Offense is the best defense

The Evolution of Ukrainian Cyber Capabilities and Lessons for Europe

Authors:

Bogdana SHYNKARENKO
Cybercrime analyst
Cybercrime Fighting Unit

Mael SARP
Threat Intelligence Team Leader
World Watch Team

Joseph MONTREY
Threat Intelligence Analyst
World Watch Team

Orange Cyberdefense's CERT brings together cyber experts across our Incident response and Digital Forensics (CSIRT), Cyber Threat Intelligence (CTI), Cybercrime and Vulnerability Operation Center (VOC) teams.

These experts work on the digital front lines against active cyber threats and attacker activity, contributing to Orange Cyberdefense's Intelligence-Led Approach to cybersecurity, ensuring our clients stay ahead of emerging threats and evolving attack techniques.

Introduction

Since 2014, Ukraine has been the target of persistent and sophisticated cyberattacks designed to disrupt its critical infrastructure, weaken its economy, and undermine public confidence. Now, after nearly four years of full-scale war and many prior of non-kinetic confrontation, **Ukraine's cyber defense architecture has evolved from an initially reactive posture into a robust, multi-layered system integrating civilian, military, and private-sector components.**

Cooperation between CERT-UA and MIL.CERT-UA, extensive technical assistance from international partners, and support from private technology firms have collectively strengthened the country's cyber resilience and crisis-time defense.

A pivotal moment in this development was the first parliamentary approval of a **dedicated Cyber Forces Command in October 2025.**[1] This new military branch, operating under the General Staff and the President's direct authority, will aim to institutionalize Ukraine's offensive and defensive cyber warfare capacity. It will standardize recruitment, training, and **align operational practices with NATO standards.**[2] This development reflects Kyiv's intent to formalize its expertise gained since 2014 and transition from ad hoc cyber defense to institutionalizing strategic cyber resilient structures.

Ultimately, this study provides a comprehensive understanding of how Ukraine's experience has **influenced global perspectives on cyber-enabled hybrid threats**, across both wartime and peacetime contexts.

From this analysis emerge critical lessons for Europe, highlighting the critical need to strengthen the cyber workforce, deepen cooperation between public and private sectors, and **adopt a political approach that treats cyber-enabled hybrid threats as a permanent and foundational element of the security landscape.**

This report accordingly analyzes the evolution of Ukraine's cyber capabilities from 2014 to 2025, examining both defensive and offensive dimensions. It will explore how Ukraine, supported by allied states and private partners, has built one of the most resilient and innovative cyber defense ecosystems in today's security landscape. Furthermore, it assesses how Ukraine's emerging offensive capabilities—developed through cooperation between state agencies, intelligence services, and pro-Ukrainian hacktivist groups—illustrate a new model of responding to hybrid warfare.

Note: the analysis cut-off date for this report was November 15, 2025. Cyber developments in the conflict are still being monitored and are the subject of specific weekly advisories.

Contextualizing hybrid warfare

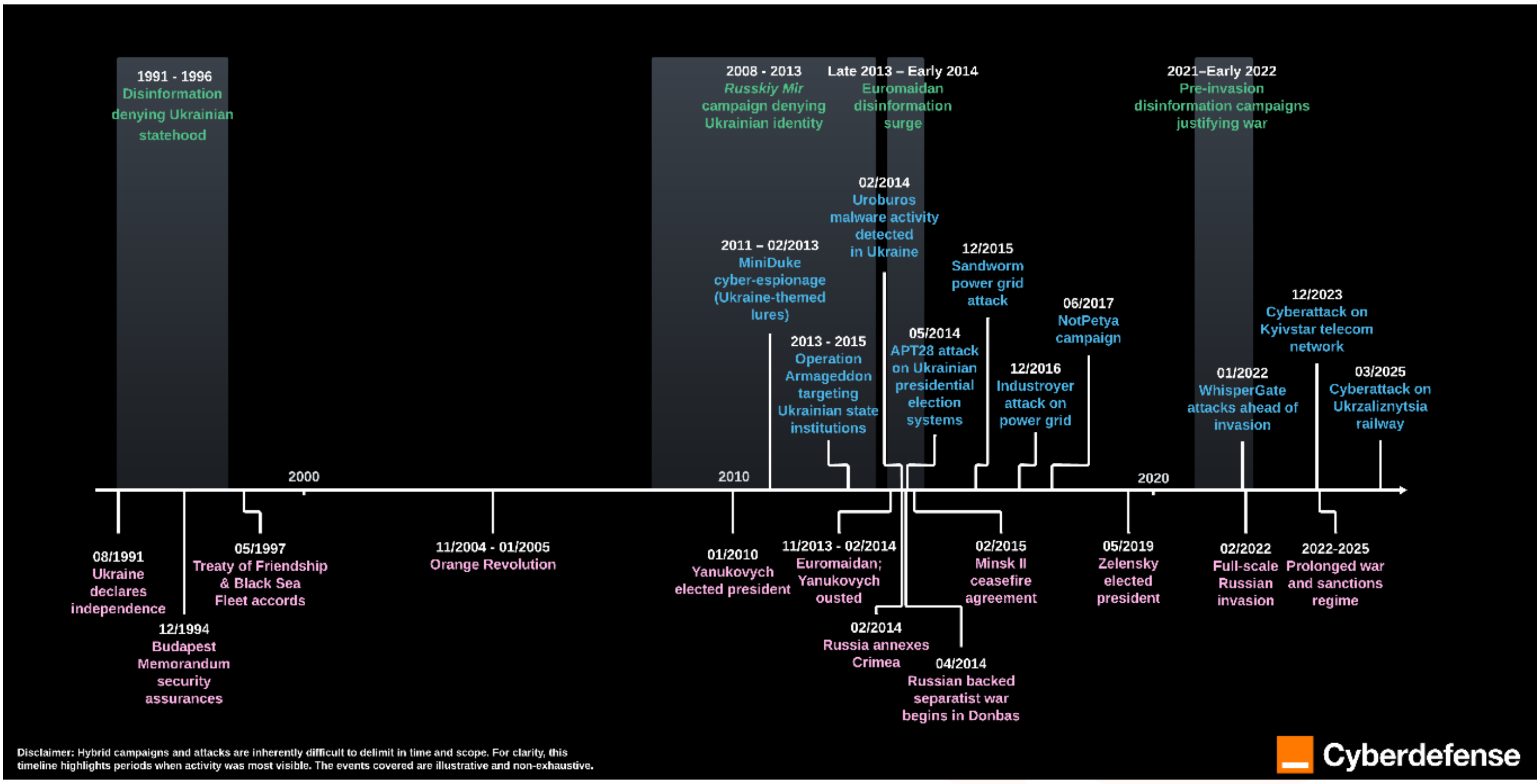
The term hybrid threats, and by extension hybrid warfare, has become central to contemporary discussions of war and security. Yet despite its frequent use, the concept often remains imprecisely defined. For the purposes of this study, **hybrid threats refer to the coordinated use of conventional and unconventional methods—both overt and covert, coercive and subversive—aimed at exploiting societal vulnerabilities**, as defined by NATO.[3]

These actions often, though not exclusively, rely on cyber operations to facilitate their effects. Beyond their physical consequences, hybrid threats aim to erode **public trust**, sow **confusion**, and fracture **social cohesion**—particularly within liberal democracies, which depend on confidence in institutions and elected officials more strongly than their authoritarian counterparts.

Within this framework, hybrid warfare can be understood as the application of hybrid threats in the context of an ongoing kinetic conflict. It represents the **fusion of digital, informational, and conventional domains** into a larger battlespace, where cyberattacks, disinformation, and military operations are coordinated to achieve strategic goals.

Following the Euromaidan uprising, Ukraine has become embroiled in a sustained hybrid conflict characterized by cyberattacks and disinformation campaigns, facilitated by cyber actors mobilized as tools of state influence. However, beginning with the Russian full-scale invasion launched in February 2022, the conflict crossed decisively into the realm of hybrid warfare.

Nearly four years later, the unprecedented scale and intensity of cyber operations have made the digital domain both **a battlefield and a laboratory for offensive and defensive innovation**. State and non-state actors now compete and collaborate across this space, redefining the contours of modern warfare.


1991 - 1996
Disinformation denying Ukrainian statehood
2008 - 2013
Russkiy Mir campaign denying Ukrainian identity
Late 2013 – Early 2014
Euromaidan disinformation surge
2021–Early 2022
Pre-invasion disinformation campaigns justifying war
02/2014
Uroburos malware activity detected in Ukraine
2011 – 02/2013
MiniDuke cyber-espionage (Ukraine-themed lures)
12/2015
Sandworm power grid attack
06/2017
NotPetya campaign
12/2023
Cyberattack on Kyivstar telecom network
2013 - 2015
Operation Armageddon targeting Ukrainian state institutions
05/2014
APT28 attack on Ukrainian presidential election systems
12/2016
Industroyer attack on power grid
01/2022
WhisperGate attacks ahead of invasion
03/2025
Cyberattack on Ukrzaliznytsia railway
2000
2010
2020
08/1991
Ukraine declares independence
12/1994
Budapest Memorandum security assurances
05/1997
Treaty of Friendship & Black Sea Fleet accords
11/2004 - 01/2005
Orange Revolution
01/2010
Yanukovych elected president
11/2013 - 02/2014
Euromaidan; Yanukovych ousted
02/2014
Russia annexes Crimea
04/2014
Russian backed separatist war begins in Donbas
02/2015
Minsk II ceasefire agreement
05/2019
Zelensky elected president
02/2022
Full-scale Russian invasion
2022-2025
Prolonged war and sanctions regime

Disclaimer: Hybrid campaigns and attacks are inherently difficult to delimit in time and scope. For clarity, this timeline highlights periods when activity was most visible. The events covered are illustrative and non-exhaustive.

Figure 1: Evolution of Ukraine-Russia relations and major cyber campaigns 1991-2025

Defensive capabilities

Defensive capabilities

From 2014 to 2022, Russia was a determined user of cyber-enabled hybrid threats for destabilization, intelligence gathering, and preparation for the battlefield in Ukraine.

Since February 2022, this trend has continued to grow, with Ukraine subjected to persistent and sophisticated cyberattacks aimed at disabling critical infrastructure, impacting military operations, and eroding public trust.[4]

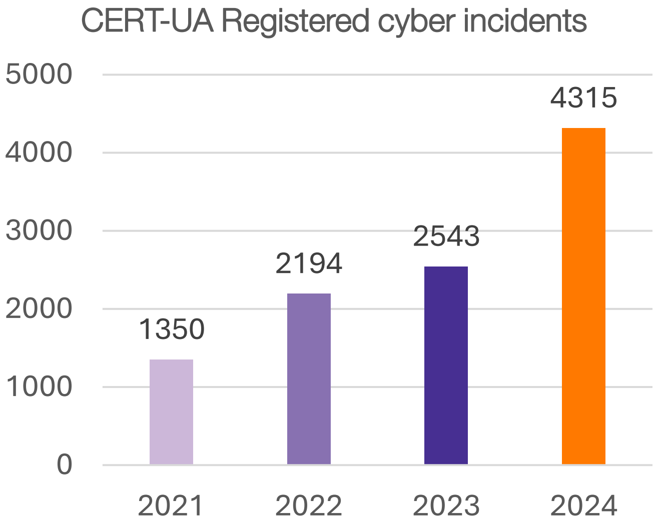


Figure 2: CERT-UA registered cyber incidents 2021-2024 | Source SSSCIP

One of the pivotal elements in Ukraine's cyber defense architecture against these attacks is the collaboration between the Government Computer Emergency Response Team of Ukraine (CERT-UA) and the Military Computer Emergency Response Team (MIL.CERT-UA) under the Ministry of Defense. This partnership reflects a **strategic and operational alignment aimed at enhancing national cybersecurity resilience** in the face of the ongoing war with Russia.

Created in 2007, **CERT-UA primarily focuses on protecting civilian government institutions**, local authorities, and critical infrastructure sectors such as energy, telecommunications, and transportation.[5]

In comparison, created in September 2024, **MIL.CERT-UA is dedicated to addressing cyber threats targeting military and defense-related assets**, including the Armed Forces of Ukraine.[6] This functional division allows both agencies to specialize in their respective domains while maintaining comprehensive coverage across the digital landscape.

Confronted with thousands of cyberattacks annually, Ukraine has accumulated significant operational experience, helping to protect itself against an ever-evolving cyber threat landscape. Despite yearly increases in the total volume of cyberattacks, according to data provided by the State Service of Special Communications and Information Protection of Ukraine, 59 critical and high-level incidents were recorded in 2024—a significant decrease compared to the 367 incidents in 2023.[7]

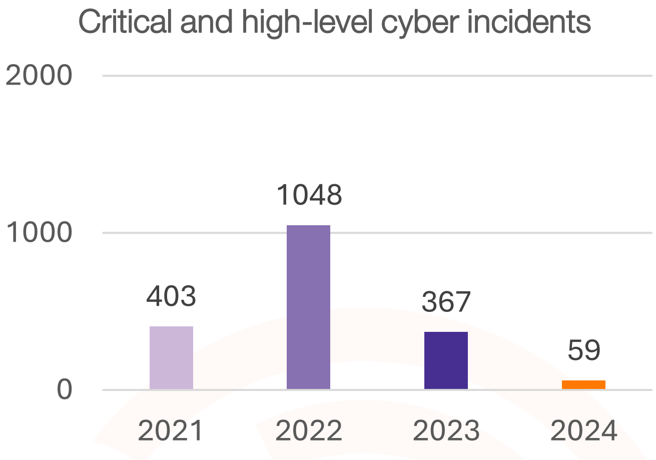


Figure 2: CERT-UA registered critical cyberattacks 2021-2024 | Source SSSCIP

This progress has been facilitated through support from international partners, particularly the United States, the United Kingdom, Canada, Poland, and the Baltic states, who provide direct technical assistance to Ukraine's cyber defense units.

This functional knowledge has been deeply integrated into the practices of Ukrainian cyber defenders. As a result, Ukraine has developed a **highly coordinated and multi-layered cyber defense structure**, strengthened by allied partners who contribute technical expertise, infrastructure security, intelligence sharing, and strategic capacity building.

This collaborative response has not only enhanced Ukraine's cyber resilience in real time but also shaped the global playbook for war-time cyber defense cooperation.

Support from allies

Ukraine has benefitted from a wide range of support from its allies, including but not limited to:

- The U.S. Cyber Command (USCYBERCOM) **"Hunt Forward" Operations**, which helped identify malware and suspicious network activity before they could impact Ukrainian systems, beginning in January 2022.[8]
- The EU Cyber Rapid Response Team (CRRT) activated on February 22, 2022, led by Lithuania and including experts from several member states, which worked with Ukraine to identify and mitigate active threats.[9]
- Ukraine was approved to join the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in March 2022.[10]
- Logistical and cyber incident coordination support from Poland, following a bilateral agreement signed in August 2022.[11]
- Cyber training platforms donated by Estonia, which also supported joint cyber defense exercises since December 2022.[12]

Beyond short-term incident response capabilities, allies have equally invested in Ukraine's long-term cyber capacity. A central pillar of that is the **Tallinn Mechanism**, a coordinated non-military cybersecurity support platform launched in December 2023 by eleven countries, including Ukraine, Estonia, Canada, Denmark, France, Germany, the Netherlands, Poland, Sweden, the United Kingdom, and the U.S., with the EU and NATO as observers.

Through this mechanism, donors have collectively raised over **€241,000,000** since its inception to fortify Ukraine's critical civilian cyber infrastructure.[13]
NATO's CCDCOE, to which Ukraine was granted full participation in 2023, has also served as a strategic platform for training and joint exercises. Ukrainian teams participated in Exercise **Locked Shields** 2024, the world's largest live-fire cyber defense simulation, gaining experience in defending complex critical infrastructure environments.[14]

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and UK's National Cyber Security Centre (NCSC) have additionally maintained regular information exchange with Ukraine's State Service of Special Communications and Information Protection (SSSCIP) and the Security Service of Ukraine (SBU). Many U.S.-led initiatives, including the **Cybersecurity for Ukraine program**, supported by the U.S. Agency for International Development (**USAID**), have trained thousands of cyber professionals and expanded cyber curricula at Ukrainian universities.[15] However, the funding freeze imposed by the Trump administration on USAID has raised operational questions for Ukraine, as it has previously contributed significant funding to support the resilience of Ukraine's telecommunications networks and cybersecurity.

Private support

Ukraine has also largely benefitted from the help provided by private cybersecurity firms. As of May 2025, the **Cyber Defense Assistance Collaborative** (CDAC), an industry-led volunteer network, has delivered over the equivalent of €35,500,000 in cyber defense tools to 25 Ukrainian entities via 32 private-sector companies.[16] Participating firms include Avast, Mandiant, Palo Alto Networks, Recorded Future, Symantec/Broadcom, and ThreatQuotient, among others. However, coordination challenges such as **fragmented communication, undefined requirements, and constrained staffing** have reportedly limited CDAC's effectiveness. initiatives.

Microsoft's Threat Intelligence Center (MSTIC), Mandiant (now part of Google Cloud), and Recorded Future have publicly acknowledged providing intelligence in near-real time, though the duration and full extent of this assistance remain unclear. [17,18,19] This has almost certainly enabled proactive defense measures across Ukrainian systems and allowed for rapid identification and neutralization of Russian cyber operations often timed to coincide with other physical or psychological operations (PSYOPS), complicated response efforts. Through their published analyses, these companies have also publicly exposed several Russian campaigns, including **WhisperGate**, **FoxBlade**, and **CadetBlizzard**.[20,21,22]

Microsoft, alongside Amazon Web Services, has additionally provided free and secure cloud services for over 60 Ukrainian government agencies.[23] This migration has not only prevented data loss from kinetic strikes, but also allowed for **scalability and redundancy**, key in ensuring operational continuity under crisis conditions. Alongside Palantir, these companies also played significant roles by offering cloud-based cyber analytics and threat modeling capabilities.

Google has likewise provided advanced threat intelligence and **anti-phishing support** to Ukrainian organizations, aimed at stopping the spread of misinformation and disrupting disinformation campaigns regularly targeting Ukraine.[24]
However, more than three years into the conflict, support from private organizations appears to be declining. Several factors may contribute to this trend, including Ukraine's strengthened digital resilience, the limited perceived impact of Russian cyber operations, donor fatigue among certain support providers, and a lack of dedicated funding for large-scale, systemic initiatives.

Evolution of Ukrainian cyber capabilities

In the immediate aftermath of large-scale campaigns launched by Russian APTs and hacktivist groups, Ukraine's cyber defense efforts were initially reactive. The Ukrainian government, working alongside private sector cybersecurity firms and international allies, focused primarily on limiting damage from these attacks. This began with the expansion of cyber defense forces, emphasizing rapid incident response teams (CSIRTs) and information-sharing protocols. This included the deployment of **advanced monitoring tools and threat intelligence platforms** to improve real-time detection and analysis of cyber threats. In 2023, to manage these responsibilities, the SSSCIP became the central authority coordinating cyber defense activities across government, military, and critical infrastructure sectors.[25]

This was followed by a broader shift toward the development of a more proactive cyber defense doctrine, improving resilience, deterrence, and offensive cyber capabilities as part of a comprehensive strategy to better protect Ukraine.

SSSCIP staff received cyber training programs, including from Western educational institutions, which helped professionalize the national cybersecurity workforce.[26]

By 2024, as demonstrated by the substantial decrease in critical cyber incidents reported by the SSSCIP, defensive Ukrainian cyber capabilities matured significantly, moving beyond reactive defense to proactive integrated cyber operations. The same year, Ukraine passed new legislation to strengthen the cyber resilience of national critical infrastructure. This law mandated comprehensive risk assessments, mandatory cybersecurity audits, and 24/7 security operations centers (SOCs) for all major public service providers.[27] **This legislative framework mirrors best practices from the EU's NIS2 Directive and has helped align Ukraine's cybersecurity posture with European standards.**

Meanwhile, Ukraine continued to participate in joint exercises with NATO partners, improving resilience against complex multi-vector cyberattacks and bolstered its ability to anticipate and counter emerging threats.[28] This new cyber strategy bolstered critical sectors, including energy, telecommunications, and finance, as organizations benefited from upgraded cybersecurity standards and incident response capabilities. The government also launched nationwide awareness campaigns to improve cyber hygiene among public institutions and citizens, mitigating social engineering and phishing risks.

The cyber defense of Ukraine has highlighted the growing interdependence between state and non-state actors in national security. This war has seen major tech firms become de facto cyber defense partners, with roles that blur the lines between civilian and military support. It has also underscored the need for agile, interoperable cyber defense postures that can respond dynamically to hybrid threats.

The cyber defense of Ukraine has highlighted the growing interdependence between state and non-state actors in national security. This war has seen major tech firms become de facto cyber defense partners, with roles that blur the lines between civilian and military support.

Ukraine's cyber resilience is not merely a result of defensive posture but of active, coordinated international cooperation, and the need for the need for an agile, interoperable cyber defense postures that can respond dynamically to hybrid threats. The joint response offers a model for how democracies can respond to state-sponsored cyber aggression—not just with technical tools, but with political will and strategic coordination.

Attacks against Kyivstar and Ukrzaliznytsia

Since 2022, multifaceted cyber campaigns have been waged against Ukraine's critical infrastructure. As a case study, the most significant targets have been Kyivstar, the nation's leading telecommunications provider, and Ukrzaliznytsia, the state-owned railway company. These attacks reflect a deliberate Russian effort to undermine both information flow and logistical mobility and demonstrate the increasing resilience of Ukraine,

MOST TARGETED SECTORS, 2021-2024

	2021	2022	2023	2024
	1350	2194	2543	4315
Public sector and local governments	20%	26%	25%	58%
Security and Defense Sector	16%	14%	7%	18%
Commercial Sector	6%	6%	5%	6%
Financial sector	6%	5%	4%	3%
Energy sector	3%	5%	4%	2%

Figure 3: Most targeted sectors in Ukraine since 2021 | Source: SSSCIP

In December 2023, a massive cyberattack on Kyivstar attributed to the Russian-state affiliated threat actor Sandworm disrupted mobile phone and internet services across Ukraine, affecting a total of nearly 24 million civilians and military personnel alike.[29]

The scale of the cyberattack suggests that Russia intended to sow confusion, diminish public morale, and impair Ukraine's command and control systems without deploying conventional armed forces. During a February 2024 cybersecurity event held in Kyiv, the CEO of Kyivstar, Oleksandr Komarov disclosed that **the adversary likely initially compromised an employee account before obtaining admin privileges.**[30] They then **gained control over the Active Directory** which enabled the launch of further malicious actions within the systems. Ukrainian authorities added that a second wave of the attack targeting physical infrastructures and specifically Kyivstar's base transceiver stations was prevented.

This attack exposed vulnerabilities within Ukraine's civilian infrastructure and demonstrated Russia's capacity to conduct complex, state-sponsored cyber operations.

The second massive campaign occurred on March 23, 2025, as Ukrzaliznytsia suffered a large-scale cyberattack that affected its online ticketing and freight systems.[31] The company was forced to revert to paper-based operations, and passengers were advised to purchase tickets on-site or aboard trains. The objective was to disrupt both passenger and military freight services, as rail transport is a vital for Ukraine's wartime logistics and economic sustainability.

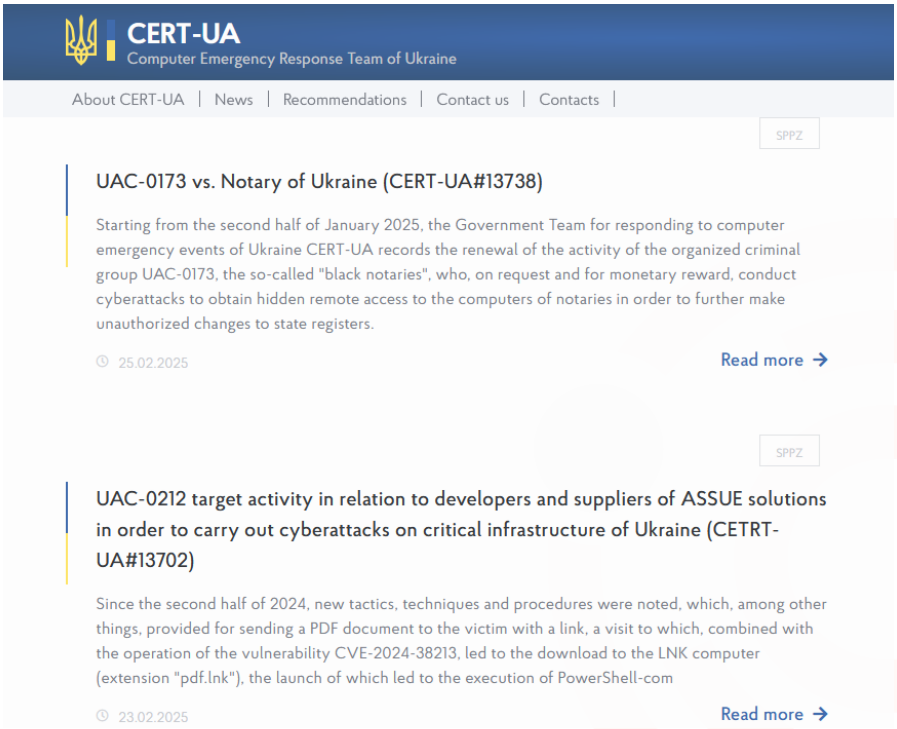
The restoration of services took 89 hours, with the involvement of Ukraine's Security Service (SBU) and CERT-UA. Despite the challenges induced by the attack, train operations continued as scheduled, and no sensitive information was reported as compromised.

When viewed together, the attacks on Kyivstar and Ukrzaliznytsia demonstrate a calculated Russian hybrid warfare strategy to erode Ukraine's ability to sustain defense efforts and maintain public order. However, Ukrainian cyber forces operationalized prior experience to contain the damage and reinforce system resilience.

Ukrainian communication strategy

Since 2022, one of the most distinctive features of Ukraine's approach to adapting its cyber defense posture has been the role of its national Computer Emergency Response Team (CERT UA), whose communication strategy represents an unusual—arguably unique—model of public cyber threat reporting under conditions of active conflict.

Contrary to the more cautious approaches adopted by many national cybersecurity agencies, **CERT-UA has consistently favored frequent, transparent, and technically detailed public disclosures** about cyber incidents. Over recent years, the agency has published a high volume of alerts and analyses, many of which include specific malware strains, indicators of compromise (IoCs), and attribution to known threat actors, often linked to Russian advanced persistent threats (APTs).


CERT-UA
Computer Emergency Response Team of Ukraine
About CERT-UA | News | Recommendations | Contact us | Contacts |
SPPZ

UAC-0173 vs. Notary of Ukraine (CERT-UA#13738)

Starting from the second half of January 2025, the Government Team for responding to computer emergency events of Ukraine CERT-UA records the renewal of the activity of the organized criminal group UAC-0173, the so-called "black notaries", who, on request and for monetary reward, conduct cyberattacks to obtain hidden remote access to the computers of notaries in order to further make unauthorized changes to state registers.

25.02.2025

UAC-0212 target activity in relation to developers and suppliers of ASSUE solutions in order to carry out cyberattacks on critical infrastructure of Ukraine (CETRT-UA#13702)

Since the second half of 2024, new tactics, techniques and procedures were noted, which, among other things, provided for sending a PDF document to the victim with a link, a visit to which, combined with the operation of the vulnerability CVE-2024-38213, led to the download to the LNK computer (extension "pdf.lnk"), the launch of which led to the execution of PowerShell-com

23.02.2025

Figure 4: Notices from the CERT-UA

This high level of transparency serves several key strategic functions:

- First, it facilitates rapid defensive action across sectors by providing organizations with the technical information needed to detect and mitigate ongoing threats. Beyond this, such communication acts as a form of strategic signaling—both to domestic audiences and international partners—positioning Ukraine as a capable, resilient, and analytically competent actor in cyberspace. CERT-UA's communications contribute to the construction of a national image that is technologically sophisticated and actively resisting Russian aggression, rather than merely reacting to it. This is especially significant in the context of hybrid warfare, where cyberattacks are not isolated incidents but exist embedded in broader campaigns of disinformation and psychological operations.

- Equally important is the tempo and timing of CERT-UA's communications. In contrast to the retrospective analysis that characterizes many Western cyber incident reports, Ukrainian authorities frequently issue warnings and technical advisories in near-real time—occasionally even while attacks are ongoing. This has operational advantages as it encourages immediate collaboration with foreign technical partners and potentially disrupts adversary operations by revealing detection.

However, the model is not without limitations. **The sheer volume of alerts may produce information fatigue among domestic and international audiences**, diluting the urgency of individual communications. Moreover, the rapid pace of publication risks inaccuracies or premature attributions.

Offensive capabilities

Ukraine's offensive cyber posture

State–Hacktivists Cooperation: A new model of hybrid warfare

Since 2022, Ukraine's cyber posture has gone beyond mere defense against Russian aggression. This effort has pioneered innovative forms of **offensive cyber mobilization**, where state institutions and civilian volunteers converge in unprecedented ways. A striking example is Ukraine's Main Directorate of Intelligence (HUR), which not only conducts covert cyberattacks, but also overtly **collaborates with pro-Ukrainian hacktivist groups** and claims responsibility for select operations.[32]

This represents a radical departure from traditional intelligence practices, mirrored by the formal recognition of foreign hacktivists by the Ukrainian military. In April 2024, (BBC, 2024) members of the One Fist collective—hacktivist volunteers from eight different countries, including the U.S., U.K., and Poland—received official commendations from Ukraine's Air Assault Forces for their cyberattacks on Russian defense companies and surveillance systems.

For the Ukrainian state, hacktivists primarily expand the scope and scale of cyber operations, leveraging diverse expertise and additional manpower to amplify impact. They also provide Kyiv with the option to manage **plausible deniability** when strategic discretion is required. These activities have **blurred the line** between national defense and grassroots digital resistance, creating a uniquely Ukrainian model of offensive cyber warfare.

The most recent step in the evolving relationship between state institutions and non-state cyber actors is the proposed creation of a Cyber Forces Command, approved in its first parliamentary reading in October 2025.[33] This new branch, under the General Staff and the President's authority, aims to formalize Ukraine's offensive and defensive cyber capabilities, standardize recruitment and training, and align operations with NATO norms. Importantly, it would also establish cyber reserves that do not require traditional military conscription and allow temporary, mission-based service—opening a legal pathway for skilled civilians, including hacktivists, to collaborate with the state within a formal structure. This reflects Kyiv's intention to permanently integrate non-state expertise into its strategic cyber architecture.

Together, these developments demonstrate how **hacktivism has become a central pillar of Ukraine's offensive cyber strategy** in wartime. Hacktivist groups operating in direct or tacit cooperation with HUR have expanded Ukraine's capacity to disrupt Russian critical infrastructure and military-industrial networks, multiplying the reach of operations beyond what formal state institutions could achieve alone. The following sections examine these collaborative relationships in detail.

The Main Directorate of Intelligence of the Ministry of Defence of Ukraine (HUR)

The Main Directorate of Intelligence of the Ministry of Defence of Ukraine (HUR) plays a pivotal role in Ukraine's offensive cyber warfare efforts. As the primary military intelligence agency, HUR operates under the Ministry of Defence and is integral to Ukraine's national security apparatus.

Since 2022, HUR has executed over a hundred large-scale cyber operations within Russian territory. These operations have targeted key sectors, including banking, energy, telecommunications, and the defense industry.[34]
HUR's cyber operations are characterized by their strategic objectives:

- Disruption of military operations: by targeting communication and surveillance systems, HUR impedes Russian military coordination and logistics.
- Intelligence collection via cyberespionage: the agency steals and analyzes sensitive data to inform the Ukrainian government on subjects such as on Russian troop movements, operational plans, and potential vulnerabilities.
- Impact critical infrastructure: attacks on energy and financial systems aim to weaken Russia's internal stability and morale.

These cyber activities are often coordinated with other Ukrainian entities, such as the Security Service of Ukraine (SBU), and have increasingly involved collaboration with volunteer hacktivist groups.

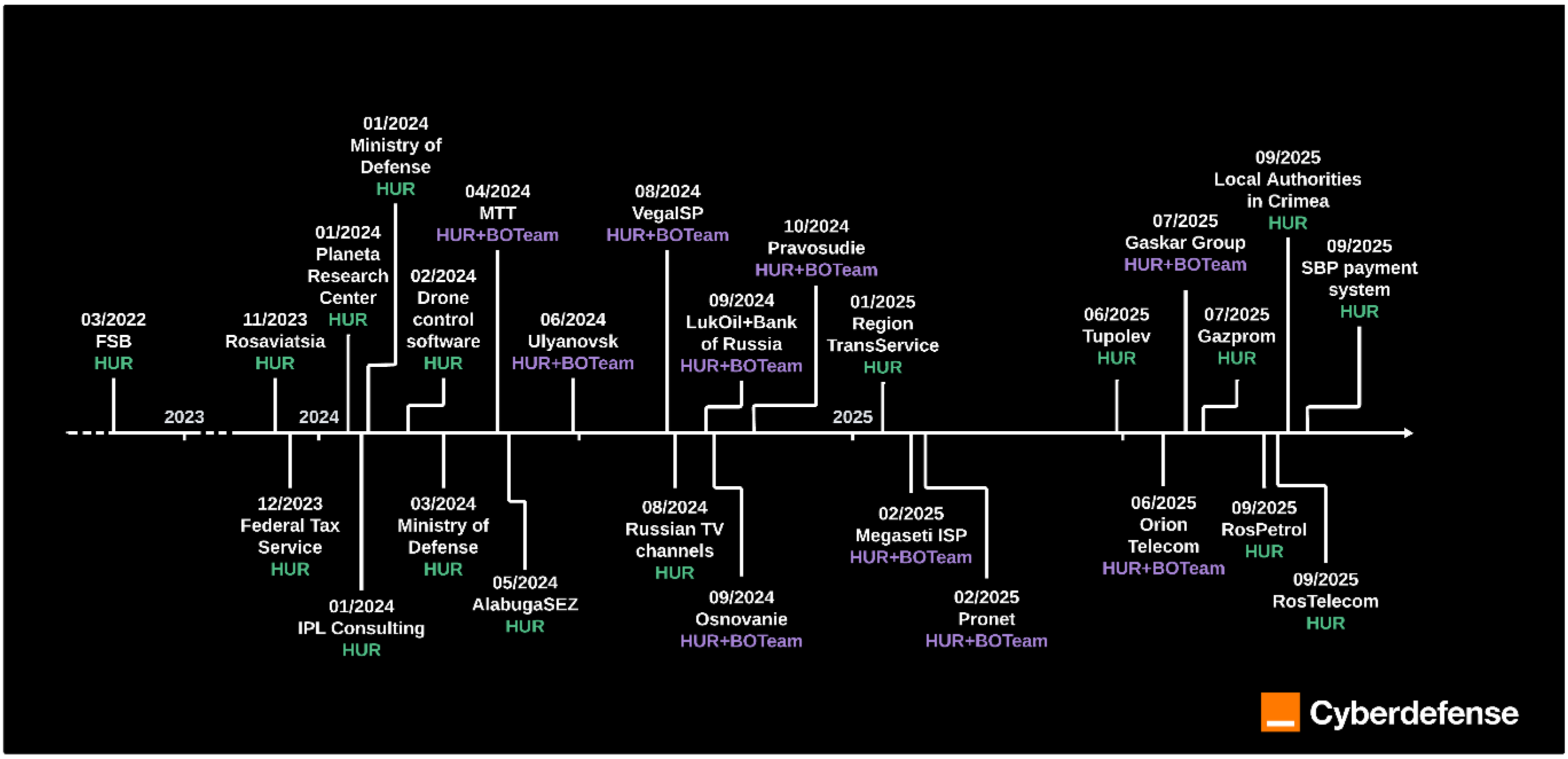

03/2022 FSB HUR
2023
11/2023 Rosaviatsia HUR
12/2023 Federal Tax Service HUR
2024
01/2024 Planeta Research Center HUR
01/2024 Ministry of Defense HUR
01/2024 IPL Consulting HUR
02/2024 Drone control software HUR
03/2024 Ministry of Defense HUR
04/2024 MTT HUR+BOTeam
05/2024 AlabugaSEZ HUR
06/2024 Ulyanovsk HUR+BOTeam
08/2024 VegaISP HUR+BOTeam
08/2024 Russian TV channels HUR
09/2024 LukOil+Bank of Russia HUR+BOTeam
09/2024 Osnovanie HUR+BOTeam
10/2024 Pravosudie HUR+BOTeam
2025
01/2025 Region TransService HUR
02/2025 Megaseti ISP HUR+BOTeam
02/2025 Pronet HUR+BOTeam
06/2025 Tupolev HUR
06/2025 Orion Telecom HUR+BOTeam
07/2025 Gaskar Group HUR+BOTeam
07/2025 Gazprom HUR
09/2025 RosPetrol HUR
09/2025 Local Authorities in Crimea HUR
09/2025 RosTelecom HUR
09/2025 SBP payment system HUR
Cyberdefense

Figure 5: Claimed cyberattacks by HUR against Russian targets

Key hacktivist actors in Ukraine's cyber ecosystem

Alongside formal agencies like HUR, a wide array of **volunteer cyber collectives** has become integral to Ukraine's offensive cyber environment. This has enabled a new model of cyberwarfare, underpinned by a fluid structure that enables frequent intersections across joint operations, collectively forming a layered **offensive framework that integrates sabotage** capabilities, **intelligence collection** through cyberespionage, and amplified informational impact.

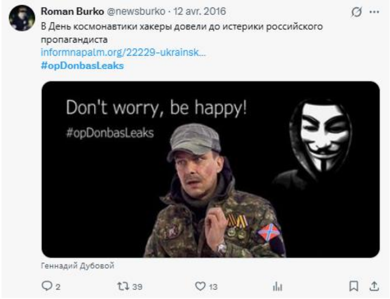
Ukrainian Cyber Alliance (UCA)

The Ukrainian Cyber Alliance (UCA) is one of the longest-standing and one of the most structured Ukraine-aligned hacktivist collectives. Formed in 2016 through the merger of legacy Ukrainian hacktivist groups FalconsFlame and Trinity, later joined by RUH8 and CyberHunta, UCA inherited networks and experience dating back to 2014, when Ukrainian cyber hacktivists first confronted Russian interference following the annexation of Crimea.[35]

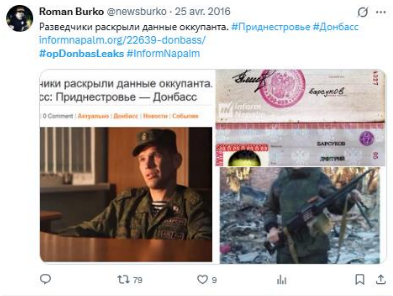
Early campaigns such as #OpDonbasLeaks and the 2016 SurkovLeaks exposed internal correspondence from the Kremlin adviser Vladislav Surkov and made public Moscow's coordination of separatist groups in eastern Ukraine.[36] These operations gave UCA international visibility and positioned it as a precursor to state-aligned cyber resistance.

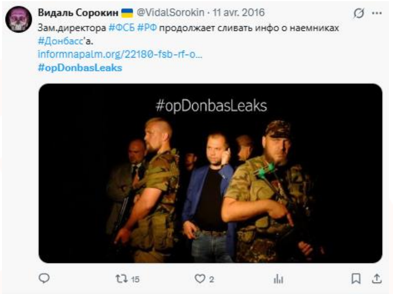
Initially acting independently, UCA's relationship with government institutions evolved gradually. Between 2014 and 2019, the group informally shared vulnerability data and compromised materials with trusted officers from the security and defense community.[37] In 2019, its members were invited to participate in discussions at the National Security and Defense Council (NSDC) to reform national information security policy and align it with the Ministry of Digital Transformation's digitalization plans.[38] Though these talks produced no structural reforms, they marked the first recognition of UCA as a legitimate civic partner rather than an illicit actor.

After February 2022, the Alliance shifted from public hack-and-leak operations to direct operational support for Ukraine's armed forces. As explained by UCA spokesperson Andrii Baranovych, **the alliance's objective was no longer to expose disinformation but to coordinate with the Ministry of Defense, the SBU, and the National Cybersecurity Coordination Centre** to deliver exfiltrated data that could assist kinetic or counter-intelligence operations.[39] The group also engaged in improving coordination between hacktivists to prevent multiple Ukrainian actors from compromising each other's access within the same Russian systems—a recurring issue during the chaotic volunteer mobilization of 2022.


Roman Burko @newsburko · 12 avr. 2016
В День космонавтики хакеры довели до истерики российского пропагандиста
informnapalm.org/22229-ukrainsk...
#opDonbasLeaks

Геннадий Дубовой
2 39 13


Roman Burko @newsburko · 25 avr. 2016
Разведчики раскрыли данные оккупанта. #Приднестровье #Донбасс
informnapalm.org/22639-donbass/
#opDonbasLeaks #InformNapalm
чики раскрыли данные оккупанта.
сс: Приднестровье — Донбасс
0 Comment | Актуально | Донбасс | Новости | События
Барсуков
БАРСУКОВ
ДМИТРИЙ
79 9


Видаль Сорокин 🇺🇦 @VidalSorokin · 11 avr. 2016
Зам.директора #ФСБ #РФ продолжает сливать инфо о наемниках #Донбасс'а.
informnapalm.org/22180-fsb-rf-o...
#opDonbasLeaks

15 2

Today, the UCA appears to function as a semi-formal component of Ukraine's broader cyber-resistance architecture. Now registered as an NGO (EDRPOU 43305353), it combines civic legitimacy with offensive capacity and proven coordination with national authorities.[40] UCA embodies the evolution of Ukrainian hacktivism from spontaneous activism into structured digital intelligence support. Its trajectory demonstrates how volunteer expertise, when effectively integrated into national defense, can transform dispersed hacktivist energy into sustained strategic capability.

The IT Army of Ukraine: State-aligned mass hacktivism

Launched on February 26, 2022, by Minister of Digital Transformation Mykhailo Fedorov, the IT Army of Ukraine was the first openly state-initiated and publicly coordinated effort to mobilize civilians for offensive cyber.[41] Within days, its official Telegram channel gathered over 250,000 volunteers. Under the coordination of the Ministry, participants conducted DDoS attacks and website defacements against Russian state institutions including the Kremlin and State Duma portals, major banks such as Sberbank and VTB, and media outlets like TASS and RIA Novosti.

The IT Army functions as a two-tiered structure:

- An outer circle of anonymous volunteers executing **mass DDoS campaigns** and disruptive attacks.
- An inner circle of semi-professional hackers capable of **intrusions, data theft, and information operations**, occasionally acting on assigned tasks in coordination with Ukrainian intelligence—such as receiving target lists or timing guidance.

This structure differs sharply from earlier understandings of hacktivism, which was more commonly decentralized, protest-driven, and anti-establishment. As George & Leidner (2019) categorizes, hacktivism has historically taken three forms—cyberterrorism, civic hacking, and patriotic hacking.[42] Ukraine's IT Army represents a new model of patriotic hacktivism: openly endorsed by the state, embedded in a defense strategy, and mobilized as a tool of hybrid warfare.

BO Team

BO Team, also known as Black Owl, emerged between late 2023 and early 2024 as one of the most technically sophisticated pro-Ukrainian hacktivist groups.[43] The group is characterized as a major threat to Russian organizations due to its unusual combination of techniques, tactics and procedures (TTPs) and its comparatively autonomous operating style within the pro-Ukraine hacktivist ecosystem. The group's operations consistently combine infiltration, espionage, and system destruction, often in coordination with the HUR.

Notably, **BO Team was involved in major infrastructure disruptions such as the Russian Railways and Orion Telecom incidents**, where the group's use of data wiping, destruction, and selective encryption of core servers and network assets turned cyber intrusions into tangible operational paralysis—disabling communications, crippling logistics systems, and halting essential services across multiple regions.[44]

Initial access for attacks is generally obtained through **spear-phishing** or **social-engineering, impersonating credible industrial or financial partners**. BO Team then deploys paid commodity tools such as **Remcos** and **DarkGate**, and its proprietary BrockenDoor malware, while relying on **legitimate Windows utilities such as PowerShell, WMIC, and msiexec** to blend in with normal activity. Investigations additionally attribute the systemic use of SDelete to erase host systems and backups to the group, complemented by the occasional deployment of the **Babuk ransomware to hinder recovery.**

BO Team's targeting strategy reflects a calculated focus on infrastructure supporting Russia's military-industrial complex. The group has repeatedly struck telecommunication and regional ISP networks including MTT/MTS, Orion, Vega, Megaseti, and Pronet/CWN to disrupt communications and logistics; energy and financial entities, including Lukoil, to generate economic friction; and scientific and defense-industrial assets such as the Planeta Space Hydrometeorology Center, whose data underpins Russian military planning. These attacks are designed not merely to cause disruption, but to degrade Russia's command, control, and production capabilities—key enablers of its operations in Ukraine.[45]

From 2024 to 2025, a clear pattern of synchronized or jointly claimed operations emerged, suggesting a pragmatic division of labor: the HUR defined strategic objectives and timing, while BO Team executed the technically demanding intrusions. This arrangement provided mutual advantages—state agencies extended their operational reach and maintained plausible deniability, while hacktivists gained access to intelligence support and mission relevance.

Even where the HUR acts independently—as during the September 2025 attacks on Russia's fuel-card networks, K-Corp Telecom, and the Central Election Commission—the techniques and effects closely mirror BO Team's methodology, underscoring a shared doctrinal evolution within Ukraine's offensive cyber sphere.[46]

Cyber Resistance

Cyber Resistance stands out within Ukraine's hacktivist landscape for its emphasis on cyberespionage rather than destructive operations. Its activities center on covertly penetrating the communication systems, email accounts, and internal servers of Russian defense contractors, paramilitary structures, and political or ideological institutions aligned with the Kremlin.

One of the group's most significant operations was the hack of the Russian drone manufacturer Albatross, during which Cyber Resistance exfiltrated approximately 100 GB of technical documentation, internal correspondence, and UAV schematics. The material was subsequently processed in cooperation with the open-source intelligence (OSINT) community InformNapalm, highlighting the group's role as a supplier of intelligence that can be transformed into actionable insights for Ukraine's defense sector.[47] In February 2025, the group provided access to the mailbox of Yuri Pavlenko, head of Military Representative Office No. 243 of the Russian Ministry of Defense. The leaked correspondence, contained sensitive information on naval construction, ship maintenance, and procurement channels, offering Ukraine a unique perspective on Russia's military-industrial vulnerabilities in the face of international sanctions.[48]

Cyber Resistance has also demonstrated a capacity for strategic information operations. In early 2025, the group announced a coordinated campaign against foreign firms continuing to supply components to Russia's defense industry, publishing technical documentation on the Kh-32 cruise missile and its modifications.[49] The leaked files showed that the weapon system is impossible to manufacture without imported components, primarily sourced from Western suppliers.

The operation, which reportedly lasted over a year, provided data to help block intermediary companies and expand international sanctions. According to Cyber Resistance, the campaign contributed to delays of four to six months in Russia's missile production program, disrupting planned strikes on Ukraine's energy infrastructure and directly saving civilian lives.[50]

Through these operations, **Cyber Resistance has positioned itself as a clandestine intelligence channel within Ukraine's hacktivist ecosystem**, providing sensitive data that supports both military decision-making and information campaigns aimed at undermining Russian resilience.

KibOrg

KibOrg emerged as a prominent actor after Russia's full-scale invasion in 2022, though it traces its roots back to the annexation of Crimea in 2014. The collective defines itself as a network of journalists and IT specialists who combine hacking with **OSINT investigations to expose Russian war crimes, collaborators, and disinformation campaigns.**[51] Often described under the symbolic label of "Legendary Cyborgs"—a name recalling the Ukrainian defenders of Donetsk airport, who became national heroes for defending the airport from May 2014 to January 2015 against overwhelming Russian-backed forces during one of the most brutal battles of the war in Ukraine's Donbas region. KibOrg positions itself as a hybrid between a hacktivist group and an investigative newsroom, curating and contextualizing stolen data to maximize informational impact.

In December 2022, KibOrg released intercepted documents from the Russian official Federal Security Service (FSB) in Crimea, revealing property nationalizations, the residences of FSB officers, and facilities under FSB control.[52] In early 2023, the group published data from the Dovzhansky–Novoshakhtynsk customs checkpoint in occupied Donbas, exposing illicit coal exports and identifying officials implicated in contraband flows.[53]

KibOrg's history of large-scale data leaks and investigative hacks culminated in March 2023, when the group released 500GB of data from Roskomnadzor, Russia's internet and media censorship authority. The files included internal correspondence, censorship directives, and references to opposition figures such as Alexei Navalny, providing unprecedented insight into the machinery of Russian state censorship.[54] That same spring, KibOrg leaked personal data on more than 600,000 Russian conscripts, extracted from government servers, offering rare visibility into Russia's personnel mobilization system.

Beyond these data-driven operations, KibOrg has also engaged in investigations of humanitarian impact. According to an in-depth report by The Independent, one of KibOrg's central missions has been tracing Ukrainian children abducted and deported to Russia, with the group claiming to have identified the whereabouts of at least 160 missing children in its initial efforts.[55] To support of this mission, KibOrg states that it shares its findings not only with Ukraine's Security Service (SBU) and the HUR but also with international bodies such as the International Criminal Court (ICC) and the United Nations. This positioning underlines its dual role as both a hacktivist entity and a contributor to war crimes investigations.

In July 2025, KibOrg has recently expanded its focus to the economic domain with the project "Pirates of the Azov Sea", documenting how Russian authorities systematically steal Ukrainian grain from occupied territories with the assistance of foreign intermediaries. This case illustrated KibOrg's ability to merge leaked documentation, OSINT techniques, and narrative reporting into a comprehensive exposé carrying significant diplomatic and economic weight.[56]

While other Ukrainian hacktivist groups primarily disrupt military systems or intelligence networks, KibOrg leverages its hybrid model to target humanitarian, economic, and diplomatic dimensions of the war. KibOrg challenges not only Moscow's occupation structures but also the legitimacy of its actions on the international stage.

COORDINATED OPERATIONS AND STRATEGIC TARGETS

December 2023
Attacks on **Russian telecom companies** following the Kyivstar hack to impose tangible costs on Russian infrastructure while undermining public trust in communication networks.

July 2024
After numerous hacks by Russian-linked hackers targeting Ukrainian **banks and government** platforms, HUR and UCA attacked Russian financial institutions.

June 2025
A DNS-layer strike that disabled the rzd.ru domain and its subdomains crippled Russian **Railways' ticketing and logistics systems**, degrading military supply chains and exposing critical vulnerabilities in state infrastructure; the operation was attributed to the HUR with techniques and timing suggesting BO Team served as the execution arm.

June 2025
Attacks on **Orien Telecom servers and switches** in a uranium-mining locality caused regional internet blackouts and wiped backups in Siberia, disrupting military-adjacent industrial operations and sowing fear about the security of sensitive sectors.

July 2025
A HUR-led cyberattack paralyzed governance in occupied Crimea by exfiltrating 100 TB of classified files, including troop logistics data, before **all government servers were destroyed**, dismantling occupation authorities' control and delegitimizing Russian authority over the annexed territory.

September 2025
Large-scale DDoS attacks disrupted RosPetrol fuel-card systems and servers of Rostelecom and Lukoil, inflicting ~€850,000–€2,500,000 in financial damage and disrupting **critical energy and telecom services**.

September 2025
A HUR attacks on **financial payment operator** K-Corp's digital infrastructure serving small arms producer Kalashnikov Concern destroyed key hardware and were followed by numerous website defacements celebrating Ukraine's Military Intelligence Day, degrading military supply chains and challenging Russian backed war narratives.

September 2025
Coordinated cyberattacks by the HUR on the **Central Election Commission servers**, Remote Electronic Voting platform, Rostelecom backbone routers, and Gosuslugi portal disrupted voting nationwide and in occupied territories, challenging the illegitimate electoral processes electoral legitimacy.

Coordinated operations and strategic targets

Beyond tradecraft and actors, the strategic objectives driving Ukrainian attacks align with those classically associated with hybrid threats, employing both coercive and subversive strategies to erode public trust, sow confusion, and fracture social cohesion. Coercively, Ukrainian cyber operations frequently target critical industries and supply chains sustaining the Russian military-industrial complex through direct cyberattacks. Subversively, tactics include reciprocity, cyberespionage to gather intelligence for future use, and the strategic targeting of administrative and civic infrastructure to erode social cohesion and confidence in institutions.

These subversive efforts effectively delegitimize occupation, annexation efforts, and even the broader motivations driving the conflict.

By combining these objectives, Ukraine maximizes the effectiveness of its cyber operations.

Notably, through these attacks, **Ukraine further blurs the line between covert and overt cyber operations**, a common trait of hybrid operations. Actions that historically used traditionally clandestine tradecraft like cyberespionage are now seen publicly claimed by official entities in official channels to maximize psychological effect against the Russian authorities and public. However, by collaboration with non-state hacktivist actors, the state preserves plausible deniability when its targets fall into legally or politically sensitive categories, such as elections. This dual model not only makes Ukraine's cyber operations more effective by enabling tailored attribution, messaging, and political exposure for different audiences, but also strengthens its ability to shape and defend its information environment, reducing the impact of Russia's own hybrid influence and intimidation efforts.

In contrast, a striking dimension of these operations also lies in how they are acknowledged—or denied—by Russia itself. In several cases, **Moscow was forced to admit the scale of disruption**. Following the June 2025 attack on Russian Railways (RZD), the company's own press service confirmed the collapse of ticketing and logistics systems. Likewise, officials in occupied Crimea admitted that public services would remain offline for an "indefinite period" after the July 2025 wipe of government servers.[57]

Even high-level officials have been forced to publicly acknowledge cyberattacks; Ella Pamfilova, Chair of the Central Election Commission, stated that "the CEC building has no internet—an attack is underway".[58]

Roskomnadzor also confirmed a "network degradation" affecting Rostelecom's backbone, underscoring the tangible impact of Ukraine's cyber operations.[59]
However, the official FSB website occasionally attributes certain attacks explicitly to Ukraine, while emphasizing that these activities were stopped by Moscow. For example, on March 6, 2025, the FSB announced that it had thwarted a HUR-led operation allegedly aimed at stealing personal data from Moscow students to "recruit" them, framing it as part of a wider NATO intelligence plot.[60]

These narratives, ranging from partial acknowledgment to outright denial or manipulation, illustrate the significance of controlling the informational dimension of cyberwarfare. Recognition and attribution can signal the scale of damage, while claims that certain activities were stopped help project control and resilience, despite serving as indirect validation of an operation's effectiveness.

A Ukrainian model of responding to hybrid warfare

Between 2022 and 2025, Ukraine's offensive cyber capabilities have evolved from volunteer-driven DDoS campaigns to sophisticated, state-coordinated joint operations. Groups such as BO Team, the UCA, and Cyber Resistance operated alongside the HUR to disrupt Russian telecommunications, transport networks, financial institutions, judicial systems, and segments of the defense-industrial complex.

These developments reveal two defining dynamics shaping Ukraine's approach to offensive cyber warfare:

- A strategy of sectoral symmetry, in which Kyiv responds to Russian cyber and kinetic attacks by targeting corresponding sectors inside Russia, reinforcing the notion of proportional retaliation and strategic balance.
- The emergence of a hybrid offensive model, where civilian cyber collectives amplify state operations while remaining legally unrecognized.

Ukraine's experience demonstrates how modern war can harness both state cyber commands and decentralized digital volunteers. This synergy has expanded Kyiv's capacity to inflict strategic damage in cyberspace, while also **challenging existing legal frameworks** under international humanitarian law and the future governance of cyber conflict.

Understanding a Post-War Landscape

Navigating Ukraine's Post-War Future

As kinetic fighting in Ukraine eventually subsides, the country must be prepared for a persistent cyber threat environment. Russia's hybrid operations will almost certainly continue regardless of battlefield conditions. Therefore, **Kyiv must treat cyberspace as a permanent front**: connected to but distinct from kinetic operations. Any post-war national security strategy should assume that cyber threats will remain an enduring dimension of geopolitical competition.

Accordingly, in a post-kinetic period, Ukraine's priority must be to maintain alignment through formal cooperation with its allies, institutionalize the most effective structures built during wartime, and address long-term cyber workforce resilience.

Regardless of Ukraine's post-war membership status in NATO and the European Union, maintaining deep integration with Western cyber frameworks will remain essential. Though Ukraine already aligns with parts of the EU's NIS2 directive and participates in EU cyber dialogues, post-war priorities should include continued adoption of EU regulations on critical infrastructure and telecommunications, participation in NATO cyber exercises, and integration into joint incident-response mechanisms. This alignment can be further bolstered through joint drills liaison programs, after-action reporting, and integrated CERT networks, with other public and private sector partners.

Close alignment, even without formal membership in existing legal structures, will enhance interoperability with partners and anchor Ukraine within the broader architecture of collective defense, providing both protection and deterrence against future Russian cyber operations.

These relationships will not only strengthen Ukraine's post-war strategic position but also offer partners meaningful returns on their wartime investments by enabling the exchange of experience with a war-tested cybersecurity ecosystem.

Such partnerships also underscore the need to permanently institutionalize Ukraine's rapidly constructed wartime cyber structures, many of which were initially improvised to counter Russian aggression. While the end of kinetic fighting and growing war fatigue could otherwise erode these institutions, those responsible for cyber defense must be preserved and formalized. Ensuring permanent fiscal backing to the Cyber Force within the armed forces would consolidate currently dispersed efforts into a coherent military service, streamlining recruitment, training, and doctrine development.

Sustaining a standing cyber force in peacetime would help refine operational standards, preserve hard-won institutional knowledge, and reduce reliance on unregulated volunteer structures. Likewise, dedicated counter-disinformation bodies must remain central to Ukraine's strategic communications architecture. Wartime innovations, such as fact-checking platforms, media-literacy initiatives, and anti-disinformation centers, should be strengthened in peacetime to ensure that Ukraine continues to take a proactive, rather than reactive, approach to countering hybrid threats.

Finally, maintaining and subsequently strengthening the foundation of Ukraine's cyber ecosystem requires a resilient and well-supported cyber workforce.

The war has already driven significant emigration and mobilization within the numerous job sectors, creating acute shortages across multiple key sectors, including cybersecurity, engineering, and IT roles.

Some companies have moved research and development abroad, only to see employees remain overseas for safety and stability. After the kinetic conflict ends, this dynamic may intensify as war-tested professionals receive attractive offers to take their expertise elsewhere. This level of sustained talent loss risks weakening Ukraine's long-term cyber-industrial base and eroding hard-won institutional knowledge. To counter this, policymakers must prioritize talent retention and workforce regeneration, reinforce existing initiatives, and create new programs where needed. Ensuring a robust cybersecurity workforce becomes a central pillar of Ukraine's post-war national strategy is essential for long-term resilience and security.

Europe's Post-War Priorities

While Ukraine remains the current primary target of Russian aggression, Moscow's hybrid campaigns are neither geographically bounded nor temporally constrained. In recent years, Europe has experienced a rising tempo of cyber intrusions, sabotage of critical infrastructure, disinformation operations, and covert activity aimed at undermining political stability.

Incidents such as coordinated influence operations during elections, probing of energy and telecommunications infrastructure, and persistent cyber espionage campaigns against government and private sector targets underline a simple reality: the tactics used relentlessly against Ukraine, have never been exclusive and are now being replicated across the continent.

Ukraine's experience is not only a case study, but an early warning of the hybrid threat landscape Europe should treat as a permanent strategic condition.

This means recognizing that hybrid operations do not follow the rhythm of conventional conflict and that they should not be viewed as rare deviations from normal security conditions. They thrive in peacetime specifically because democratic systems must balance diverse public priorities, which makes governments less continuously focused, less coordinated, and slower to mobilize across sectors compared to their authoritarian counterparts.

Urgent lessons from Ukraine's wartime adaptation highlight the need to treat cyber-enabled hybrid threats as core security concerns, not niche technical challenges. To counter the weaknesses of democratic governance, Europe must become more alert, better coordinated, and faster in its responses. It must advance three strategic pillars: a stronger and more sustainable cyber workforce, more integrated collaboration across sectors and borders, and political determination to support decisive collective action.

Ukraine's experience has clearly demonstrated that a broad, robust cyber workforce is the single most important factor in sustaining societal resilience to cyber-facilitated hybrid threats. When companies, institutions, and public bodies all employ skilled cyber professionals, good practices become widespread, attack surfaces narrow, and adversaries face greater friction at every stage of their attack process

Enlarging university-level cybersecurity tracks, expanding apprenticeships, creating mid-career reskilling pathways, and investing in research ecosystems that anchor talent domestically are all prominent methods to support this goal.
A corresponding focus on the public sector is also pertinent, as without highly trained cyber personnel inside public institutions, Europe will struggle to deter and respond effectively to large-scale or persistent campaigns.

Just as Ukraine rapidly mobilized cyber talent, EU member states should consider building similar **capacity for structured cyber reserves, implemented in national cybercommands to best institutionalize volunteers and private-sector specialists.** These units could enable flexible surge capacity during crises while avoiding long-term reliance on unregulatable entities like hacktivist groups.

Second, **Europe must pursue a far deeper culture of collaboration across borders, sectors, and institutions**. One of the defining features of Ukraine's cyber defense has been its ability to blur traditional boundaries: national agencies work directly with private tech firms, ecosystem experts, and international partners in ways that traditional European bureaucracies have long struggled to replicate. Europe must normalize this wartime model in peacetime by ensuring that all national CERTs can exchange data rapidly and seamlessly, that private companies are integrated into national and EU-level response frameworks, and that cyber crisis mechanisms can **switch from information-sharing to joint action delays**. Interoperable technical standards, shared incident-reporting requirements, and regular multinational exercises that simulate real-world disruptions to critical infrastructure are all practical priorities.

Europe already has the NIS2 Directive to support this effort, but uneven and slow implementation across member states has failed to remove systemic vulnerabilities that adversaries are well positioned to exploit.

If this foundation is prioritized and effectively implemented with an improved focus on collaboration, Europe can build a more cohesive model for cross-sector and cross-border resilience to cyber hybrid threats.

Finally, Europe must undergo political recalibration. The current political environment does not incentivize a strong and resilient cyber ecosystem. Too often, **cybersecurity emerges as a priority only in the aftermath of a crisis.** Europe must instead treat hybrid defense as a standing, structural element of collective security and as a foundational pillar of traditional defense planning. A central part of this political shift is improving the ability to attribute hostile activity with clarity and confidence. Although many cyber operations are designed to cloud technical attribution, the strategic authorship is often still apparent. Yet, because evidentiary trails are rarely perfect, many governments remain cautious, reluctant to assign public responsibility for fear of miscalculation or retaliation.

This hesitation can further distort an already manipulable information environment and leave societies more vulnerable to hybrid threats. In contrast, Ukraine has already demonstrated the strategic value of clear and timely attribution: when used effectively, it can shape international understanding, mobilize support, and impose political costs on malicious actors. European leaders must be prepared to take firmer, more decisive public stances that convey zero tolerance for cyber-enabled hybrid threats. This will anchor hybrid defense as a central element of strategic planning and strengthening the European informational environment against manipulation, facilitating the potential development of appropriate actions.

Ultimately, Europe's key takeaway from Ukraine's experience cannot merely be that hybrid threats are growing.

Democratic societies must adapt to cyber-enabled hybrid aggression at the same speed and scale that their adversaries embrace it. Europe currently benefits from advance warning rather than crisis induced necessity, and it should use that advantage to prepare before a transformation is forced. Building this kind of resilience demands investment in people, the institutionalization of cross-sector collaboration, and the political will to make hybrid defense a priority. By doing so, Europe will be better positioned to deter attacks, limit their impact, and respond collectively when threats materialize.

References

[1] Kyiv Independent. (2025, October). Ukraine's parliament backs creation of cyber forces in first reading. https://kyivindependent.com/ukraines-parliament-backs-creation-of-cyber-forces-in-first-reading/

[2] Verkhovna Rada of Ukraine. (2024, December 19). Draft Law on the Cyber Forces of the Armed Forces of Ukraine (Registration No. 12349). https://itd.rada.gov.ua/billinfo/Bills/Card/45453

[3] NATO. (2024, May). Countering hybrid threats. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats/

[4] SSSCIP. (2025, June). Ukraine's Cyber Resilience: Key Success Factors and International Cooperation. A Report by the SSSCIP. https://cip.gov.ua/en/news/ukraine-s-cyber-resilience-key-success-factors-and-international-cooperation-a-report-by-the-ssscip

[5] National Security and Defense Council of Ukraine – Center for Countering Disinformation. (n.d.). History. https://scpc.gov.ua/en/history

[6] Militarnyi. (2025). Як Міністерство оборони захищає кіберпростір від ворожих атак. Militarnyi. Як Міністерство оборони захищає кіберпростір від ворожих атак

[7] SSSCIP. (2025, June). Ukraine's Cyber Resilience: Key Success Factors and International Cooperation. A Report by the SSSCIP. Retrieved from https://cip.gov.ua/en/news/ukraine-s-cyber-resilience-key-success-factors-and-international-cooperation-a-report-by-the-ssscip

[8] Vergun, D. (2022, December 3). Partnering with Ukraine on cybersecurity paid off, leaders say. U.S. Department of Defense. https://www.war.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/

[9] European Parliamentary Research Service. (2022). Russia's war on Ukraine: Timeline of cyber-attacks. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

[10] Reuters. (2022, March 4). Ukraine to join NATO cyber defence centre as 'contributing participant'. Euronews. https://www.euronews.com/2022/03/04/ukraine-crisis-cyber-nato

[11] Cabinet of Ministers of Ukraine. (2022, August 22). Uriady Ukrainy ta Polshchi pidpysaly memorandum pro spivpratsiu u sferi kiberzakhystu [The governments of Ukraine and Poland signed a memorandum on cooperation in the field of cyber defence]. Cabinet of Ministers of Ukraine. https://www.kmu.gov.ua/en/news/uriady-ukrainy-ta-polshchi-pidpysaly-memorandum-pro-spivpratsiu-u-sferi-kiberzakhystu

[12] e-Estonia. (2022, December 5). eGA and CybExer Technologies completed the set-up of a cyber lab for the Ukrainian Armed Forces. https://e-estonia.com/ega-and-cybexer-technologies-completed-the-set-up-of-a-cyber-lab-for-the-ukrainian-armed-forces/

[13] Ministry for Europe and Foreign Affairs. (2025, October 31). Tallinn Mechanism partners commit over 241.7 million euros to strengthen Ukraine's cyber defences amid escalating Russian aggression. Tallinn Mechanism Partners Commit Over 241.7 million euros to Strengthen Ukraine's Cyber Defences Amid Escalating Russian Aggression (31.10.25) - Ministry for Europe and Foreign Affairs

[14] National Security and Defense Council of Ukraine. (2024, April 17). Ukraine to participate in NATO CCDCOE Locked Shields cyber defense exercise. https://www.rnbo.gov.ua/en/Diialnist/6854.html

[15] Kyiv Polytechnic Institute. (2024, August 20). Kyiv Polytechnic, USAID, and partners strengthen Ukraine's cyber resilience. https://kpi.ua/en/2024-08-20

[16] Common Good Cyber. (2025, May 29). CDAC: "The scale of what we can do is severely hampered by not having funding for dedicated staff" [Interview]. https://commongoodcyber.org/news/interview_cdac_funding/

[17] Microsoft. (2022, February 28). Digital technology and the war in Ukraine. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

[18] Temple Raston, D. (2022, December 2). Exclusive: Rounding up a cyber posse for Ukraine. The Record from Recorded Future. https://therecord.media/exclusive-rounding-up-a-cyber-posse-for-ukraine

[19] Recorded Future. (n.d.). Recorded Future continues to provide critical intelligence to protect Ukraine from cyber, physical and kinetic threats. https://www.recordedfuture.com/newsroom/press-releases/recorded-future-continues-provide-intelligence-ukraine

[20] Microsoft Digital Security Unit, Microsoft Incident Response, & Microsoft Threat Intelligence. (2022, January 15). Destructive malware targeting Ukrainian organizations. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[21] Microsoft Threat Intelligence. (2023, June 14). Cadet Blizzard emerges as a novel and distinct Russian threat actor. Microsoft Security Blog. https://www.microsoft.com/en_us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-Russian-threat-actor/

[22] Microsoft Security Intelligence. (2022, February 23). TrojanDownloader:Win32/FoxBlade.B!dha [Threat Encyclopedia entry]. Microsoft. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:Win32/FoxBlade.B!dha
[23] Ministry of Digital Transformation of Ukraine. (2025, January 9). Microsoft to continue supporting Ukraine in 2025 by providing free cloud services. Ukrainska Pravda. https://www.pravda.com.ua/eng/news/2025/01/09/7492769/
[24] Google. (2022, December 1). New ways we're supporting Ukraine. Google Public Policy Blog. Retrieved from https://blog.google/outreach-initiatives/public-policy/new-ways-were-supporting-ukraine/
[25] Administration of the Public Service of Special Communication and Information Protection of Ukraine. (2023, May 31). Order No. 465: About approval of criteria by determination of the companies, organizations and organizations which are important for national economy in spheres of the organization of special communication, information protection, cyberprotection, protection of critical infrastructure during the special period (as amended on June 9, 2023). CIS Legislation. https://cis legislation.com/document.fwx?rgn=152082
[26] NATO Cooperative Cyber Defence Centre of Excellence. (2024). Luxembourg to support Ukrainian internships at NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/news/2024/luxembourg-to-support-ukrainian-internships-at-nato-cooperative-cyber-defence-centre-of-excellence
[27] Verkhovna Rada of Ukraine. (2025, March 27). Verkhovna Rada of Ukraine adopted the Law on protection of information and cyber defence of state information resources and critical information infrastructure [Press release]. https://www.rada.gov.ua/news/razom/260570.html
[28] National Security and Defense Council of Ukraine. (2024, October 31). Strengthening the transatlantic partnership: Nataliia Tkachuk participated in the meeting of the NATO CCDCOE Steering Committee. https://www.rnbo.gov.ua/en/Diialnist/7037.html
[29] Digital Watch Observatory. (2024, January 5). Russian hackers target Ukraine's Kyivstar telecoms giant in major cyberattack. https://dig.watch/updates/russian-hackers-target-ukraines-kyivstar-telecoms-giant-in-major-cyberattack/
[30] Antoniuk, D. (2025). CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers. The Record (Recorded Future News). https://therecord.media/kyivstar ceo on russian cyberattack telecom/
[31] RailTarget. (2025). Cyberattack hits Ukrzaliznytsia: Online services return after 89 hour recovery effort. https://www.railtarget.eu/technologies-and-infrastructure/ukrzaliznytsia-cyberattack-march-2025-online-systems-restored-10377.html/
[32] Interfax Ukraine. (2025, July 15). Intelligence Agency cyber specialists paralyze operation of one of major UAV manufacturers in Russia. https://en.interfax.com.ua/news/general/1087946.html
[33] Verkhovna Rada of Ukraine. (2025, October 9). We are together — against Russian aggression: The Verkhovna Rada of Ukraine supported the creation of a new military command body — Cyber Forces of the Armed Forces of Ukraine. https://www.rada.gov.ua/news/razom/266780.html/
[34]Defence Intelligence of Ukraine. (n.d.). Operations of the Defence Intelligence of Ukraine in cyberspace. https://gur.gov.ua/en/content/operatsii-hur-v-kiberprostori/
[35] InformNapalm. (2017, February 2). Cyberguerre : florilège du top des actions menées par la Cyber Alliance ukrainienne (UCA) en 2016. InformNapalm.org. https://informnapalm.org/fr/cyberguerre-florilege-top-actions-menees-cyber-alliance-ukrainienne-uca-2016
[36] InformNapalm. (2017, October 2). Cyberwar: top operations of Ukrainian Cyber Alliance (UCA) in 2016. InformNapalm.org. https://informnapalm.org/en/cyberwar-top-operations-of-Ukrainian-cyber-alliance-uca-in-2016/
[37]Burdina, E. (2023, November 27). «Цивільне населення завжди брало участь у війнах: хтось працює в тилу, хтось проводить диверсії». Учасник «Кібеpальянсу» про хакерів на війні та сумнівні правила «Червоного хреста» [Interview]. DOU. https://dou.ua/lenta/interviews/ukrainian-cyber-alliance-at-full-scale-war-2023/
[38] Ibid
[39] Ibid
[40] YouControl. (2025). Ukrainian Cyber Alliance (UCA) company profile [Company profile]. YouControl. https://youcontrol.com.ua/catalog/company_details/43305353/
[41] Fedorov, M. [@FedorovMykhailo]. (2022, February 26). We are creating an IT army. We need digital talents [Tweet]. Twitter. As cited in Hybrid Threats report. https://x.com/FedorovMykhailo/status/1497642156076511233?/
[42] George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. Information and organization, 29(3), 100249.
[43] Antoniuk, D. (2025, June 2). Pro Ukraine hacker group Black Owl poses 'major threat' to Russia, Kaspersky says. The Record from Recorded Future News. https://therecord.media/pro-ukraine-hacker-group-black-owl-major-threat-russia
[44] Stezhensky, A. (2025, June 12). Hackers paralyze Russia's Orion Telecom, disrupt uranium city's network. The New Voice of Ukraine. https://english.nv.ua/nation/largest-siberian-internet-provider-attacked-in-hur-cyber-strike-50521666.html

[45] Suspilne Media. (2025). Cyberattack on Crimea: Ukrainian intelligence has gained access to servers with all documentation of the occupation authorities. Retrieved from https://suspilne.media/crimea/1075253-kiberataka-na-krim-ukrainska-rozvidka-otrimala-dostup-do-serveriv-z-usieu-dokumentacieu-okupacijnoi-vladi-rbk/
[46] Ukrinform. (2025, September 8). HUR Cyber Corps blocks fuel cards in Russia, disrupts dozens of online platforms – source. https://www.ukrinform.net/rubric-ato/4034165-hur-cyber-corps-blocks-fuel-cards-in-russia-disrupts-dozens-of-online-platforms-source.html/
[47] Antoniuk, D. (2024, April 15). Ukrainian hacktivists claim to breach Russian drone developer. The Record (Recorded Future News). https://therecord.media/Russia-albatross-drones-alleged-data-leak-Ukraine-cyber-resistance
[48] InformNapalm. (2025, February 28). Russia building its navy despite sanctions: hacking of the 243rd Military Representative Office of the Russian MoD. https://informnapalm.org/en/russia-building-its-navy-despite-sanctions/
[49] New Voice of Ukraine. (2024, March 9). Ukraine gains intel on Russian missile manufacturers from Cyber Resistance activists. https://english.nv.ua/nation/ukraine-has-received-documentation-on-russian-missile-manufacturers-from-cyberresistance-activists-50399718.html/
[50] Troian, V. (2024, March 8). “Кібер Спротив” анонсував інформаційну кампанію проти фірм, які допомагають РФ виготовляти зброю [“Cyber Sprotyv announces information campaign against firms helping RF produce weapons”]. Hromadske. https://imi.org.ua/news/kiber-sprotyv-anonsuvav-informatsijnu-kampaniyu-proty-firm-yaki-dopomagayut-rf-vygotovlyaty-zbroyu-i59788
[51] KibOrg. (n.d.). Хто ми? https://kiborg.news/hto-my-shho-my
[52] Voloshko, V. (2022, December 26). Імена та адреси — перехоплені таємні документи ФСБ РФ в Криму. KibOrg News. https://kiborg.news/2022/12/26/vysoki-standarty-zhyttya-i-nyzki-metody-vykonannya-obovyazkiv-yak-praczyuye-rosijska-sluzhba-bezpeky/
[53] Dudchenko, M. (2023, May 2). Вугілля Донбасу: квиток в один кінець. KibOrg News. https://kiborg.news/2023/05/02/vugillya-donbasu-kvytok-v-odyn-kinecz/
[54] Dudchenko, M. (2023, March 2). «Зловживання свободою масової інформації у ЗМІ»: злиті документи Роскомнагляду. KibOrg News. https://kiborg.news/2023/03/02/zlovzhyvannya-svobodoyu-masovoyi-informacziyi-zlyti-dokumenty-roskomnaglyadu/
[55] Stezhensky, A. (2025, March 1). Kiborg: Inside Ukraine’s secret hacker groups helping track down children abducted by Russia during the war. The Independent. https://www.independent.co.uk/news/world/europe/ukraine-russia-war-hackers-children-kiborg-b2701487.html
[56] Dudchenko, M. (2025, July 15). Пірати Азовського моря: Як росіяни крадуть українське зерно за сприяння данської компанії Baltic Control. KibOrg News. https://kiborg.news/projects-pirates/
[57] Akymova, Y., & Danishevska, K. (2025, July 25). Cyber blast in Crimea. Ukrainian intelligence crashes Russian occupation servers. RBC Ukraine. https://newsukraine.rbc.ua/news/cyber-blast-in-crimea-ukrainian-intelligence-1753431641.html
[58] RIA Novosti. (2025, September 15). Рамфилова рассказала об атаках на ресурсы ЦИК [Pamfilova spoke about attacks on CEC resources]. RIA Novosti. https://ria.ru/20250915/pamfilova-2042016497.html
[59] Interfax Russia. (2025, December 18). ЦБ РФ будет взыскивать с банков Европы убытки из за неправомерной блокировки его активов. https://www.interfax.ru/russia/1063965/
[60] Federal Security Service of the Russian Federation. (2025, March 6). Press release: [ФСБ России пресекла операцию ГУР МО Украины по перехвату персональных данных учащихся образовательных организаций г. Москвы и Московской области с целью их дальнейшей вербовки] [Press release]. http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10440212%40fsbMessage.html/