP DESCRIBE requests with embedded credentials (including default/generic brute-force attempts). Successful RTSP/1.0 200 OK responses exposed snapshots and stream metadata, enabling tactical monitoring. From an agency-held sample of >10,000 targeted cameras, activity concentrated on Ukraine (81.0%) and bordering states (Romania 9.9%, Poland 4.0%, Hungary 2.8%, Slovakia 1.7%), consistent with monitoring border crossings and logistics nodes supporting materiel flows into Ukraine, including via municipal traffic-camera services.[5]

Gamaredon

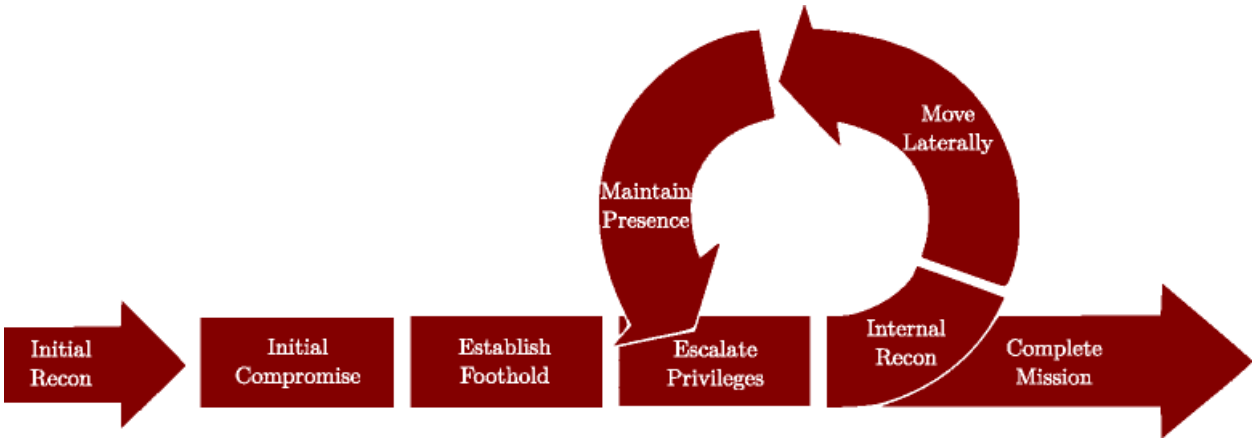
Aliases	Aqua Blizzard (Microsoft), Armageddon, ACTINIUM, Shuckworm, DEV-0157, Trident Ursa...
Identity	Attributed to Center 18 of the FSB (Federal Security Service), and GRU later on[6].
Operational Logic	Functions as a "data factory," prioritizing the frequency of attacks and the velocity of exfiltration.
Modus Operandi	Frequent spearphishing waves (often short, repeated bursts) that use fast-executing loaders (LNK/HTA/HTML-smuggling chains) and lightweight implants/tooling.

[5]https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF

[6]https://www.diplomatie.gouv.fr/en/country-files/russia/news/2025/article/russia-attribution-of-cyber-attacks-on-france-to-the-russian-military

	Collection is optimized for speed and yield, prioritizing user-accessible document stores and common work product, with constant re-obfuscation and infrastructure churn; C2 is routinely shielded behind legitimate third-party services (e.g., Cloudflare/Telegram-style relays) to resist takedown and blocking.
Attributed operation	Repeated mobilization-themed spearphishing campaigns delivering weaponized LNK/HTA artifacts with war-adjacent lures (including "mobilization"-themed filenames) for near-immediate document theft.[7] Reporting from 2024 to 2025 documents large batches of malicious LNK files disguised as Office documents with war/troop-movement themes that trigger second-stage payloads and enable rapid document harvesting, reflecting a high-tempo collection model prioritizing speed over stealth.[8]

APTs can be differentiated by their **specific tradecraft and objectives:**



The APT life-cycle
Source: Mandiant

[7] https://cyble.com/blog/gamaredons-spear-phishing-assault-on-ukraines-military/
[8]https://www.eset.com/us/about/newsroom/research/eset-research-russias-gamaredon-apt-group-unleashed-spearphishing-campaigns-against-ukraine-with-an-evolved-toolset/
https://blog.talosintelligence.com/gamaredon-campaign-distribute-remcos/

II. Cyber Operational Tradecraft and Effects

2.1 DDoS: Asymmetric Volumes and Diverging Actor Concentration

DDoS attacks remain the most frequently observed disruptive activity in the Russia-Ukraine cyber conflict, particularly in operations targeting Ukrainian entities.

DDoS operations generate high-volume traffic intended to overwhelm targeted services and degrade availability. They can disrupt access to government services and expose resilience limitations during periods of heightened tension, though their effect remains immediate and does not extend to persistent system compromise.

Pro-Russian

Between January 2025 and January 2026, DDoS activity targeting **Ukraine** remained concentrated and large-scale, with **1,391 recorded incidents. NoName057(16)** alone accounts for 913 of these, while OverFlame (101), Z-ALLIANCE (33), and Dark Storm Team (32) operate at significantly lower volumes.

Compared with the January 2024 to January 2025 baseline, the overall volume is broadly stable (1,391 vs 1,377), but actor concentration has increased: NoName057(16)'s share has grown significantly, reinforcing its role as the primary driver of large-scale disruptive campaigns.

In the opening phase of the full-scale invasion, DDoS campaigns surged, **peaking** on 25 February 2022, just after Russia's **recognition of the Donetsk and Luhansk People's Republics**, with the targeting of major Ukrainian institutional portals including the Parliament, Ministry of Foreign Affairs, and Council of Ministers[9]. Operations continue to follow **a reactive pattern**, with coordinated surges **aligned to political or military developments**, consistent with the use of DDoS as a rapidly deployable disruption tool.

[9] https://t[.]me/+nCXg3HajFNtjYzNk

Ukrainian-Aligned

In contrast, **DDoS activity targeting Russian entities** remains significantly **lower** in volume, with 41 incidents recorded between January 2025 and January 2026, down from 86 in the previous period. The decline is visible both in absolute terms and relative to other tactics such as data-breach claims and defacement.

The pro-Ukrainian group HIMARS DDOS accounts for more than half of these incidents. No single actor dominates at scale, and operations remain distributed across multiple groups, contrasting with the concentration observed on the Ukrainian side.

Sectoral targeting remains consistent with earlier observations, concentrated on **Network and telecommunications** (14 incidents) and **Government administration** (5), with smaller volumes across **Education, IT services, and Media.**

DDoS campaigns against Russia continue to coincide with **high-visibility political or symbolic events**, indicating an opportunistic role tied to short-term visibility rather than sustained disruption.

Comparative Observations

The observed dataset reinforces a clear asymmetry in the use of DDoS across the conflict:

- **Ukraine** remains the **primary target of large-scale DDoS activity**, with sustained high volumes and strong concentration around a major actor, NoName057(16)
- Russia is targeted at significantly lower volumes, with DDoS representing a smaller share of overall activity and no dominant operator
- The actor landscape diverges: highly centralized on the pro-Russian side, more fragmented among Ukrainian-aligned groups

Compared with the 2024-2025 baseline, the most notable evolution is the **decline in DDoS activity targeting Russia**, alongside continued **consolidation on the Ukrainian front** around a small number of high-volume actors.

2.2 Defacement: A Signaling Tactic Predominantly Targeting Russia

Defacement, the unauthorized modification of website content to display messages or imagery, remains a visible hacktivist tactic in the Russia-Ukraine conflict. Its purpose is primarily symbolic: increasing exposure and amplifying messaging rather than degrading operations.

Activity Targeting Russia

Between January 2025 and January 2026, 152 **defacement incidents targeting Russian** entities were recorded, up from 15 in the previous period. This sharp rise marks a shift in Ukrainian-aligned activity, with defacement emerging as a primary **visible tactic** against Russian targets.

Activity is concentrated around a single actor, **Anonymous Italia**, which accounts for 133 of the 152 incidents. The group is affiliated with the broader Anonymous collective, a decentralized network of ideologically aligned actors coordinating campaigns against Russian interests. Other actors are present but contribute marginally.

Sectoral **targeting** focuses on **public-facing and widely accessible digital environments:** Building and construction (17 incidents), Education (14), and Retail (10). These sectors are associated with exposed websites suitable for high-visibility defacement operations.

Compared with the previous period, the rise in volume is accompanied by greater actor concentration and higher operational tempo, pointing to a more structured use of defacement within Ukrainian-aligned campaigns.

Activity Targeting Ukraine

In contrast, **defacement activity targeting Ukraine has declined** in the current reporting window, with 47 incidents recorded between January 2025 and January 2026 compared with 63 in the previous period. This points to a reduced role for defacement within pro-Russian campaigns, where DDoS remains the dominant tactic.

Activity is also more distributed across actors, with no single group standing out. The most active are Z-ALLIANCE (8 incidents), Z-PENTEST ALLIANCE (4), and NoName057(16) (4).

Sectoral targeting is limited in scale and spread across multiple sectors, including **Education** (5 incidents), **Government administration** (5), and **Network and telecommunications**, with other sectors at low volumes.

Compared with activity targeting Russia, defacement operations against Ukraine are less frequent, less concentrated, and occupy a more marginal place within pro-Russian tradecraft.

Comparative Observations

The updated dataset highlights a clear shift in defacement dynamics across the conflict:

- **Activity targeting Russia has increased** significantly in both volume and concentration, now driven primarily by Anonymous Italia
- **Activity targeting Ukraine has declined** in relative importance, remaining limited in scale and distributed across multiple actors
- The tactical role diverges: **Ukrainian-aligned groups use defacement as a high-visibility** signaling tool, while pro-Russian operations continue to prioritize large-scale disruption through DDoS

2.3 Data Breach Claims: Distinctive Features of Pro-Ukrainian Activity

Data breach claims constitute a significant share of observed cyber activity in a conflict, as information stands at the core of multiple **objectives: exploitation of data for intelligence purposes, search for public recognition through the announcement effect, and contribution to the psychological dimension of the war.**

Between January 2025 and January 2026, 359 data breach claims were recorded against Russia, compared to 156 against Ukraine, making breach activity the **dominant observed tactic in the Russian-facing dataset.** This section focuses on the actions and modus operandi of attacks conducted by Ukrainian state-linked actors or by groups aligned with their cause.

Ukrainian and pro-Ukrainian actors stand out for their hack-and-leak model, oriented toward more immediate objectives: operational exploitability, psychological effect, and visibility, in contrast with the more silent espionage posture of APT-style activity discussed earlier.

As an example of an operation primarily aimed at producing a psychological effect, **on March 28, 2022, the GUR published on its official portal a nominal list of 620 alleged FSB officers**, exposing for each individual a detailed set of professional and personal information: full patronymic names, dates of birth, military unit numbers (VCh) and service locations (e.g., Lubyanka HQ), internal employee identification numbers, phone numbers, and database security hashes (MD5/SHA) used for internal authentication. This operation falls within a doxing logic, deliberately exposing individuals professionally engaged in state functions tied to military activity during the conflict. Beyond its informational value, such disclosure is designed to produce a psychological effect on the targeted personnel and, more broadly, to induce a sense of vulnerability within the adversary camp, calling into question the state's capacity to protect both its personnel and its population.

As an example of claimed data theft serving both operational and public-resonance objectives, in January 2024 Ukraine's military intelligence (DIU/GUR) reported the compromise of **Russian**

Ministry of Defense systems and the exfiltration of approximately 100 GB of data, reportedly supporting operational analysis.

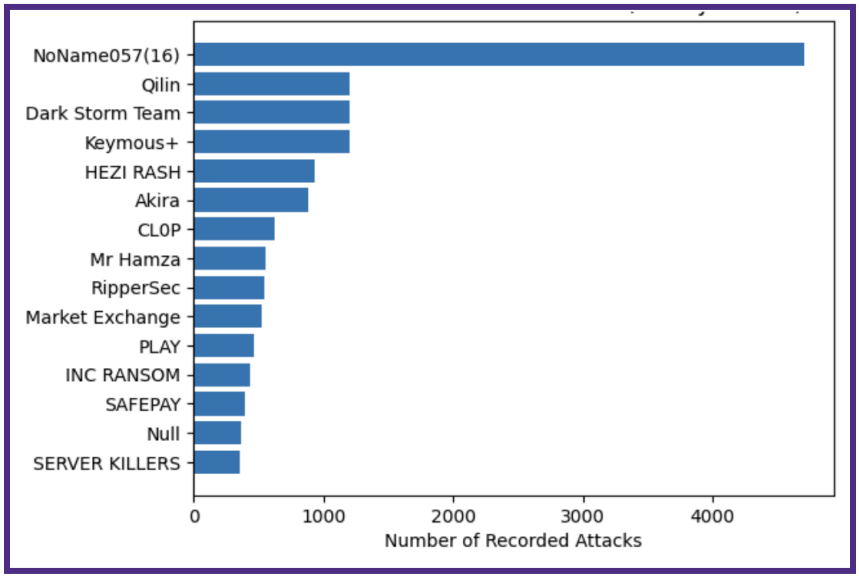
It is important to note, however, that outside the perimeter of the conflict, the actor set and **motivations remain heterogeneous**, including **opportunistic and financially motivated groups.** Data breach claims should therefore not be read as exclusively conflict-driven. Actors such as BreachLaboratory, X0Frankenstein, and Sophia display opportunistic or multi-geography behavior, and their sectoral targeting (e-commerce, government, financial services, retail) is consistent with a data-accessibility and monetization logic rather than with a conflict-related agenda.

III. Cross-Border Spillover: The NoName057(16) case

Pro-Russian groups remain **the most active operators against Ukraine**, but their targeting extends well beyond Ukrainian networks. **EU and NATO** member states perceived as politically or militarily supportive of Kyiv have increasingly been **subjected to disruptive campaigns**, broadening the geographic footprint of the conflict.

3.1 A Primary Driver of Targeting Against Ukraine's Supporters

Since January 2025, **NoName057(16)** has recorded approximately **5000 attack claims** globally, making it the most active threat actor worldwide during this period. By comparison, Qilin, Dark Storm Team, and Keymous+ each recorded around 1,200 incidents, placing them significantly behind in volume. Unlike other actors whose expertise is heavily focused on DDoS attacks, Qilin distinguishes itself as a ransomware operator, which is more time-consuming and complex to deploy on victims' systems. The number of claimed attacks suggests extremely significant and noteworthy activity, as demonstrated by the analysis.



Most Active Threat Actors Worldwide (since January 2025)

This dominance is largely explained by **DDoSia**, a **crowdsourced attack platform** launched by the group in 2022. Volunteers install a dedicated client, register through a Telegram bot, and receive automatically updated target lists against which their machines generate denial-of-service traffic. A **gamified participation model** with cryptocurrency rewards sustains engagement and has drawn several thousand registered volunteers, turning a hacktivist group into an **industrial-scale disruption engine against Ukrainian government institutions, telecommunications providers, and public-facing services** relied upon in wartime.

A significant share of NoName057(16)'s activity has been directed at NATO member states, particularly Germany, followed by Italy, France, and Spain. The group is the most frequently observed threat actor against each of these countries during the reporting period.

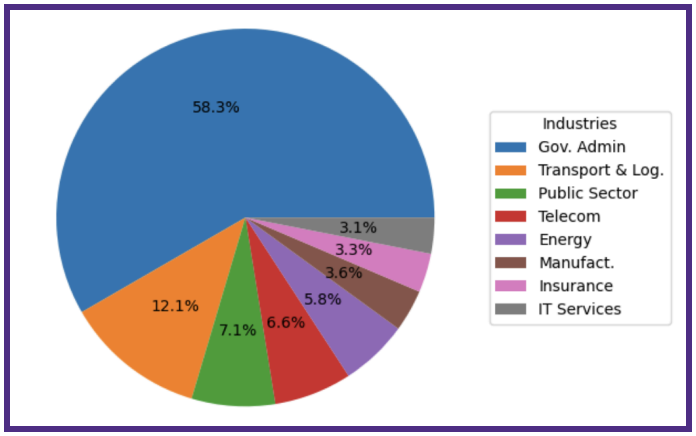
This targeting is geographically consistent with states providing military or political support to Ukraine, a pattern aligned with efforts to impose pressure on Kyiv's partners.

A recent evolution also deserves attention: **pro-Russian hacktivism is increasingly overlapping with pro-Iranian and anti-Israel campaigns.** In March 2026, several pro-Russian groups participated in operations aligned with pro-Iranian messaging, and NoName057(16) ranked among the most active actors targeting Israel after 28 February. This points to an increasingly fluid landscape, where groups shift their focus from one conflict to another based on immediate political opportunity.

3.2 Sectoral Targeting in states supporting Ukraine

Public and government-sector entities represent the largest share of NoName057(16)’s cross-border targets, with 1,800 incidents affecting **government administration** since January 2025, followed by: **transportation & logistics, government & public sector, network & telecommunications, energy & utilities, manufacturing, insurance.**

Spillover activity in allied states mirrors the targeting logic observed in Ukraine, albeit at lower operational intensity. The objective remains to consistently create disruption within governance and critical systems linked to national resilience.



NoName057(16) Industry Target Share (since January 2025)

3.3 Reactive Spikes Following Political or Military Events

There are notable spikes in NoName057(16)'s operations, particularly **following major political or military events unfavorable to Russia's position**, suggesting that the group's activity patterns are consistent with a reactive, event-driven targeting logic.

For example, in August 2024, as Ukrainian forces advanced into Russia's Kursk region, the group launched a coordinated DDoS wave targeting government and critical infrastructure entities in both Ukraine and NATO states, reaching 82 unique targets on August 6 alone.[10] Similarly, in March 2025, French government entities were targeted following public statements supporting Ukraine. Italian institutions were also targeted in February 2025 after political declarations backing Kyiv.

[10] Kursk Region Government Telegram Channel: https://t[.]me/kurskadm/72726

IV. Defensive Implications and Recommendations

4.1 How to Interpret the Figures Presented

Geopolitical events translate into cyberspace according to two very different timescales, which must be distinguished to properly calibrate one's defense.

On the one hand, **the response is immediate and highly visible:** an official statement, a parliamentary vote, or an announced arms shipment triggers waves of **DDoS and defacement** attacks within 24 to 72 hours, carried out by hacktivist groups such as NoName057(16). Openly claimed on Telegram, these operations account for 84% of the incidents recorded against Ukraine.

On the other hand, there is a continuous, discreet, and patient activity, pursuing deeper, strategic objectives: espionage and pre-positioning conducted by **state-sponsored groups** (APT28, Gamaredon, and, beyond the scope of this report, Sandworm and Turla, for example). This activity is **rarely claimed** by its perpetrators and seldom translates into publicly visible incidents in the short term, and therefore appears only marginally in the figures (3.4% for initial access claims against Ukraine). Rather than being event-driven, it **aims at long-term data collection, sustained access, and high-impact actions** such as sabotage, particularly in critical industrial environments (as illustrated by the Industroyer2 and FrostyGoop cases mentioned above), and preserving the option of future action.

The dataset volumes therefore correlate with where media and political pressure is concentrated, not with where actual adversarial activity takes place. An organization that calibrates its defense solely on visible figures is preparing for the wrong threat: it protects the storefront, not the vault. This is the key caveat to keep in mind when reading the recommendations that follow.

4.2 Mitigation Recommendations

- **Inventory and reassess the role of internet-exposed connected devices**, particularly IP cameras. The APT28 campaign of May 2025, documented above, targeted more than 10,000 IP cameras via the RTSP protocol (used by most CCTV systems to stream their feeds), with 81% of the attacks focused on Ukraine and 18% on neighboring countries (Romania, Poland, Hungary, Slovakia). When repurposed by an adversary, this type of equipment becomes a remote Intelligence, Surveillance, and Reconnaissance (ISR) asset: in this case, it was used to monitor logistical corridors supplying Ukraine. Organizations exposing such equipment must recognize that its primary function can be turned against them and must therefore inventory every IP-connected device reachable from outside, then either decommission those without operational need, isolate the rest on a segmented network, or harden their access controls.

- **Strengthen detection of LNK and HTA files in inbound email traffic.** The Gamaredon modus operandi described in this report relies on repeated spearphishing waves using files disguised as Office documents or other legitimate-looking files, with military-mobilization themes as decoys. Successful intrusions are followed by rapid exfiltration of recently modified documents. Organizations with strong ties to Ukraine are plausible targets for these lures. Static detection on these extensions, combined with email sandboxing and dedicated EDR rules covering LNK/HTA execution chains, remains a worthwhile investment.

- **Conduct practical testing of the IT-to-OT intrusion chain for critical operators.** The Industroyer2 (April 2022, high-voltage substations, neutralized before triggering) and FrostyGoop (January 2024, district heating systems, outages affecting hundreds of civilian buildings) cases follow a consistent pattern: initial compromise of the corporate IT network, lateral movement, and execution against ICS/SCADA systems. For essential service operators such as energy and water, perimeter availability matters less than containment: stopping IT-to-OT lateral movement within the first 48 hours is what determines whether an intrusion remains an IT incident or escalates into a service disruption.

- **Extend DDoS protection beyond the main portal to all internet-facing services.** NoName057(16) heavily targets public administrations (382 incidents in Ukraine, 1,800 cross-border incidents), with activity concentration that has further increased since 2024. Based on the dataset analyzed in this report, attacks often succeed on unprotected technical assets such as exposed subdomains and public APIs, as well as on citizen-facing services such as payment portals and appointment-booking platforms. It is therefore worth verifying that protection covers not only the main portal but the full attack surface.

- **Set up an early-warning capability that correlates political events with cyber activity.** The link between the two is well documented: a peak in August 2024 during the Ukrainian advance into the Kursk region (82 unique targets on 6 August alone), a wave against France in March 2025 following pro-Ukrainian statements, and a wave against Italy in February 2025 after similar positions. NoName057(16) campaigns triggered this way typically last three to seven days, with a peak in the first 48 hours. For public administrations and organizations in sensitive sectors, temporarily raising the defensive posture during the 48 to 72 hours that follow a major political trigger (official statement, parliamentary vote, announced arms delivery) is a low-cost measure that is rarely implemented. It requires no particular technical investment, only a standing coordination between public-affairs teams and the security operations center. In that sense, monitoring political announcements and tracking open-source channels used by threat actors are two essential "listening" measures.

- **Pre-build the narrative response to a hacktivist incident.** Despite their limited technical impact and short duration, DDoS attacks and defacement are deployed for their signaling value: a two-hour outage of a public service routinely generates media coverage out of all proportion to its operational severity, which is precisely the attacker's objective. Predefined talking points, clear criteria for escalating the communication response*,* a commitment to acknowledge the incident publicly before media framing sets in*, and pre-established coordination with national authorities* such as ANSSI in France, BSI in Germany, or CCN-CERT in Spain prevent rushed crisis communication and the amplification effect the attacker is seeking.

- **Expand sectoral threat-sharing beyond the traditional perimeter.** Two shifts in the dataset deserve attention. Insurance has risen to third place among targeted sectors in Ukraine (85 incidents), against a marginal position in the previous dataset. Logistics and transportation now account for 12% of NoName057(16)'s cross-border targets, just behind public administration. These sectors are not spontaneously perceived as exposed to a geopolitical cyber risk, which is precisely what makes them attractive to attackers. National CERTs and sector-level ISACs should therefore extend their information-sharing scope and tabletop exercises to insurance, logistics, and transportation operators, which today rely mostly on generic cyber programs disconnected from geopolitical threat models.

- **Account for the convergence of hacktivist ecosystems.** A hacktivist group's commitment to a given cause rarely implies a narrow scope of involvement. Such groups tend to follow an ideological coherence that ties them to a broader political logic, with implications reaching well beyond the conflict in which they are most visibly engaged. NoName057(16) illustrates this pattern: in March 2026, it joined other pro-Russian collectives in campaigns aligned with pro-Iranian narratives, targeting Israel from 28 February 2026 onward. For an organization, exposure to these groups depends on its overall geographical presence and geopolitical positioning. Entities present in several sensitive countries accumulate exposures that can no longer be treated separately.

4.3 Final remarks

Examined in this note through its use, patterns, and evolution, the cyber dimension is confirmed as a central component of the conflict. Its presence can be observed across **three principal and cross-cutting dimensions:**

- **the state apparatus and the industries directly contributing to the war effort;**
- **essential services and critical infrastructure;**
- **civil society, including the organizations and individuals that compose it.**

The first has historically been the primary actor of war and is therefore, by nature, its primary target. This continues to hold true in the current hybrid-warfare context.

The second, sitting at the junction between the State and society, has imposed itself as a privileged target, used to weigh on and destabilize both the State and the society. This trend is confirmed by our dataset.

The third, while it has long been recognized as a major component of any conflict, now occupies a particular and redrawn place, both as a target and as an actor.

Civil society organizations are not spared, and the place of the individual is the most visibly redefined. As a target, the individual is exposed to the full breadth of the cyber toolkit: an object of propaganda, a subject of psychological pressure (collective and individual), and the focus of operations designed to degrade quality of life and constrain everyday capabilities. The individual has become a high-priority target, sought for itself.

Conversely, the individual can also assert themselves as a fully-fledged actor in this digital confrontation, even with limited resources. Their actions, conducted alone or aggregated within digitally-formed collectives, **can carry a level of resonance and impact disproportionate to the means mobilized**, illustrating a particularly effective form of digital "weak-to-strong" posture.

In a war whose stated objectives may appear primarily territorial, but in which each side ultimately seeks to assert its narrative dominance and its standing on the international stage, **the digital front of the Russia-Ukraine war reveals significant transformations in the contemporary practice of war: in its aims, in the means deployed, in the modes of action, and in the actors involved.**

Scan, Prioritize, Resolve External Threats

Contact us:

react@cybelangel.com

CybelAngel