Whitepaper

Hacktivism in 2025:
Where Politics Meets Cyberspace

SOCRadar®
Your Eyes Beyond

socradar.io

Hacktivism in 2025: Where Politics Meets Cyberspace

Executive Summary:
Hacktivism has grown from small online protests into a regular part of the cyber world. What started as activism through hacking now often connects to much larger political or strategic goals. Hacktivist activity is frequent and fast. Many attacks aim for attention more than damage. Leaks, DDoS, defacements, and ransomware now appear together. Telegram and X (Twitter) are key hubs for planning and spreading claims.

Key points:

- Most incidents are timed to matter, elections, wars, and diplomatic crises draw the most activity.
- Many groups that call themselves hacktivists work with, or benefit, state actors. This blurs attribution and slows response.
- Leaks are a core tactic: stolen data gets published to damage reputations, sow doubt, and shift public opinion.
- Regions to watch: South Asia (reactive attacks tied to local clashes), the Middle East (conflict-driven campaigns), and Russia–Ukraine (highly organized, state-linked operations).

What to expect:

- More leak-based campaigns around major events.
- Hybrid attacks that mix disruption, theft, and disinformation.
- Continued use of activist labels to hide true sponsors.

What organizations should do:

- Treat hacktivism as a strategic risk, not a one-off nuisance.
- Prepare combined technical and public-response plans.
- Monitor channels where groups announce or organize.

Bottom line: In 2025, hacktivism is not just protest. It is a weapon of influence used by diverse actors to shape politics and public debate.

Introduction

Hacktivism brings hacking and activism together. It uses cyberattacks to make a statement, raise awareness, or protest. Some people act alone, while others form groups that work toward a common goal.

But hacktivism is rarely straightforward. A group's cause might be real, or just a cover for something else. In cybersecurity, that difference matters. To some, hacktivists are digital rebels; to others, they're vandals or even terrorists. Behind the screen could be a beginner, an expert hacker, or maybe a government employee.

Motives vary by region. In South Asia, it often grows from territorial disputes. In the Middle East, from religion and ideology. In the West, it takes the shape of protest. In Russia, it is framed as patriotic defense. The hacktivists we are discussing here are hackers before they are activists.

Ukraine has accused Russian "hacktivists" of fronting for state intelligence. Israel's *Predatory Sparrow* (*Gonjeshke Darande*) poses as a hacktivist group, but its precision hints at military-level skill. Once, Anonymous stood as the face of "true" hacktivism. Today, its name has become a brand—used by countless offshoots seeking credibility, echoing Voltaire's remark that the "Holy Roman Empire" was neither holy, Roman, nor an empire.

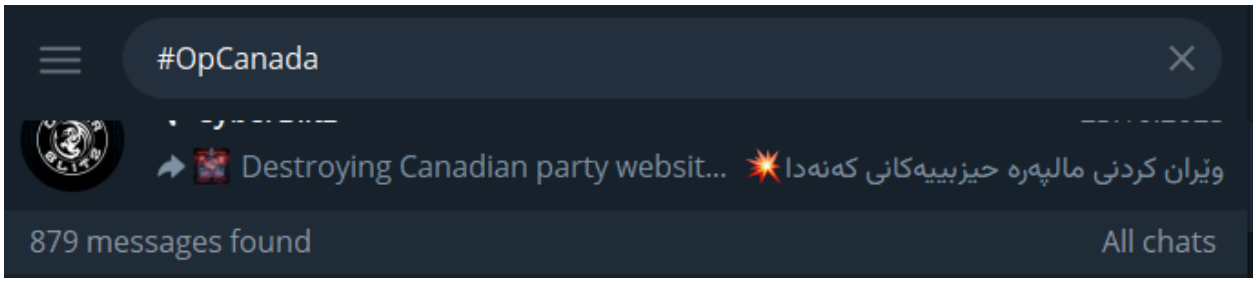
Hacktivism meant hacking for a cause. Now it mirrors digital chaos. Criminals use it as cover for profit. States hide cyberattacks beneath its banner. Others chase attention. Some deface websites to make a statement; others use DDoS attacks to disrupt. Even ransomware now carries political slogans.

Hacktivism has become a web of belief, politics, money and ideology that increasingly overlaps with nation-state cyber-attacks.

Hacktivism in 2025

Like every entity in cyberspace, hacktivism is in constant change, and in recent years, hacktivism has shifted from episodic digital protest to constant pressure on the cyber frontier. Across Europe alone, the European Union Agency for Cybersecurity (ENISA) logged nearly **4,900** incidents between July 2024 and June 2025. Of those, ideologically motivated attacks by self-declared hacktivist groups accounted for **nearly 80 %** of cases.

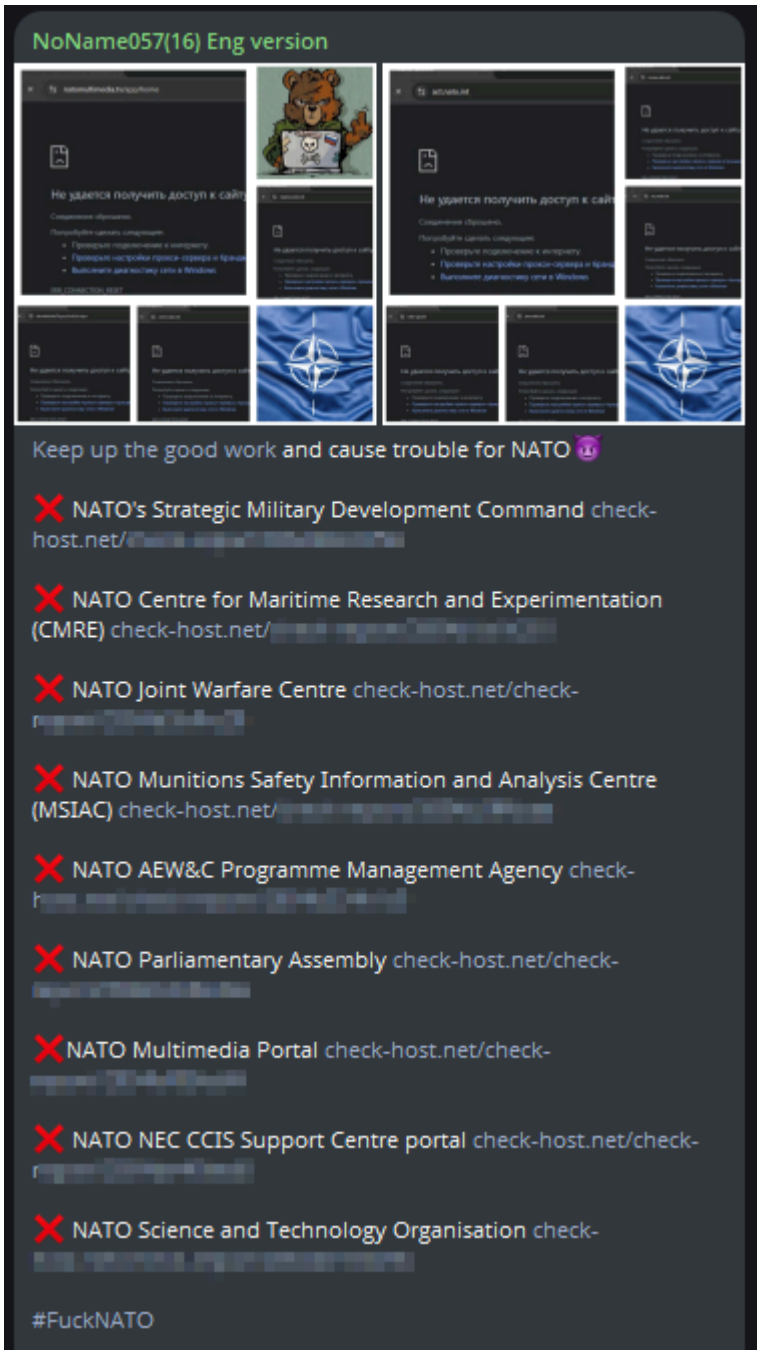
Operations move through open channels. Overwhelmingly on **Telegram**, secondarily on X. Hashtags and shared target lists allow quick mobilisation. This lowers the barrier to entry and speeds campaigns. It also creates copycat waves. One provocation can trigger dozens of small attacks within hours.



*Hashtag activity related to **#OpCanada** on Telegram. The operation, active from 2024 through 2025, shows nearly 900 messages and posts in channels we monitor.*

Persistent

The bulk of these attacks took the form of DDoS operations, **77 %** of incidents in the reporting period were outages and floods of web traffic. Most inflicted limited damage individually, yet their sheer number signalled a new kind of digital activism: **high volume, low impact, but persistent.**



NoName057(16) has been one of the most active hacktivist groups since 2022. Maintaining continuous operations for one to two years is rare in this landscape, yet their persistence has defied expectations. Even after temporary disruptions, the group reemerged more aggressive and organized than before.

*Operation Eastwood, launched in mid-July, briefly disrupted NoName057(16). The group was **inactive for only a few days** before rebounding, increasing both the frequency of its attacks.*

Convergent

This year also saw the lines between hacktivism, cybercrime, and state-sponsored operations blur. Hacktivist groups adopted **ransomware**, financial extortion, and supply-chain attacks. Simultaneously, states aligned with known intelligence services used hacktivist-style campaigns to muddy attribution.

*BQTLock Ransomware mixes political messaging with financial motives. Though it promotes ideological causes, profit drives its actions, **blending hacktivism with cybercrime**, it maintains links with pro-Palestinian hacktivist groups.*

Interlinked

Hacktivist alliances have become an essential part of today's digital conflicts. These alliances are not formal organizations but loose coalitions united by ideology or a shared enemy. Telegram channels serve as their main coordination hub, where groups cross-promote campaigns, exchange target lists, and amplify propaganda.

In the Middle East, operations like **#OpIsrael** or **#AlAqsaFlood** brought together pro-Palestine collectives.

In Russia's orbit, groups like *NoName057(16)*, and TwoNet coordinate with many smaller affiliates across Eurasia through shared botnets and mirrored channels.

In South Asia, rival groups from India and Pakistan frequently mirror each other's tactics, launching reactive DDoS or defacement attacks after regional provocations.

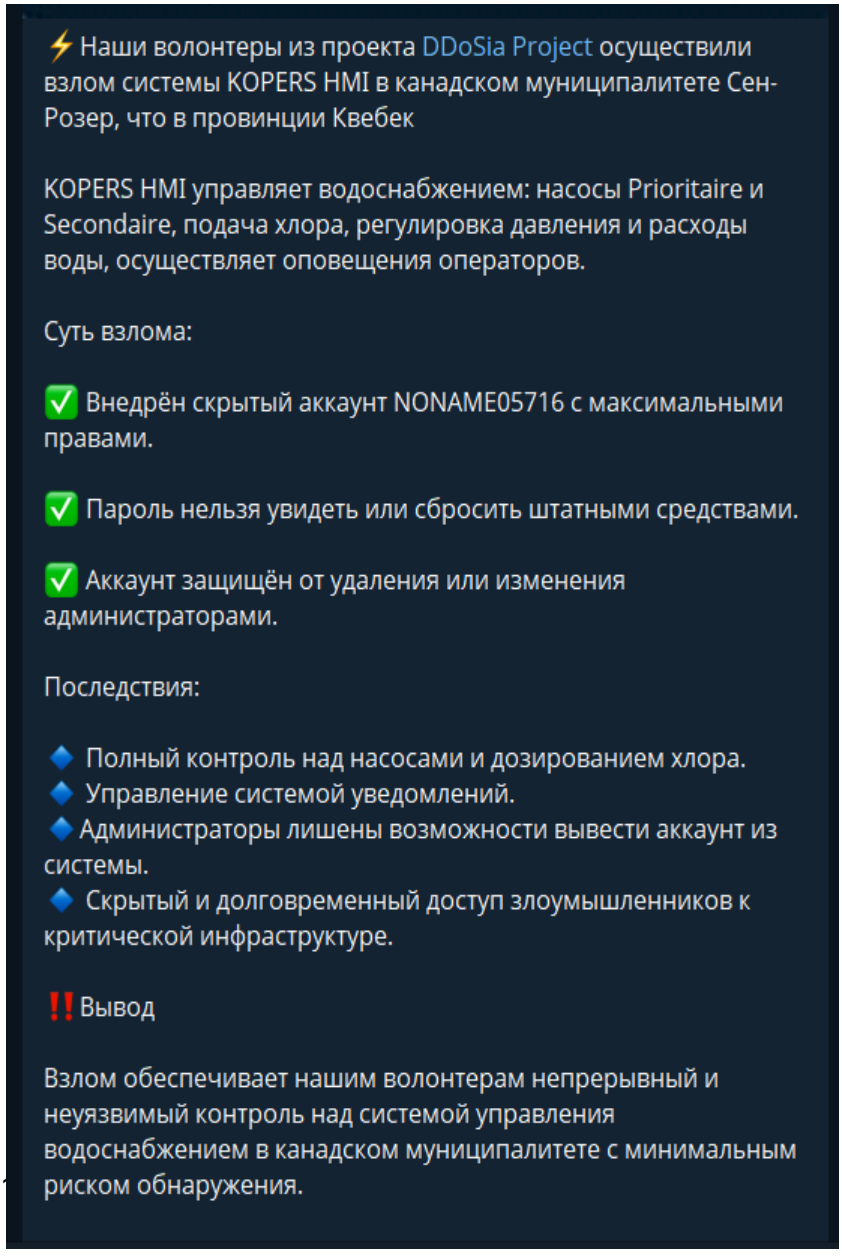
While South East Asian countries with a Muslim majority prefer to act together, Indian groups are having a harder time finding international alliances.

In hacktivism, alliances function less like formal partnerships and more like mutual amplification networks. They offer protection, validation, and visibility. By forming such alliances, smaller groups gain legitimacy and reach, while larger ones consolidate influence and control narratives.

Geopolitical

Political tensions, conflicts, and elections shape both timing and target selection. In many EU countries, public-administration websites, transport portals and banks were frequent targets for hacktivist groups, especially around elections, national security announcements or foreign-policy shifts.

Beyond Europe, North America also raised alarms, Canada issued a public warning recently that hacktivists had compromised "critical infrastructure systems," including municipal control environments.



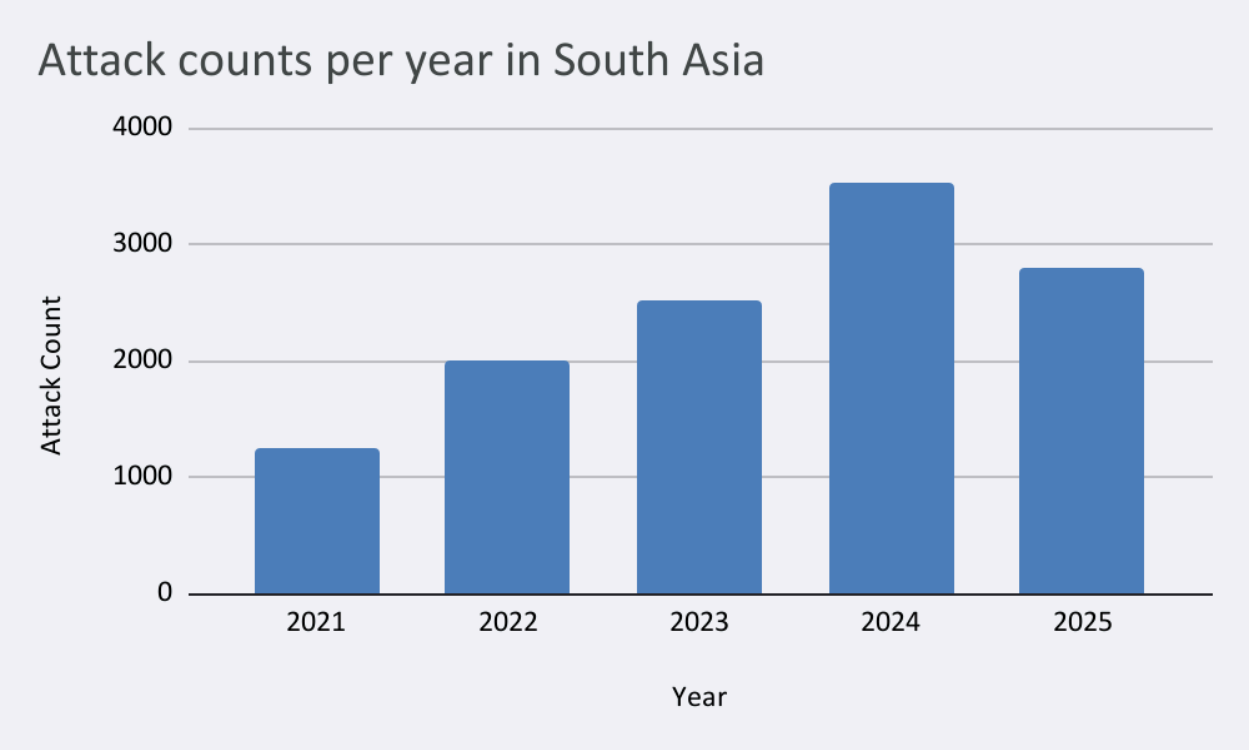
NoName057(16): "Our volunteers from the DDoSia Project hacked the KOPERS HMI system in the Canadian municipality of Sainte-Rose, in the province of Quebec. KOPERS HMI controls the water supply: Prioritaire and Secondaire pumps, chlorine dosing, pressure regulation and water flow, and it sends operator alerts..."

Battle Theaters

Hacktivism mirrors the world's geopolitical map. It thrives where real-world tensions run hottest, turning wars and disputes into ongoing digital campaigns. Modern hacktivism now tracks the same conflict lines that dominate headlines: Ukraine's defense against Russia, Israel's clashes with Iran, ongoing war on Gaza, and the friction between India and Pakistan over Kashmir.

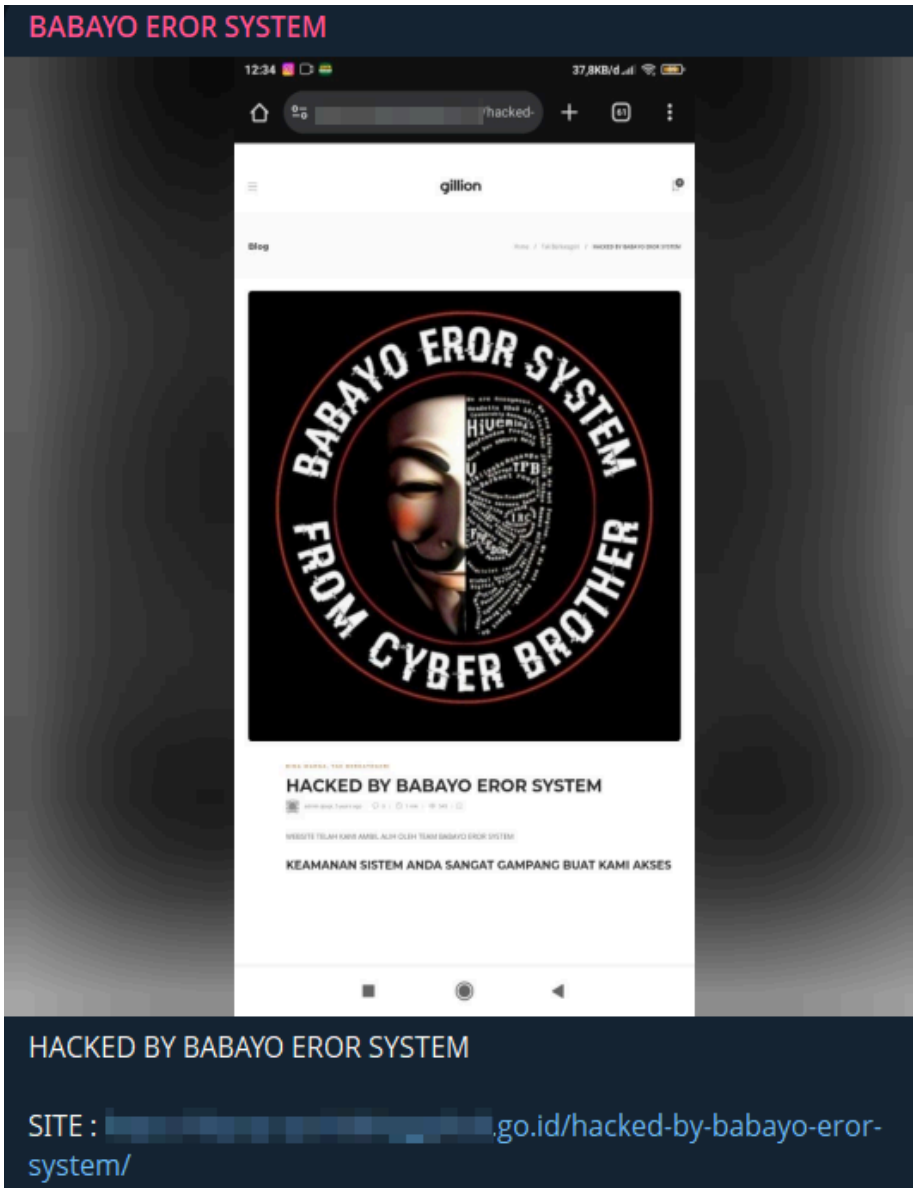
South Asia

Hacktivism in South Asia follows the region's long political and territorial tensions. Cyber campaigns spike whenever tensions rise on the ground. The Kashmir conflict is the clearest example. When clashes or political moves occur, online actors, from loose collectives to organised crews, rush to make a statement.



*Cybercrime activity targeting South Asia has increased sharply since 2021, reaching its highest levels in 2024. The year **2025** represents activity through the **first three quarters**, suggesting that the region will likely match or exceed the previous year's total once full-year data are available. (Source: SOCRadar, Dark Web News)*

Targets tend to be visible and symbolic. Attackers aim at government portals, news sites, police pages and local service websites. They prefer actions that show fast results: DDoS floods that take a site offline, defacements that post political messages, and small data leaks that embarrass local officials.



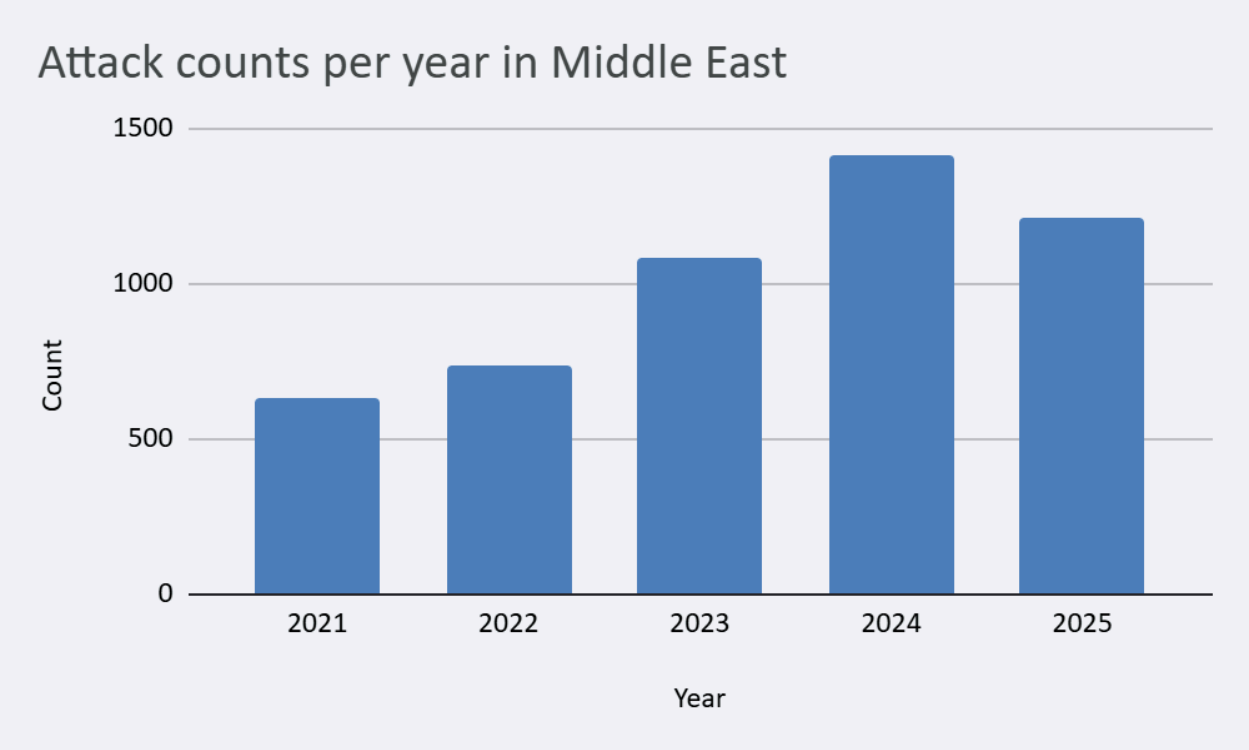
Defacement attack by the "Babayo Eror System," a hacktivist collective active in Southeast Asia. Defacement remains the most common form of hacktivist activity in the region, favored for its simplicity and visibility. However, many such incidents target low-traffic or poorly secured websites, serving more as symbolic gestures than meaningful disruptions.

Groups are diverse. Some are patriotic volunteers who see themselves as defenders of the nation. Some are opportunists who use political cover to gain attention or profit. In this region, few show skill levels equal to actual cyber criminals.

State involvement sits on a spectrum. Some campaigns clearly aim to support official narratives. Others appear independent but benefit a state interest. Intelligence services and military cyber units do not always claim these actions. This ambiguity helps both sides: activists get cover and states gain plausible deniability.

Middle East

Hacktivism in the Middle East mirrors the region's geopolitical volatility. The Israel–Iran conflict shapes much of the landscape, merging state-backed operations, patriotic volunteers, and ideological hacktivists into one active ecosystem. Telegram remains the main platform for coordination, with thousands of messages exchanged each month among groups aligning along religious or political lines.



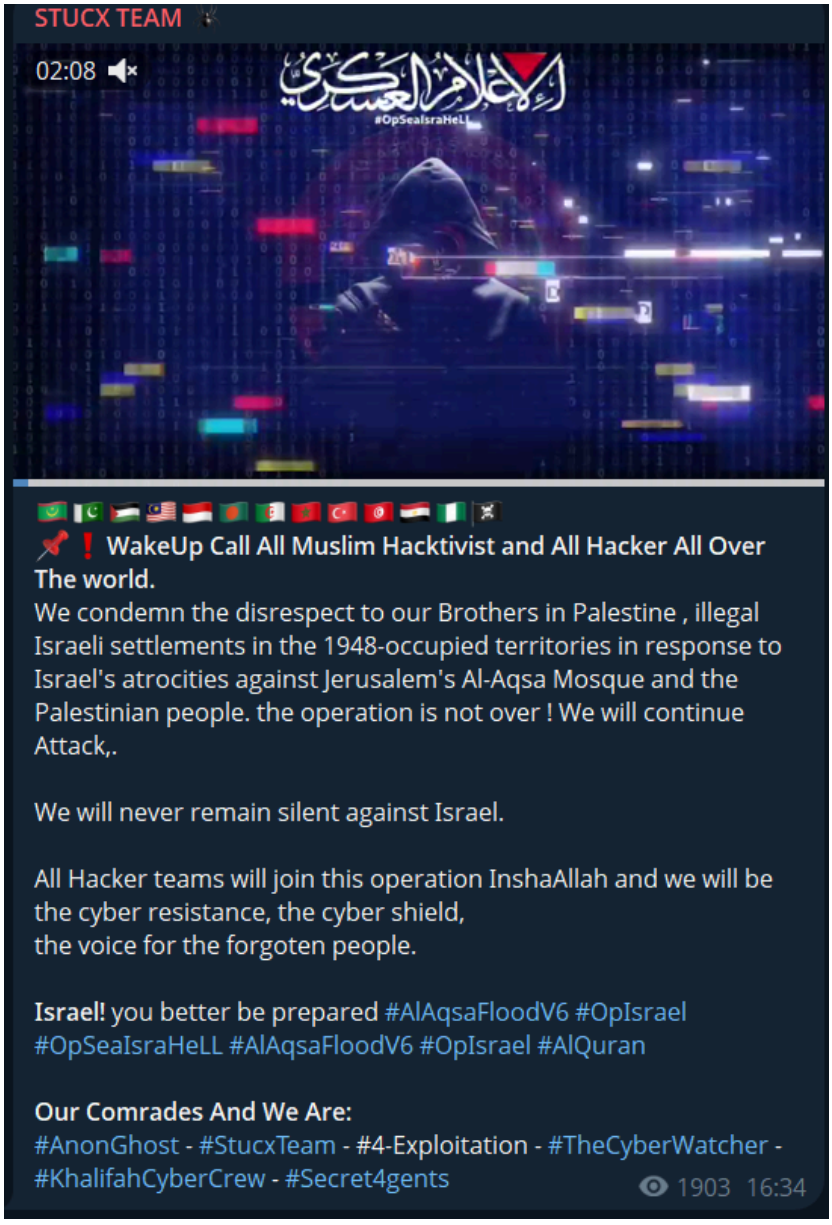
Cyber incidents in the Middle East show a consistent upward, 2025 reflects only partial-year data but already indicates sustained activity levels. (Source: SOCRadar, Dark Web News)

Hacktivist activity in the region surged during the escalation of hostilities in late 2023 and remained intense throughout 2025. Waves of attacks often corresponded directly to military events. For example, after airstrikes or major announcements, activity spiked within hours, flooding Israeli, U.S., and Gulf-region targets with DDoS and defacement attempts.

*In June 2025, during "Operation Rising Lion," over **600** unique cyberattack claims appeared across **100** Telegram channels in just two weeks, many backed by partial proof of disruption. Check out our Iran-Israel report for the full analysis.*

From the Middle East but not limited to...

Their operations expand beyond Israel to include Western allies like the US and Arab states, accused of supporting Tel Aviv. Attacks typically target telecom, **government**, and media infrastructures, often justified as "retaliation" for political or military cooperation.



Propaganda post by Stucx Team, a pro-Palestinian hacktivist collective, calling for joint participation in #OpIsrael and related campaigns.

The dominant tactic remains **DDoS**, used in nearly two-thirds of all verified claims. Defacements, credential leaks, and low-level data disclosures follow. However, most of these actions serve propaganda more than disruption. Many campaigns emphasize optics, posting screenshots of "proof" and flooding social media with hashtags like ***#FreePalestine***, ***#OpIsrael*** to reinforce collective identity.

Unlike South/east Asia, the line between hacktivism and state operations is thin. Iranian state-linked APTs such as **OilRig (APT34)** and **MuddyWater** operate alongside hacktivist collectives, using the same narratives and timing their actions to complement strategic goals

On the opposite side, Israeli-aligned entities, like **Predatory Sparrow** carry out highly coordinated attacks that seem far beyond the reach of ordinary hacktivists.

Russia & Ukraine

Hacktivism tied to the Russia–Ukraine conflict remains the most persistent and politicized digital battleground of the decade. What began as a parallel front to the kinetic war has evolved into a global ecosystem of cyber groups aligned along ideological, patriotic, and strategic lines. These operations now extend well beyond Ukraine, shaping cyber-conflict trends across **Europe, North America, and NATO.**

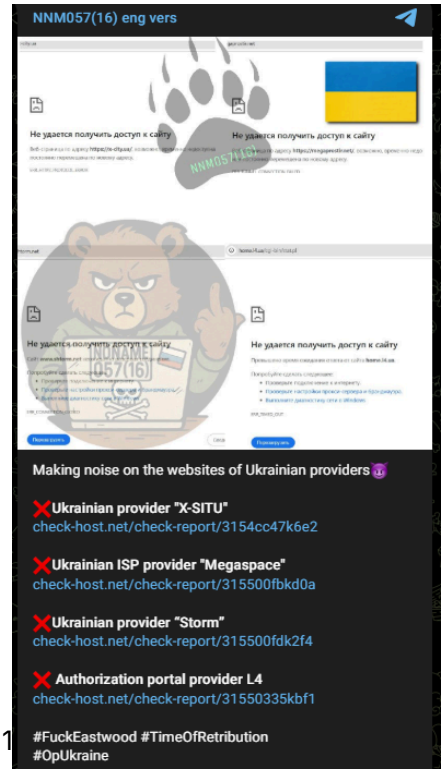
NATO countries have become routine targets of pro-Russian retaliation. DDoS attacks on **Polish**, **German**, **British**, and **Canadian** ministries surge during political flashpoints such as sanction packages or arms shipments to Kyiv. Early 2025 brought waves of coordinated disruptions against logistics and aviation networks in Europe, showing growing precision and organization behind these “hacktivist” campaigns.

The United States and Canada have also reported incidents where pro-Russian actors probed critical-infrastructure systems under the guise of hacktivism. Most recently, Canadian authorities warned that municipal control systems had been accessed through compromised interfaces, a sign that politically motivated operations can easily cross into national-security domains.

In 2023, Illia Vitiuk, head of cyber-security at Ukraine’s SBU, argued that genuine Russian hacktivism is mostly a myth. He claimed that over **90** percent of cyber-attacks on Ukraine are directed or sponsored by the state, with most so-called hacktivist groups serving as proxies for intelligence agencies. While the exact figure is definitely debatable, the overlap between state and hacktivist operations is undeniable.

This view is partly reinforced by Google’s 2024 report on APT44 (Sandworm), which detailed how the group leverages hacktivist fronts to amplify Russian state narratives.

*Sandworm (also known as APT44) blends traditional information-operations methods with hack-and-leak tactics. The group was posting sensitive documents or "proof" of operations on Telegram to maximise visibility, and it used now mostly defunct (maybe hacktivist-branded groups such as **XakNet Team**, **CyberArmyofRussia_Reborn1** and **SoIntsepek** to claim responsibility, tying those so called hacktivist channels into a wider state-linked ecosystem.*



***NoName057(16)** maintains near-daily activity across Ukraine and NATO networks and it stands out for its endurance: active for over three years and still highly operational after a temporary disruption during Operation Eastwood in mid-2025. Its quick resurgence and sustained attack tempo illustrate a level of coordination rarely seen among self-proclaimed hacktivists.*

Taken together, these examples show how Russian hacktivism has become a **state-aligned** ecosystem.

State Sponsored Hacktivism

Modern “hacktivism” is increasingly difficult to distinguish from state-sponsored espionage. What began as cyber protests has, in many cases, evolved into a new arm of government information warfare. Today, hacktivist tactics are used not only by independent collectives but also by state-aligned groups instrumentalizing cyber activism for geopolitical aims.

As we showcased a few examples, this phenomenon has been observed in conflicts like Russia’s war in Ukraine, where *patriotic* hacktivists on both sides carried out coordinated attacks benefiting their respective governments. As a study notes, “*the boundary between genuine digital activism, cybercrime, and covert state operations has increasingly blurred*" and "*states have learned to exploit hacktivism.*"

For example, the pro-Russian hacker group called “Cyber Army of Russia Reborn” (CARR) , allegedly an independent hacktivist group, was revealed to be linked to Russia’s GRU Sandworm unit.

Dark Web Profile: Cyber Army of Russia Reborn

Likewise, an Iranian hacker group dubbed “CyberAvengers” (or CyberAv3ngers) claiming activist motives was later tied to Iran’s Revolutionary Guard (IRGC).

Dark Web Profile: Cyber Av3ngers

Information Warfare Through Leaks

Breach-and-leak operations are cyberattacks meant to shape politics, not earn profit. Hackers break into targets, steal private data, and publish it to damage reputations or spread distrust. The aim is to influence public opinion, weaken faith in institutions, and create division.

These leaks often appear at moments of high tension, such as elections, wars, or diplomatic crises. Attackers pose as “hacktivists” to hide their real identities and avoid blame. The timing of these releases is deliberate, chosen to cause the most political harm or confusion.

History of "Hacktivist" Driven Political Cyber Leaks

Event	Actors / Methods	Impact
2016 U.S. election	Russia-backed groups using "Guccifer 2.0" and WikiLeaks to leak campaign emails	Influence voters, weaken trust in democratic processes
2024 U.S. election	Iran-linked APT42 hacked a presidential campaign and leaked emails under an "anonymous" persona	Disrupt campaign operations and sow political chaos
2017 French election	Russian GRU's "Fancy Bear" leaked internal party communications	Damage targeted candidates before the vote
Russia-Ukraine war (2022–)	Ukraine's "IT Army" vs. pro-Russian groups like KillNet and XakNet	Leak enemy data, shape wartime narratives
2014 Ukraine election	"CyberBerkut" used GRU-linked malware to post fake election results	Undermine election credibility and justify intervention
Israel–Hamas conflict (2023-)	Iran-aligned groups leaked Israeli data under hacktivist banners	Support Iran's stance and amplify propaganda
"Ghostwriter" campaign (Europe)	Belarusian unit working with Russia leaked doctored emails from NATO allies	Undermine pro-Western leaders, fuel division
Poland migrant crisis (2021)	Belarusian hackers posing as activists leaked false government files	Stir anti-immigrant sentiment and retaliate politically

Election Interference

Hack-and-leak has become a favored tactic around major votes. The paradigm was set in 2016, when Russia-backed actors famously hacked and leaked U.S. campaign emails via fronts like “Guccifer 2.0” and WikiLeaks. Similar methods persist. In the 2024 U.S. election cycle, an Iranian state-linked hacking unit (tracked as APT42, aka “Mint Sandstorm”) compromised multiple staffers of a presidential campaign and leaked their emails under an “anonymous” hacktivist. U.S. officials indicted three members of this Iranian group, alleging they acted on behalf of Iran’s IRGC to influence the election.

Conflicts and Military Escalations

After Russia’s 2022 invasion, Ukraine’s “IT Army” targeted Russian sites, while pro-Russian groups like KillNet and XakNet attacked Ukraine and its allies. Both sides leaked stolen data to embarrass opponents.

Many of these so-called hacktivists actually work with state agencies. For example, alleged hacktivists’ 2014 attack on Ukraine’s election system used malware tied to Russia’s GRU. Later, Mandiant linked groups like XakNet and CyberArmyofRussia_Reborn to the GRU’s Sandworm unit. These teams coordinate with Russia’s military goals, leaking stolen files through Telegram to spread propaganda while appearing independent.

Similar tactics appear elsewhere. During the 2023 Israel–Hamas war, many “hacktivist” attacks on Israeli systems were traced to Iran-aligned groups. Analysts found Iran used cyber operations and online propaganda together to support its position.

Diplomatic and Political Crises

Hacktivist-style leaks also appear during diplomatic disputes. Russia and Belarus have used such tactics to target European politicians and NATO members. The “Ghostwriter” campaign, traced to Belarusian forces, spread fake documents to damage pro-Western leaders. In 2021, false leaks from Poland’s government tried to stir anti-immigrant anger. These leaks exploit political friction, mixing truth with lies to divide societies.

Recommendations and Risk Forecast

A. Strategic Preparation

1. Recognize hacktivism as a persistent, political risk.
Hacktivist attacks now occur frequently and in response to real-world events. These can range from large-scale DDoS waves to symbolic defacements and targeted leaks. Even if your organization is not directly involved in conflict, political alignment or visibility can attract attention.

2. Prepare for multi-pronged incidents.
Modern hacktivist operations often mix tactics. A DDoS campaign may be paired with a website defacement or a data leak. Incident response plans should address combinations, not just isolated threats.

B. Operational Monitoring

3. Monitor Telegram, X, and mirrored sites.
Hacktivist groups announce targets, share tools, and claim attacks in open channels. Tracking these spaces, especially during heightened tensions, can give early warning of planned campaigns.

4. Watch for global ripple effects.
Attacks often spread beyond the conflict zone. For example, U.S. or European institutions may face retaliation simply for political statements or aid commitments elsewhere. Expect spillover.

5. Map symbolic exposure.
Hacktivists often seek visibility over impact. Review your digital presence (public-facing sites, social media, affiliated brands) for elements that could be interpreted as politically symbolic.

C. Communication & Resilience

6. Assume visibility, even for small incidents.
Even a short outage or minor breach might be claimed, amplified, and misrepresented by attackers. Having a clear public communication plan in place helps manage narratives.

7. Train for deflection, not just defense.
Technical defenses matter, but response time, message control, and digital hygiene can be just as critical when dealing with high-noise, politically charged threats.

Risk Forecast

- **More leak-based operations.** Political leaks will increase around global events, elections, wars, and summits.
- **Blurred actor lines.** Expect continued overlap between hacktivist branding and state involvement.
- **Hybrid campaigns.** Ransomware, DDoS, and leaks will increasingly mix in the same operations.
- **High noise, low clarity.** Attribution will remain hard. Some leaks may be staged or modified, and many actors will hide behind activist language to avoid blame.

Conclusion

Hacktivism today is not just digital protest. It is a tool used in conflicts and power struggles between states. Leaks that appear spontaneous often serve strategic goals. As the line between activism and espionage fades, defenders must stay alert—not just to who is attacking, but to **why** and **when**.

References

1. https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists
2. https://tdhj.org/blog/post/hacktivism-russia-cyber-strategy-2/
3. https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/
4. https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups
5. https://www.lemonde.fr/en/pixels/article/2025/06/20/who-is-gonjeshke-darande-the-group-behind-the-cyberattack-targeting-sepah-bank-in-iran_6742524_13.html
6. https://t.me/nnm05716english/40
7. https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf
8. https://revistacugc.es/article/download/7923/8900/34896
9. https://www.fastcompany.com/91191776/u-s-elections-four-cyber-threats-organizations-can-expect
10. https://www.nbcnews.com/tech/security/us-confirms-trump-campaign-claim-was-breached-iranian-hackers-rcna167285
11. https://www.theguardian.com/world/2025/apr/29/france-says-russian-hackers-behind-attack-on-macrons-2017-presidential-campaign
12. https://www.washingtonpost.com/world/europe/meta-belarus-kgb-poland-facebook/2021/12/02/ffaa73f8-534d-11ec-83d2-d9dab0e23b7e_story.html