***Dr. Eleni Kapsokoli**, Post-Doc Researcher*
Department of International and European Studies of the University of Piraeus, Athens, Greece
Email: elenikapsokoli1989@gmail.com

DOI: https://doi.org/10.37458/ssj.6.2.3
Review paper
Received: May 28, 2025
Accepted: July 26, 2025

WEAPONIZING CYBERSPACE: THE RUSSIA-UKRAINIAN WAR

Abstract: *In recent years, cyberspace has emerged as a critical fifth operational domain, where state and non-state actors engage in complex confrontations. Malicious cyber activities frequently target military assets, critical infrastructure, the private sector, citizens, and essential national services, resulting in significant political, social, and economic repercussions. This paper examines the strategic significance of cyberspace in the Russia-Ukrainian war, framing it as a new battlefield in modern warfare. This war exemplifies how activities like cyber-espionage, cyberattacks, hacking, disinformation campaigns, and cyber-surveillance are conducted to achieve military and geopolitical outcomes. The paper examines the frequency, complexity, and impact of these cyber activities during the conflict. Russia has employed state-directed and state-sponsored cyber activities, focusing on espionage, infrastructure disruption, and information manipulation, though often hampered by limited coordination with kinetic operations. Ukraine's resilient responses, including external support from the private sector, foreign governments, and individual hackers, alongside the formation of a 'cyber-army', serve as case studies of resilience to this evolving form of warfare. Lastly, the paper identifies key lessons on the role of cyberspace and information and communication technologies (ICTs) in modern conflicts and highlights the importance of developing resilient strategies.*

Keywords: *Russia-Ukrainian war, cyberspace, cyberattacks, hacking, cyber activities, cyber-army, artificial intelligence*

Introduction

The digital age has been defined by the widespread expansion of information communication technologies (ICTs), creating deeply interconnected, high-speed network societies. While this interconnectedness fosters innovation – from artificial intelligence (AI) to audience-tailored communication systems, and real-time universal dissemination of information – it also exposes vulnerabilities and reshapes how information is shared, perceived, and weaponized. Warfare, once confined to physical battlefields and with traditional military means, now extends into cyberspace, where operations can be as strategically significant as kinetic confrontations. In this field, both state and non-state actors conduct cyber activities that influence military, economic, and social systems, often with far-reaching and lasting consequences.

Cyber activities exploit computer networks, cyber-physical systems, and information infrastructure for purposes ranging from surveillance and espionage for collecting intelligence, information prohibition, sabotage, and integration of kinetic activities, selective disruption and destruction of critical and information infrastructure, and dissemination of disinformation campaigns. These activities often target civilians, state institutions, private industry, and essential services. The ongoing Russia-Ukrainian war illustrates this shift, with cyberspace emerging as a critical domain that shapes the trajectory of the conflict. The frequency, sophistication, and diversity of these activities underscore both the advanced capabilities of the actors involved and the strategic weight of the digital front. Some cyber activities are deliberately covert, while others, despite being designed for visible impact, may evade detection until they achieve disruptive effects.

The paper examines the multifaceted role of cyberspace in modern warfare, focusing on the Russia-Ukrainian war. It uses the term ‘cyber activities’ and no other related terms like cyber operations or information operations, cause the purpose of the research is to highlight the critical role of cyberspace and not engage in a definitional debate. Thus, cyber activities encompass direct attacks on critical infrastructure and the information environment (e.g., disruption, sabotage, espionage, and cyberattacks), as well as operations aimed at shaping perceptions and behaviors (e.g., disinformation and the dissemination of fake news). Such activities are conducted by a diverse set of actors, including private companies, civilians, hackers, state entities, or proxy groups. The analysis focuses on how both Russia and Ukraine have weaponized cyberspace, Kyiv’s reliance on external support, and the emergence of new ‘cyber militias’ in response to evolving threats. It begins by examining

cyberspace as an operational domain and reviewing Russia's cyber activities during the past decade. It then analyzes the spectrum of cyber activities observed from February 2022 to June 2025, before identifying lessons learned about the strategic significance of cyberspace in this ongoing conflict.

Methodologically, the paper adopts a qualitative multi-source approach, based on open-source intelligence (OSINT) from government and military reports, official statements, cybersecurity firm disclosures, media investigations, independent investigations, and academic publications. This approach mitigates the challenges of studying cyber activities, where timelines are blurred and often preceding open hostilities, attribution is contested, and many operations remain classified or obscured by false-flag tactics. To increase the reliability of findings, the study uses triangulation by comparing and evaluating multiple open-source intelligence sources to identify consistent patterns and reduce the risk of bias or misattribution. Additionally, it considers collateral effects, such as malware spreading into neutral networks, and the evolving roles of non-state actors, including cyber militias. By identifying these challenges, the paper seeks to offer a clear understanding of how cyberspace is reshaping warfare and what this means for the future of global security.

Pre-war Russian cyber activities

Cyberspace is recognized as the fifth domain of warfare, alongside land, sea, air, and space, which plays a critical role in both military and non-military operations. It enables state actors like Russia to gather intelligence, conduct surveillance, engage in espionage, and disrupt adversary systems. Cyber activities can be understood through both narrow and broad interpretations, which are designed to achieve objectives in or through cyberspace. The narrow view focuses on activities taken using computer systems or networks and has technical implications such as cyberattacks, distributed denial-of-service (DDoS) operations, and service disruptions. The broad approach exemplified by Russia integrates these technical capabilities with information warfare, including psychological and information operations, disinformation campaigns, and media manipulation. This broader approach enables operations that not only cause physical or technical harm but also cause cognitive effects on humans by shaping public narratives, influencing perceptions, and destabilizing societies without direct combat.

Russia's information warfare strategy is rooted in two primary components. The first, known as 'information and psychological activities', is aimed at influencing public

perception, morale, and behaviour. The second component, 'information technical activities', targets the disruption or degradation of critical infrastructure and information systems through cyberattacks (Giles, 2016; Hakala and Melnychuk, 2021). This integration blurs the distinction between wartime and peacetime operations, allowing Russia to apply the same strategic tools continuously. It reflects a philosophy that extends beyond conventional military means, incorporating cyber activities, space assets, electronic warfare, and intelligence operations. Together, these elements form a multifaceted strategy designed to assert power, erode the sovereignty of neighboring states, and influence political and strategic outcomes. In this context, cyber activities offer a low-cost, low-risk, and plausibly deniable means of advancing national interests without provoking direct military confrontation.

Russia has a well-documented history of leveraging its cyber capabilities against former Soviet republics, particularly those seeking integration with Western institutions like NATO and the European Union (EU). In such cases, cyber activities are often integrated into broader strategic campaigns during both periods of overt conflict and peacetime tension, as seen in the Russia-Georgia (2008) and the Russia-Ukrainian war (2022). Attacks against government institutions are typically intended to collect necessary intelligence, undermine public trust in democratic institutions, and erode confidence in the state's ability to protect its citizens. Attacks on other entities, like the private sector, can cause financial losses, reputational damage, and legal liabilities. At the same time, coordinated efforts to manipulate narratives through social media and online platforms aim to amplify the sense of insecurity, fear, and uncertainty, which weaken the psychological resilience of citizens. The effects of such attacks are highly context-dependent, ranging from immediate and direct impacts to more subtle and long-term consequences.

A clear pattern of state-linked cyber aggression emerged in 2007, when Estonia was targeted by a series of cyberattacks following a political confrontation between the two countries and the decision of Tallinn to join NATO and the EU in 2004. These attacks, widely attributed to actors affiliated with the Russian government, involved altering website content to disseminate pro-Moscow propaganda and conducting DDoS attacks that disrupted Estonia's critical infrastructure (Liaropoulos, 2012: 43). A similar pattern emerged during the 2008 conflict with Georgia, where cyberattacks were coordinated alongside military operations. Georgian government websites were rendered inaccessible

and replaced with antagonistic content, effectively suppressing the country's official narrative during a time of crisis (Kapsokoli, 2021, 50-63).

This strategy intensified in Ukraine beginning with the 2013 Maidan Revolution, which marked a decisive shift in the country's geopolitical orientation toward the EU and NATO. In response, Russia conducted a series of cyberattacks aimed at paralyzing Ukraine's state capacity and destabilizing its institutions (FP Analytics, 2023: 6). In March 2014, just before the Crimean referendum, cyberattacks targeted Ukraine's information and telecommunications systems, diverting attention from Russian military deployments in the region (Tidy, 2022). In May of the same year, the pro-Russian hacking group CyberBerkut attempted to interfere with Ukraine's presidential election by attacking the Central Election Commission (European Parliament, 2022). While the operation ultimately failed, it highlighted Russia's readiness to employ cyber tools to undermine democratic processes.

Russia's cyber campaign escalated further with the 2015 Black Energy cyberattack, attributed to the pro-Russian hacking group Sandworm. This incident disrupted Ukraine's power grid, exposing the vulnerability of critical infrastructure to cyber sabotage (America's cyber defense agency, 2021). Two years later, the NotPetya malware attack further underscored the implications of interconnected digital systems. Although it originated via a compromised Ukrainian accounting software, the malware rapidly spread to global networks in the USA, Europe, and Asia. With estimated damages of approximately $10 billion, the attack was one of the most devastating cyber incidents to date. While the methods resembled those of Sandworm, definitive attribution remains contested (Kapsokoli, 2020: 380).

These incidents underscore how Russia has integrated cyber activities into a broader strategy of coercion, disruption, and influence. The challenges of attribution, the lack of legal accountability, and the challenge of formulating proportional responses complicate international efforts to deter such activities. At the same time, Russia's cyber activities highlight the vulnerabilities of open, democratic, and digitally interconnected societies. The lessons from these pre-war activities highlight an evolving and complex threat landscape.

Cyber activities during the Russia-Ukrainian war

The conflict in Ukraine was the first military operation where cyberspace was extensively utilized alongside traditional military means. Both states have employed cyber activities to constrain their opponent's operational capabilities and achieve strategic objectives. By the

third year of the war, Russia had not launched large-scale cyber activities targeting Ukraine and its allies. Instead, it focused on cyber sabotage, disinformation campaigns, and attempts to erode support for Kyiv. Both states used three primary activities: disseminating disinformation and propaganda to redirect public opinion and weaken external support; collecting intelligence through surveillance and espionage to support military operations; and hacking and conducting cyberattacks against government, critical infrastructures, and other entities to gradually weaken the state's functionality and resilience.

From the invasion's onset, disinformation campaigns have played a pivotal role, using the social media ecosystem to spread fake news and deepfake content. These campaigns, which distort facts about battlefield casualties, internal divisions, doubts about the conflict, or diplomatic intentions, have significant implications for both local and international audiences. Moreover, the collection of sensitive information through surveillance and espionage tactics has been instrumental for both states. These activities include the real-time geolocation of high-ranking state officials for timely and precise strikes, the interception of communication channels to anticipate troop movements, and the acquisition of logistical data to disrupt supply chains and critical infrastructure. Such intelligence is pivotal not only for operational success on the battlefield but also for shaping long-term strategies to weaken the adversary's resilience. In addition, the destruction or disruption of critical infrastructure by both sides has aimed to limit the execution and support of military operations, such as logistics and intelligence, while also contributing to the gradual destabilization of their respective societies. Russian and Ukrainian cyber actors have conducted a combination of cyberattacks, including DDoS, wiper malware, ransomware, and hacking.

Russian cyber activities

Expanding on the overall cyber activities during the war, this section delves deeper into Russia's actions. These efforts represent a critical component of its wider strategy, leveraging advanced technologies to undermine Ukraine's societal resilience, reduce solidarity, erode public trust and international support, and demoralize the population. Tactics range from cyberattacks and hacking to AI-driven disinformation campaigns conducted by state-sponsored hacking groups, intelligence services, and aligned media actors. The Kremlin has effectively weaponized cyberspace to discredit Kyiv's objectives. It exerts strict control over the flow of information by fragmenting the domestic Internet

(Runet) and manipulating media outlets with overt and covert disinformation campaigns. Affiliated entities, including the Kremlin Spokesperson, state-controlled media, and proxies like State TV, Sputnik, The Russophile, and InfoBaltica, amplify these efforts (Kelley, 2024). Each outlet tailors content to specific demographic groups, promoting pro-Russian narratives. Many disinformation campaigns rely on AI-generated content, disseminated not only through bot and troll accounts but also via both Western and Russian media sources.

Moscow's narratives include several accusations: that Kyiv uses children as soldiers, alleged genocide against Russian speakers in eastern Ukraine (FP Analytics, 2023: 9), and support of Nazism. Additionally, these narratives claim that the Ukrainian government is led by a neo-Nazi junta and target Ukrainian President Volodymyr Zelenskyy to discredit him and question Western support for Ukraine (Li, Allen, and Siemazko, 2023). There are also accusations that the USA is secretly developing biological weapons in laboratories in the country (Reuters, 2022). This narrative was amplified by China's Foreign Ministry, framing Russia's invasion as a defensive move (Rising, 2022). Russia has claimed that the 2014 revolution in Ukraine was orchestrated by Washington rather than Moscow. Additionally, there is a misleading representation of widespread Ukrainian approval of Moscow's policies. Russian disinformation narratives may appear more credible to audiences in countries that are already inclined to view the West with suspicion or hostility.

A major influence operation known as 'Doppelgänger' was designed to disseminate pro-Russian narratives and erode Western support for Ukraine. It functions through a decentralized architecture comprising multiple sub-operations or 'avatars', each contributing to a broader strategy of disinformation. The primary avatars associated with the campaign include the following. The first one was 'Recent Reliable News' (RRN), which served as the campaign's central content hub and operated under the guise of an anonymous news media outlet. RRN initially launched under the name Reliable Russian News, which primarily hosts propaganda content, including content with pro-Russian figures. One such case involved an interview with French Member of Parliament Thierry Mariani, which was subsequently removed after French authorities revealed the outlet's ties to Russian influence operations.

The other avatar was 'Matriochka' (named after the Russian nesting dolls) included fake media content disseminated in multi-platform fake and real accounts. In addition, the 'Overload' specifically targeted journalists and media organizations, aiming to flood the

information space and disorient credible sources (EU Disinfo Lab, 2025). Finally, the avatars 'Storm-1099' and 'Storm-1679' were identified by Microsoft as malicious actors supporting the campaign's broader operations (Watts, 2024). The Doppelgänger campaign employed several key tactics to disseminate disinformation. It cloned websites of established news outlets (Le Monde, The Guardian, Der Spiegel) using typosquatting[1]. While these spoofed websites closely replicate the visual identity of legitimate media, they publish content that is often poorly written, misleading, or overtly propagandist. The website 'War on Fakes' was launched shortly after the invasion as part of the above campaign. Although it mimics the structure and language of independent fact-checking sites, it instead disseminates pro-Russian narratives and disinformation. Notably, this website shares technical infrastructure with RRN, highlighting a coordinated approach within the campaign.

One notable example was a deepfake video broadcast on a Ukrainian TV channel on 16 March 2022, showing President Zelenskyy urging citizens to surrender because the war was over (The Telegraph, 2022). The video was shared online multiple times, gathering 120.000 views on Twitter/X in a short period and spreading on communication platforms like Telegram. However, it had a minor impact as the Ukrainian President quickly debunked it via his personal Instagram account. What stood out most in this incident was the use of a credible platform to distribute fake content, amplifying its initial reach. This example highlighted the credibility risks posed by fake content.

The disinformation campaigns are often bolstered by advanced AI technologies. As revealed in leaked documents from 2023, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) developed a project involving AI bot accounts designed to infiltrate social media platforms like VKontakte, Odnoklassniki, Facebook, Twitter/X, Telegram, TikTok, and YouTube. These bots promote pro-Russian narratives while bypassing detection through 'shadow' purchases of SIM cards and pre-made accounts on the illegal market. These efforts aimed to undermine certain publications and sentiments in Ukrainian, Russian, and Belarusian communities (Tracking Exposed, 2022).

[1] Typosquatting is a cyberattack technique in which malicious actors register domain names closely resembling legitimate websites, often using common misspellings or slight variations, to deceive users who mistype URLs. It is a social engineering tactic that exploits user errors to redirect them to fraudulent or malicious sites. Microsoft. (2025). *'What is typosquatting?'*.

Despite countermeasures like TikTok's removal of more than 3.000 bot accounts, in May 2023, pro-Russian hashtags like #thisisnotmyukraine continue to gain significant traction, highlighting the persistence and adaptability of these disinformation efforts at discrediting the mobilization efforts in Ukraine and the actions of the Territorial Center of Completion (TCC). Within a month, the pro-Russian hashtag garnered more than 10 million total views, making it one of the top three most popular hashtags at the end of July. These figures reflect 41.000 publications and an average weekly reach of several million views, highlighting the extensive scope and effectiveness of AI-driven propaganda (SPRAVDI, 2024).

TikTok has become one of the key platforms for disseminating narratives against the Ukrainian government. A video of a speech by Putin claiming that 'today's neo-Nazis have taken power in Ukraine' and that responsibility for any bloodshed in the country lies with those in power in Kyiv. This video was viewed 1.7 million times and shared more than 15.000 times by 14 March 2022, just 9 days after its release. In Spring 2023, a fake French animated series, 'Corporation Ukraine', was released, portraying President Zelenskyy as corrupt and addicted to alcohol and drugs (SPRAVDI, 2023). The series was distributed via YouTube, TikTok, X, and Facebook, with help from paid promotions, bloggers, and 'independent' news sources.

After Zelenskyy's presidency ends, some TikTok users, including former Ukrainian Parliament member Igor Mosiychuk, have demanded that elections be held during the war. They have accused Zelenskyy of usurping power and being a dictator or suggested that he should transfer the authority to the Chairman Verkhovna Rada (Korotunenko and Rayevskyi, 2024). The same ideas were supported by President Putin and his spokesperson Dmitry Peskov, amplifying the anti-Ukrainian government narratives. Moreover, these troll accounts posted videos and pictures from civilians and military personnel, featuring Ukrainian prisoners of war, glorifying the Russian military as an 'invisible army' and portraying Putin as a 'strong leader' to shape foreign perceptions.

Russian disinformation campaigns target not only Ukrainian society but also its supporters worldwide. On 3 March 2024, German authorities announced the leak of an audio recording in which 4 military officers discussed the use of Taurus missiles to support Ukraine against Russia (Politico, 2024). Boris Pistorius, Germany's Defense Minister, stated that Moscow had leaked the recording as part of an 'information war' (Posaner and Donovan, 2024). This claim was supported by analysis from the research center

NewsGuard, which indicates that TikTok engages in 'shadow promotion' of Russian propaganda by disseminating false and misleading information about the war, irrespective of users actively searching for this news on the platform. If a user searches on the Internet for generic terms related to the war, like 'Ukraine' and 'Donbas', TikTok suggests multiple videos with disinformation content.

Russian hacking groups and intelligence services have long engaged in malicious cyber activities like espionage and cyberattacks. Even before the conflict's outbreak, they sought to destabilize Ukraine's defence by targeting governmental and military systems to hinder effective operational activities (Bateman, 2022). Moscow has deployed state-sponsored cyber actors linked to intelligence agencies such as the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), the Russian military intelligence (GRU), and the Information Operations Troop to support various cyber activities. In January 2023, pro-Russian hacking groups - Sandworm, Killnet, Killnet 2.0, Just Evil, Conti ransomware group, CoomingProject, XakNet Team, Beregini, NoName057, Anonymous Russia, Phoenix, and People's Cyber Army – formed the 'Digital Army of Russia' to conduct coordinated attacks against Ukraine and allied targets, with activities spanning from disruptive to destructive attacks (KELA Cyber Intelligence Center, 2024).

In October 2024, Amazon Web Services published a report on a new espionage campaign developed by Cozy Bear (APT29), which stole credentials through phishing emails and gained access to targeted information systems (Moses, 2024). In December 2024, the Sandworm group targeted the Ukrainian military application called 'Army+' to obtain important operational information. This espionage campaign involved creating fake websites that mimicked the official app, making it easier for users to perform tasks such as submitting reports to their commanders. As a result, many users inadvertently downloaded malicious files during the app's installation process. Once installed, the program granted intruders covert access to the information system, allowing them to export sensitive data. Ukraine's Military Computer Emergency Response Team (MIL.CERT-UA) attributed the campaign to Sandworm. However, many details regarding the extent of the attack, the number of victims, and the attackers' objectives remain unclear (Antoniuk, 2024). This incident highlights the persistent and evolving nature of Russian cyber activities targeting Ukraine's military and civilian infrastructure.

Between April and June 2022, Aqua Bizzard (ACTINIUM) conducted phishing campaigns targeting humanitarian organizations operating in Ukraine and investigators of

Russian war crimes (Microsoft Threat Intelligence, 2023). They focused on Ukrainian military applications like Delta and Bachu, as well as webcams and closed-circuit television (CCTV) services to monitor the delivery of Western aid. Impersonation tactics included fake social media accounts posing as Ukrainian military personnel and requesting humanitarian and military aid. Similarly, in January 2022, the Belarusian group Ghostwriter (UNC1151) targeted Ukrainian government entities and tech companies (PolySwarm Tech Team, 2022). On 23 February 2022, the malware Hermetic Wiper (FoxBlade) infected several Ukrainian government entities, followed the next day by Isaac Wiper (Lasainraw), aiming to compromise data and prevent analysis. Hermetic Wiper was linked to Cypriot company Hermetica Digital Ltd, which had issued a code-signing certificate in 2021 (ESET, 2022). Moreover, the group UAC-0165 conducted phishing attacks on at least 11 Ukrainian telecommunications providers, causing service disruptions (Cyber Peace Institute, 2023: 4-5). On 14 March 2022, the malware Dubbed Caddy Wiper infiltrated the Ukrainian government and financial institutions to collect economic data (ESET, 2022). The Security Service of Ukraine (SSU) reported in January 2024 that Russian intelligence hacked online surveillance cameras to monitor air defense activities and critical infrastructure in Kyiv before recent missile strikes (Coker, 2024). These incidents illustrate how Russia coordinates its cyber activities in conjunction with military operations.

Since early 2023, more than 400 cyberattacks have been documented against Ukraine's national infrastructure (Cyber Peace Institute, 2023: 11). A significant cyberattack occurred on the day of the invasion, disrupting KA-SAT ViaSat's satellite broadband access and affecting tens of thousands of users in Ukraine and Europe, thereby weakening Kyiv's defence capabilities (Page, 2022). This cyber incident caused the most widely reported collateral damage outside the Ukrainian borders. As of 10 March 2022, thousands of KA-SAT satellite network modems were rendered inoperable, including devices in France, Greece, Hungary, Germany, Italy, and Poland (Canadian Centre for Cyber Security, 2022).

Similarly, on 8 April 2022, an attempt was made to disrupt power generation and distribution systems, affecting millions. In May 2022, cyberattacks targeted Ukrainian government websites, telecommunications services, and infrastructure, coinciding with military operations in Odesa and further underscoring the scale of Russian cyber activities (Barichella, 2022). In December 2023, an attack on Ukraine's largest mobile operator, Kyivstar, rendered services inoperative, destroyed IT infrastructure, and disabled systems

used to track and alert against air raids (Hunder, Landay, and Bern, 2023). On 4 January 2024, Sandworm conducted another attack on Kyivstar, causing more than 24.3 million customers to lose phone reception (Ngendakumana, 2024). On 25 January 2024, Naftogaz, Ukraine's largest oil and gas company, was targeted in a large-scale attack on its data centers (Masters, 2024). Throughout 2024, the group Gamaredon (UAC-0010) was responsible for 277 cyber incidents against Ukraine (Antoniuk, 2025). In March 2025, a cyberattack targeted Ukrzaliznytsia, the state railway operator, disrupting its ticketing app and online services, though train schedules were not affected[2]. These incidents highlight the critical role of cybersecurity in protecting essential infrastructure, especially during wartime, when disruption to services can have far-reaching consequences.

Many Ukrainian media outlets continue to face cyberattacks and disinformation campaigns, limiting their ability to broadcast crucial information, particularly in occupied regions. On 24 February 2022, a cyberattack targeted the communication systems of Kyiv Porst, highlighting the need to protect the critical infrastructure (European Parliamentary Research Service, 2022). In 2023, Google recognized the rise in attacks targeting Ukrainian media and civil society websites and decided to expand its Project Shield protection against these threats[3]. Similarly, on 9 May 2024, Ukraine's satellite channels StarLight Media and Inter were hacked and broadcast Moscow's Victory Day parade footage alongside images of destroyed cities and casualties from Russian military operations (Kyiv Post, 2024).

Russian cyberattacks also extended to allied countries, targeting the USA, Poland, Canada, Romania, and Germany between late 2022 and mid-2023 (Cyber Peace Institute, 2023: 14). From 15 to 22 April 2022, Killnet claimed responsibility for over 20 DDoS attacks against critical infrastructure in Czechia, Estonia, Latvia, Poland, Romania, Lithuania, the UK, and the USA (Greig, 2022). France similarly experienced a series of cyberattacks against its government information systems in March 2024 (Roussi, 2024).

Ukrainian cyber activities

The Ukrainian side has similarly developed cyber activities in response to Russian aggression. These activities encompass a broad spectrum of goals, including countering Moscow's disinformation campaigns and propaganda, fostering international solidarity and morale by showing the human side of the war, disrupting adversarial operations and critical infrastructure, and collecting intelligence. Kyiv's cyber activities showcase a multifaceted

[2] Link of the post: https://t.me/UkrzalInfo/6671
[3] For more information: https://projectshield.withgoogle.com/landing

strategy based on proactive measures to ensure the state's resilience and adaptability in the face of new threats.

Kyiv has weaponized information to debunk Moscow's narratives and media. They have used fake news like fabricated reports of aerial bombings, designed to instill fear and disrupt societal stability. Examples of fake news include claims of foreign military support for Ukraine and the photoshopped footage of the Russian President from his press conference on 5 March 2022, intended to hide the fact that he was not in Moscow. Another example is the footage of Zelenskyy from 2021 that was used to promote the idea that he is out there fighting for his country. Finally, the 'Ghost of Kyiv' was one of the viral trends of the war that claimed to show Ukrainian pilots shooting down Russian jets, but the shootings were from the 'Digital Combat Simulator' videogame (NewsGuard, 2024).

Humorous and satirical deepfake videos have been strategically employed to undermine President Putin's legitimacy. In March 2022, a manipulated audio clip circulated on social media, falsely suggesting that Ukraine had initiated negotiations[4]. The clip's content was derived from Putin's 21st February 2022 speech, where he recognized the independence of two separatist regions in eastern Ukraine (Baig, 2022). In addition, the films 'Downfall' and 'The Great Dictator' were used to portray him as one of their infamous characters, amplifying satirical critique. Polish director Patryk Vega took a more direct approach, creating the English-language film titled 'Putin' using deepfake technology to question the Russian President's legitimacy and mental health (Stilwell, 2024).

Deepfake technology has also been employed by the Ukrainian government for various purposes, such as launching disinformation campaigns and informing citizens about the war. However, not all users have shared accurate content; some videos were debunked as misleading, featuring footage from unrelated conflicts or global events, aimed at strengthening solidarity and support for Ukraine (Twomey, Linehan, and Murphy, 2023). On the other hand, Ukrainians have created videos that allow viewers worldwide to witness the human side of the war and create a sense of intimacy with the audience (Liaropoulos, 2023: 200). An important example is user Valerisssh, who shared videos depicting daily life in bomb shelters. Other videos document the destruction of buildings, wreckage of military equipment, or acts of resistance, such as a viral clip titled 'Time of the Strong', showing a Ukrainian soldier attacking a Russian target. This topic extends to the TikTok account

[4] Post: https://web.archive.org/web/20220318073121/https:/twitter.com/sternenko/status/1504090918994993160

'time_of_the_strong', which has over 250.000 followers, celebrating the military resilience and success of Ukrainian soldiers[5].

The government created a mobile app, 'Dia' (The State and me), which allows displaced people to cross borders using a wartime digital ID (Nelson and Wilde, 2023). It also offers updates regarding the war while reducing disinformation activities. Another app, 'eVorog' (eEnemy), serves as a citizen-reporting tool for gathering intelligence about the activities of the Russian military (The Economist, 2023). This enables the government to make citizens the 'eyes and ears' of the war, integrating them into national defence efforts. The development of such apps demonstrates Ukraine's digital resilience during the war, where technology enhances governance, security, and communication with citizens.

Ukraine has conducted cyberattacks against Russia's critical national infrastructure to cause dysfunction and collect information through espionage methods, leveraging its cyberwarfare units. A unique aspect of this war has been the mobilization of civilians who voluntarily engaged in cyber activities. On 26 February 2022, Ukraine's Ministry of Digital Transformation made a call for IT specialists who wanted to support the country's cyberspace (Raffray, 2022). Volunteer hackers, such as the 200.000 member IT Army of Ukraine, conduct various cyberattacks and hacking against Russian targets through platforms like Telegram (Tidy, 2023). These individuals have exposed sensitive Russian data as a means of punishing the country for its crimes in Ukraine (Menn, 2022) and used facial recognition software to identify and notify the families of deceased Russian soldiers (Biggerstaff, 2022). They also developed the digital campaign 'OPRussia', which conducted hack and leak attacks against important Russian organizations like the Bank of Russia (Osorio, 2022).

The Ukrainian government developed the 'Diia' services application, which includes an 'e-Enemy' feature that enables citizens to report the positions and movements of Russian troops. The information collected through this feature contributes to 'Delta', a situational awareness platform used by the Ukrainian military. As a result, civilians are motivated to participate in combat support activities (Danylov, 2023). Additionally, the gathering of open-source information supports the establishment of accountability for war crimes and atrocities. On the contrary, Russia has attempted to debunk these accusations of war crimes by producing videos and disseminating them via fake social media accounts (BBC Monitoring, 2022). At the beginning of 2024, they hacked the Russian

[5] Video: https://www.tiktok.com/@time_of_the_strong

telecommunications company Akado, which provides internet services to state organizations (Antoniuk, 2024).

In addition to these volunteers, other hacking groups, including Anonymous and Network Battalion 65 (NB65), have also targeted Russian government institutions, research and development firms, as well as Transneft, RuTube, Roscosmos, Russian television networks, and the Killnet hacking group (Statista, 2023). The hacking group Hdr0 conducted 4 breach attacks against Russian entities in early 2023, and the BO Team hacked the State Research Center for Space Hydrometeorology (Planeta) in January 2024, destroying its database and valuable equipment (Cyber Peace Institute, 2023: 8-9). In September 2024, pro-Ukraine hackers claimed responsibility for a cyberattack on the agency Osnovanie, defacing its websites, destroying critical data, and leaking it for sale (Antoniuk, 2024). In December 2024, the group Silent Crow hacked and leaked data from the employees of the government agency Rosreestr as retaliation for a series of cyberattacks against Ukrainian entities[6]. In January 2025, many hacking groups conducted cyberattacks against Russia's critical infrastructure. The group Ukrainian Cyber Alliance claimed to have destroyed the internet provider Nodex via a cyberattack[7]. The group Cyber Anarchy Squad had attacked the tech company Infobis and stolen data[8]. The group Yellow Drift claimed responsibility for the cyberattack against the electronic trading platform, Roseltorg, and the deletion of its 550 terabytes of data[9]. The group Sticky Werewolf developed a cyber-espionage campaign that targeted many Russian ministries, like the Ministry of Industry and Trade (Antoniuk, 2025).

Likewise, the intelligence services and military forces support Kyiv's cyber activities against Russia. On 23 November 2023, Ukraine's Military Intelligence (GUR) Service breached Russia's Federal Air Transport Agency (Rosaviatsia), allegedly exposing challenges in aircraft repairs due to sanctions. The data was leaked online but later removed, making it impossible to verify its legitimacy (Defence Intelligence of the Ministry of Defence of Ukraine, 2023). In December 2023, the agency also disrupted the central servers of Russia's Federal Tax Service (FNS), erasing critical tax and financial information (Antoniuk, 2023). On 27 January 2024, Ukraine's Main Intelligence Directorate (HUR) conducted a cyberattack against the information system infrastructure of IPL Consulting, a

[6] Post on telegram with the claim of responsibility: https://t.me/cybersecs/3534
[7] Post on telegram with the claim of responsibility: https://t.me/UCAgroup/38
[8] Post on telegram with the claim of responsibility: https://t.me/cyber_anarchy_squad/353
[9] Post on telegram with the claim of responsibility: https://t.me/yellow_drift/3

company specializing in implementing information systems in the Russian industrial sector, and destroyed over 60 terabytes, dozens of servers, and databases (Masters, 2024).

International involvement and cyber allies

Cyber activities in modern warfare have introduced innovative strategies and expanded participation beyond traditional state actors. Notably, governments, private companies, hacktivist groups, and individuals now directly engage in these conflicts, blurring boundaries and raising questions about their legal and strategic status.

The involvement of pro-Ukraine and pro-Russia hacking groups has become increasingly significant in shaping the dynamics of the conflict. While volunteer hackers may view their efforts as resistance or retaliation, their civilian involvement raises important ethical and legal concerns. Organizations like the International Committee of the Red Cross caution that such individuals could be considered members of an organized armed group or civilians directly engaged in hostilities (Biggerstaff, 2023). In response, Ukraine is considering legislation to formally integrate the 'IT Army of Ukraine' into its armed forces, seeking to manage the long-term implications of civilian involvement (Waterman, 2023). This situation highlights the growing indistinction between government-backed and independent entities in the conflict, along with the possible repercussions of an ungoverned and fragmented cyber conflict.

Governments, organizations, individuals, and the private sector have collectively bolstered Ukraine's defence. The USA, the EU, and organizations like NATO have been primary allies, providing technical resources, cybersecurity practices, intelligence sharing, and equipment to strengthen Ukraine's resilience. Since February 2022, the US Cyber Command has worked with Ukrainian Computer Security Incident Response Teams (CSIRTs) to address potential threats. On 21 March 2022, President Joe Biden urged US business leaders to strengthen cybersecurity capabilities, considering Russia's escalating cyber capabilities (Vazquez, Judd, Lyngaas, and Cohen, 2022). In July 2022, the US Cybersecurity and Infrastructure Security Agency (CISA) and Ukraine's SSSCIP signed a Memorandum of Cooperation to exchange information and best practices for cyber incident management (Kaushik, 2023: 7). In May 2025, a joint cybersecurity advisory co-signed by 11 allied nations and 21 intelligence agencies from the UK, USA, Germany, France, Canada, Poland, Czechia, Australia, Estonia, Denmark and the Netherlands, formally attributed cyberattacks and espionage to the 85th Main Special Service Center (85th GTsSS),

military unit 26165 of the GRU and associate groups such as Fancy Bear and APT28 (US Department of Defence, 2025). This coordinated attribution represented a significant act of political and diplomatic solidarity, signaling unified attribution and condemnation of Russian cyber activities. Strategically, it reinforced NATO's collective cyber defence stance and sent a clear geopolitical signal of unity in protecting democratic institutions and norms in the digital domain.

Ukraine's participation in NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), formalized in 2023, and extended support pledges at the NATO Vilnius Summit underscore the long-term commitment to its security and integration (NATO, 2024). Canada has also provided cybersecurity expertise and satellite communication services to ensure the continuity of critical infrastructure (Communications Security Establishment, 2023). In June 2021, the EU established the EU-Ukraine Cyber Dialogue to enhance operational capabilities in cyberspace and counter disinformation (Stano, Massrali, and Quatresols, 2021). Following Ukraine's request in February 2022, the EU activated its PESCO Cyber Rapid Response Teams (CRRTs) to provide operational support (EDA, 2022). The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (2022) has delivered critical insights and organized simulation exercises to prepare for cyber threats. These combined measures have significantly fortified both the EU and Ukraine's cyber defence capabilities and resilience.

Similarly, the private sector has played an unprecedented role in shaping Ukraine's cyber defence. Technology companies have essential services, intelligence, situational awareness, and technical infrastructure such as space reconnaissance sensors, commercial satellites, and advanced telecommunications systems (Beecroft, 2022). Amazon, Cloudflare, Apple, HP, Cisco, Google, and Microsoft migrated Ukrainian government data and services from domestic data centers to cloud servers and provided cybersecurity programs and upgraded hardware and software (Mitchell, 2022). On 17 February 2022, just before the invasion, Ukrainian authorities moved national data to the public cloud to mitigate risks from malicious attempts. Microsoft created dedicated disaster response teams to assist those affected by aggression. Elon Musk's Starlink was one of the 'cyber amplifiers' on Ukraine's side, offering connectivity to restore battlefield communications disrupted by Russian forces in February 2022 (Champion, 2023). Although not designed as a military system, its attributes made it suitable for military use. In February 2023, Starlink implemented limitations on usage, stating that the system should not be utilized for

offensive activities, including facilitating communications for managing drones that conduct attacks on Russian forces (Marquardt and Fisher, 2023).

In an innovative approach to accountability, the Ukrainian government persuaded Meta, Twitter/X, and TikTok to archive content for potential war crimes trials (Simonite, 2022) - a practice that had not been employed in prior conflicts such as Syria, Myanmar, and Libya. This cooperation represents a transformative shift in private sector engagement in conflict prevention and atrocity documentation. Ukraine's Minister of Digital Transformation described the tech sector's role as integral to the war effort, paralleling it to 'a real army' working alongside the armed forces (Sheftalovich, 2022).

Overall, the Russia-Ukrainian war has underscored that international engagement now extends far beyond traditional alliances, encompassing cyber capabilities, technological partnerships, intelligence sharing, and diplomatic coordination. The heavy reliance on private sector involvement, particularly for Ukraine, has provided strategic advantages and resilience. At the same time, it raised questions about accountability, regulatory compliance, durability of such commitments, and long-term ramifications for the international system. In future conflicts, the loyalties of technology firms, government, and organizations may shift in line with their strategic and commercial interests, making their role a variable and integral part of modern warfare.

Lessons learned from the Russia-Ukrainian war

The cyber activities during the Russia-Ukrainian war have significantly influenced the evolving character of warfare. They have confirmed that the digital battlefield is now a fully integrated extension of military operations, shaping strategies and outcomes in profound ways, while offering distinct tactical advantages alongside psychological effects. Although malicious cyber activities did not directly result in catastrophic outcomes, such as loss of life, their destabilizing effects amplified the impact of conventional military operations. These activities, whether in the form of surveillance, filtering, infrastructure disruption, or disinformation, often go undetected for extended periods, complicating early detection and response. Furthermore, the attribution process remains a persistent challenge, which is essential for accountability, imposing sanctions and countermeasures, and accurate assessment of overall impact. The complexity of identifying responsible actors has also hampered diplomatic responses, with many governments limiting their actions to sanctions rather than broader, active countermeasures.

Russia's cyber activities have primarily focused on espionage, data and financial theft, disrupting critical infrastructure, and instilling fear among citizens. In 2024, pro-Russian hacking groups conducted more than 1.024 cyberattacks, targeting governmental, military, and critical infrastructure assets. According to the State Special Communications Service of Ukraine (SSSCIP), such groups aimed not only to compromise information systems but also to enhance military operations by providing intelligence (The State Cyber Protection Centre, 2025). However, the lack of effective coordination with kinetic operations, inefficient targeting, and Ukraine's resilient defence, strengthened by external cyber allies, limited their strategic impact (Mueller, Jensen, Valeriano, Maness, and Macias, 2023). This disconnect revealed a structural weakness in Russia's approach, constraining the effectiveness of its digital campaigns.

Russian strategists have increasingly concluded that networks offer greater long-term value for intelligence collection than for immediate destruction. Thus, the focus has shifted from dismantling systems to exploiting them, prioritizing persistent access to open networks over short-term disruption. This doctrinal adjustment has not, however, altered Russia's broader military priorities, which continue to favor electronic warfare over cyber activities (Maundrill, 2023). Mobile operational and tactical electronic warfare units remain embedded with major formations and directly integrated into battlefield units, constituting the primary digital combat elements, rather than dedicated cyber units. This emphasis underlines Russia's ongoing focus on electromagnetic spectrum dominance rather than real-time integration of cyber capabilities into battlefield decision-making.

Ukraine, by contrast, has demonstrated remarkable cyber resilience in the face of Russian cyber aggression, which stems from prior experience, investments in critical infrastructure, advances in digital technologies, and sustained international support. Foreign governments and the private sector have been pivotal in enhancing Ukraine's cyber defence. Kyiv's defensive capacity has improved measurably since the start of the war. In 2023, cyber incidents fell to 2.5 times fewer than the 7.000 reported in 2022 (FP Analytics, 2023: 13). Conversely, the first half of 2024 saw an increase to 1.739 incidents, a 20% rise (SSSCIP, 2024). The Security Service of Ukraine (SSU) has been the vanguard of Kyiv's cyber defence efforts. For example, it implemented the Malware Information Sharing System (MISP-UA), an open-source software for sharing threat intelligence (Kaushik, 2023: 7).

Ukraine's resilience efforts have included widespread voluntary civilian participation, with citizens contributing to intelligence collection and operational support (Smith-Boyle, 2022). Another critical takeaway is that durable cyber defence depends on a diverse network of international partnerships, including engagement from the private sector and civilians. Ukraine's collaboration with technology firms and cybersecurity providers enabled operational adaptability and state functionality, but reliance on these actors carries inherent risks. Support is influenced by market conditions, political priorities, shareholder expectations, and shifting geopolitical interests. Future defence strategies must therefore account for the possibility that these actors may reduce or withdraw their assistance, ensuring resilience even in the absence of external private-sector and state backing.

Concluding remarks

The Russia-Ukrainian conflict marks a defining moment in the evolution of warfare, integrating cyber activities as a core component of military strategies. It has exposed how deeply modern societies rely on ICTs and the vulnerabilities that stem from this reliance. Thus, the conflict demonstrates that safeguarding critical infrastructure and government information systems is no longer optional but vital to national security. Both sides engaged in a diverse range of activities to meet their goals, including espionage, the art of deception, the subtleties of subversion, and the persuasive influence of propaganda initiatives. The unfolding of these strategies promises to shape the dynamics in unexpected ways. Disinformation campaigns, often utilizing AI-generated content and amplified through platforms like TikTok, have significantly influenced public perception and global awareness, earning the conflict the label 'First TikTok War' (Liaropoulos, 2023: 200). This highlights the importance of digital and media literacy in countering these threats.

While Moscow's disinformation efforts faced resistance due to Ukraine's societal resilience, Russia shifted focus to alternative methods, such as cyber-espionage, real-time intelligence gathering, communications interception, and targeted cyberattacks. Yet, Ukraine's robust cyber defence, built on prior experience, international support, and strong private-sector partnerships, significantly limited its strategic effect. The involvement of volunteer hackers and civilians, notably Ukraine's 'IT army' and Russia's state-sponsored hacking groups, points out the decentralization of cyber warfare and the blurring of lines between combatants and civilians. Meanwhile, Ukraine's coalition of domestic and international partners represents a new model of 'digital solidarity', wherein public and

private entities maintain the state's survival and functionality. Cyber capabilities are now in the hands of both states and non-state entities, enabling them to influence conflict outcomes. This trend raises pressing ethical and legal questions, highlighting the need for an evaluation of international norms and legal frameworks to address the accountability, status, attribution, and protection for cyber volunteers.

This war serves as a forerunner for the future of conflict, highlighting the wide range of activities in a fragmented, decentralized, connected, and algorithm-driven information environment, but also the existence of multiple state and non-state actors operating simultaneously. In practice, cyberspace has played a predominantly disruptive rather than destructive role, especially once open conflict began. Specifically, while cyber activities could be central during the pre-war period, their significance often diminishes once open military conflict begins, at which point malicious cyber activities take on a more auxiliary role. Therefore, cyber activities have complemented, rather than replaced, conventional military operations. These are rarely decisive, but they are indispensable in augmenting and shaping the dynamics of warfare at the level of the tempo, perception, and resilience.

In the case of Russia, cyberspace is more often employed for censorship, propaganda, and cognitive warfare. The asymmetric nature of cyberspace, particularly in a fragmented, closed, and well-controlled network like Runet, makes the analysis and attribution of such activities complicated because their exploitation relies on governmental and state-sponsored actors. In contrast, Ukraine operates within an open and interconnected digital environment where networks and data are not isolated from the global internet. Much of the information regarding cyber activities comes from private technology companies collaborating with Kyiv, while national institutions actively disclose a significant number of cyber incidents. This transparency improves situational awareness and supports international cooperation, but it also leaves Ukraine vulnerable to persistent and highly visible cyber threats.

The inability to coordinate digital operations with kinetic warfare, as seen in this analysis, reveals the need for doctrinal adaptation, not just technological investment. More broadly, it reinforces the urgency of establishing shared international norms and credible attribution frameworks to deter irresponsible cyber behaviour and ensure accountability. The battlefield of Ukraine affirms that resilience, alliances, and agile digital infrastructure have become foundational pillars of national defence. Cyberspace is no longer a peripheral

theatre of operations; it is a contested strategic domain where influence, capability, and resolve are constantly tested.

References

America's cyber defense agency (20 July 2021). *Cyber-attack against Ukrainian critical infrastructure.* https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01
Antoniuk, D. (2023). 'Ukraine's intelligence claims cyberattack on Russia's state tax service'. *The Record.* https://therecord.media/ukraine-intelligence-claims-attack-on-russia-tax-service
Antoniuk, D. (2024). 'Pro-Ukraine hackers claim attack on agency that certifies digital signatures in Russia'. *The Record*. https://therecord.media/russia-osnavanie-digital-signatures-cyberattack-ukraine
Antoniuk, D. (2024). 'Sandworm-linked hackers target users of Ukraine's military app in new spying campaign'. *The Record*. https://therecord.media/ukraine-military-app-espionage-russia-sandworm?utm_medium=email&_hsenc=p2ANqtz-9Xfrusd8755Hwknr35j1UrpLmTRQa1PnWfF25Ij9ksrGYwlCIlBiZXZOPYp_6P4BgsswgJqmRAD2PQrHygi9RDDM-SG1urmPhWzEXsMwHXMhxqvOI&_hsmi=339424039&utm_content=339430154&utm_source=hs_email
Antoniuk, D. (2024). Ukrainian hackers claim attack on Russian scientific research center. *The Record. https://therecord.media/ukrainian-hackers-hit-russian-scientific-center*
Antoniuk, D. (2025). 'Russian espionage and financial theft campaigns have ramped up, Ukraine cyber agency says'. *The Record.* https://therecord.media/russian-espionage-financial-theft-campaign
Antoniuk, D. (2025). 'Suspected Ukrainian hackers impersonating Russian ministries to spy on industry'. *The Record.*
Baig, R. (18 March 2022). The deepfakes in the disinformation war. *Deutsche Welle.* https://www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433
Barichella, A. (2022). Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe. *Europe in the World, no.281*
Bateman, J. (16 December 2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. *Carnegie.* https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en
BBC Monitoring. (11 April 2022). Bucha killings: Satellite image of bodies site contradicts Russian claims. *BBC.* https://www.bbc.com/news/60981238
Beecroft, N. (2022). Evaluating the International Support to Ukrainian Cyber Defense. *Carnegie.* https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en
Biggerstaff, W.C. (2022). Ukraine Symposium photos of the dead. *Lieber Institute. https://lieber.westpoint.edu/photos-of-dead/*
Biggerstaff, W.C. (2023). The status of Ukraine's IT Army under the Law of Armed Conflict. *Lieber Institute https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/*
Canadian Centre for Cyber Security. (2022). *'Cyber Threat Bulletin. Cyber Threat Activity Related to the Russian Invasion of Ukraine'.*

https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf
Champion, M. (8 September 2023). 'Elon Musk has power in Ukraine. Does he know how to use it?'. *Bloomberg.* https://www.bloomberg.com/opinion/articles/2023-09-08/ukraine-war-it-doesn-t-matter-how-elon-musk-got-involved-he-s-in-it
Coker, J. (3 January 2024). 'Russia Spies on Kyiv Defenses via Hacked Cameras Before Missile Strikes'. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/russia-spies-kyiv-hacked-cameras/
Communications Security Establishment. (2023). '*Communications Security Establishment Annual Report 2022-2023'* https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-%20establishment-annual-report-2022-2023
Cyber Peace Institute. (2023). '*Cyber Dimensions of the Armed Conflict in Ukraine*'. https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf
Danylov, O. (2022). 'The unique Ukrainian situational awareness system Delta was presented at the annual NATO event. ' *Mezha*. The unique Ukrainian situational awareness system Delta was presented at the annual NATO event • Mezha.Media
Defence Intelligence of the Ministry of Defence of Ukraine. (2023). *Defence Intelligence of Ukraine conducted a cyber operation against Rosaviatsia - sanctions accelerate Russia's aviation collapse.* https://gur.gov.ua/en/content/voienna-rozvidka-ukrainy-zdiisnyla-kiberspetsoperatsiiu-shchodo-rosaviatsii-sanktsii-pryskoriuiut-aviakolaps-rf.html
EDA. (24 February 2022). *Activation of first capability developed under PESCO points to strength of cooperation in cyber defence.* https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence
ESET. (1 March 2022). *ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper.* https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/
ESET. (15 March 2022). *CaddyWiper: New wiper malware discovered in Ukraine.* https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
EU Disinfo Lab. (Last update 15 May 2025). 'What is the Doppelganger operation? List of Resources'. https://www.disinfo.eu/doppelganger-operation
European Parliament. (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
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
FP Analytics. (2023). *Digital front lines. A sharpened focus on the risks of, and responses to, hybrid warfare* https://digitalfrontlines.io/2023/05/25/the-evolution-of-cyber-operations-in-armed-conflict/
Giles, K. (2016). *Handbook of Russian Information Warfare.* NATO Defense College
Greig, J. (12 May 2022). 'Italy stops wide-ranging Russian attack of websites of parliament, military, health agency'. *The Record.* https://therecord.media/italy-killnet-hacking-military-parliament-national-health-institute

Hakala, J. and Melnychuk, J. (2021), Russia's Strategy In Cyberspace, *NATO Strategic Communications Centre of Excellence*, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

Hunder, M., Landay, J., and Bern, S. (13 December 2023). Ukraine's top mobile operator hit by biggest cyberattack of war. *Reuters.* https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

Hybrid CoE. (18 March 2022). *Hybrid CoE continues to work to support European security and Ukraine.* https://www.hybridcoe.fi/news/hybrid-coe-continues-to-work-to-support-european-security-and-ukraine/

Kapsokoli, E. (2020). 'European Union and Cybersecurity: institutions and strategies', in Daskalakis, I. (ed.) The Defense Integration of the European Union, Infognomon (in Greek).

Kapsokoli, E. (2021). The security challenges that the EU is facing in cyberspace", in Sidiropoulos, S., Tzagkarakis, I. and Kritas, D. (eds.) *1st POLITEIA International Conference Proceedings - Europe at the Crossroads: Leadership, Challenges and State of Play*, Hellenic Association of Political Scientists (HAPSc), Athens, pp.50-63

Kaushik, A. (2023). 'The War on Ukraine: a look at underemphasized Russian cyber operations'. *GLOBSEC.* https://www.globsec.org/what-we-do/publications/war-ukraine-look-underemphasised-russian-cyber-operations

KELA Cyber Intelligence Center. (25 February 2024). *Russia-Ukraine war: pro-Russian hacktivist activity two years on.* https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/

Kelley, M. (2024). 'Understanding Russian Disinformation and How the Joint Force Can Address It'. *US Army War College.* https://publications.armywarcollege.edu/News/Display/Article/3789933/understanding-russian-disinformation-and-how-the-joint-force-can-address-it/

Korotunenko, S. and Rayevskyi, D. (5 August 2024). 'Ihor Mosiychuk is a Ukrainian politician with a bad reputation, a popular blogger and Russian propaganda darling. Why he is so loved'. *Babel.* https://babel.ua/en?utm_source=page&utm_medium=main

Kyiv Post. (9 May 2024). *Russian Hackers Hack Ukrainian, Latvian Channels to Broadcast Moscow Victory Day Parade. https://www.kyivpost.com/post/32400*

Li, D., Allen, J. and Siemaszko, C. (24 February 2022). 'Putin using false 'Nazi' narrative to justify Russia's attack on Ukraine, experts say'. *NBC.* https://www.nbcnews.com/news/world/putin-claims-denazification-justify-russias-attack-ukraine-experts-say-rcna17537

Liaropoulos, A. (2012). Deterrence in cyberspace: implications for National Security. *MCIS Yearbook 2012.*

Liaropoulos, A.N. (2023). 'Victory and Virality. War in the age of social media'. *Georgetown Journal of International Affairs 24,* no.2.

Marquardt, A. and Fisher, K. (9 February 2023). 'SpaceX admits blocking Ukrainian troops from using satellite technology'. *CNN* https://www.cnn.com/2023/02/09/politics/spacex-ukrainian-troops-satellite-technology

Masters, J. (26 January 2024). 'Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline'. *MSSP Alert.* https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion

Maundrill, B. (7 March 2023). 'Russia's Cyber Tactics in Ukraine Shift to Focus on Espionage'. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/russias-cyber-tactics-shift-to/

Menn, J. (1 May 2022). Hacking Russia was off-limits. The Ukraine war made it a free-for-all. *The Washington Post.*
Microsoft. (Last update 5 August 2025). *'What is typosquatting?'.* https://support.microsoft.com/en-us/topic/what-is-typosquatting-54a18872-8459-4d47-b3e3-d84d9a362eb0
Microsoft Threat Intelligence. (15 March 2023). *A year of Russian hybrid warfare in Ukraine.* https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf
Mitchell, R. (15 December 2022). 'How Amazon put Ukraine's 'government in a box' – and saved its economy from Russia', *Los Angeles Times*, https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data
Moses, C.J. (24 October 2024). 'Amazon identified internet domains abused by APT29'. *AWS Amazon.* Amazon identified internet domains abused by APT29 | AWS Security Blog
Mueller, G.B., Jensen, B., Valeriano, B., Maness, R.C. and Macias, J.M. (2023). Cyber operations during the Russo-Ukrainian War. *On future War.*
NATO. (10 May 2024). *Relations with Ukraine.* https://www.nato.int/cps/en/natolive/topics_37750.htm
Nelson, A. and Wilde, G. (18 April 2023). 'How cyber support to Ukraine can build its democratic future'. *Cyberscoop.* https://cyberscoop.com/ukraine-cyber-aid-russia-war/
NewsGuard. (16 December 2024). *'Russia-Ukraine Disinformation Tracking Center: 645 Websites Spreading War Disinformation and The Top Myths They Publish'.* https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/
Ngendakumana, P.E. (4 January 2024*). 'Ukraine says Russian hackers penetrated major telecoms network for months'.* https://www.politico.eu/article/ukraines-cyber-spy-chief-vitiuk-says-russia-hackers-penetrated-kyvstarg-telecoms-system-for-months/
Osorio, N. (6 June 2022). 'Russia's Cyber Warfare Reputation Lies in Ruins As Anonymous Hacktivists Raid Central Bank Again'. *International Business Times*. https://www.ibtimes.com/russias-cyber-warfare- reputation-lies-ruins-anonymous-hacktivists-raid-central-bank-3530912
Page, C. (31 March 2022). Viasat cyberattack blamed on Russian wiper malware. *TechCrunch.* https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1
Politico. (3 March 2024). *'Germany investigating leak in Russia of audio purportedly showing talks on Ukraine aid'.* https://www.politico.eu/article/germany-investigating-leak-in-russia-of-audio-purportedly-showing-discussion-of-ukraine-aid/
PolySwarm Tech Team. (9 March 2022). *HermeticWiper & IsaacWiper Target Ukraine.* https://blog.polyswarm.io/hermeticwiper-isaacwiper-target-ukraine
Posaner, J. and Donovan, H. (3 March 2024). *'Germany accuses Moscow of 'disinformation attack' in leaking senior officers' call'.* Politico. https://www.politico.eu/article/german-defense-minister-accuses-moscow-of-a-disinformation-attack-in-leaking-call-by-senior-officers-taurus-pistorius-ukraine-war/
Raffray, E. (2022). 'Ukraine: 100 days of war in cyberspace'. *Cyber Peace Institute.* *https://cyberpeaceinstitute.org/news/ukraine-100-days-of-war-in-cyberspace/*
Reuters. (10 March 2022). *U.S. dismisses Russian claims of biowarfare labs in Ukraine.* https://www.reuters.com/world/russia-demands-us-explain-biological-programme-ukraine-2022-03-09/

Rising, D. (11 March 2022). *'China amplifies unsupported Russian claim of Ukraine biolabs'.* Associated Press. https://apnews.com/general-news-39eeee023efdf7ea59c4a20b7e018169

Roussi, A. (11 March 2024). 'French government hit with cyberattacks of 'unprecedented' intensity'. *Politico*. https://www.politico.eu/article/french-government-hit-with-cyberattacks-of-unprecedented-intensity/

Sheftalovich, Z. (18 May 2022). 'Ukraine targeting Russians in information war, Kyiv says'. *Politico.* https://www.politico.eu/article/ukraine-targeting-russians-in-information-war-kyiv-says/

Simonite, T. (2022). The Race to Archive Social Posts That May Prove Russian War Crimes. *Wired.* https://www.wired.com/story/open-source-russia-war-crimes-ukraine/

Smith- Boyle, V. (2022). 'How OSINT Has Shaped the War in Ukraine', *American Security Project* https://www.americansecurityproject.org/osint-in-ukraine

SPRAVDI. (2024). *'Exploiting TikTok for malicious influence on ukrainian audience'.* https://spravdi.gov.ua/en/exploiting-tiktok-for-malicious-influence-on-ukrainian-audience/

SPRAVDI. (2023). *'Advertising Captivity and Smear Ads against Ukrainian Counter-Offensive: Spring Activation of Russian Propaganda'.* https://spravdi.gov.ua/en/advertising-captivity-and-smear-ads-against-ukrainian-counter-offensive-spring-activation-of-russian-propaganda/

SSSCIP. (2024). *'Cyber operations by russia: new goals, tools and groups. Analytics on the hacker attacks against Ukraine in H1 2024'.* https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report

Stano, P., Massrali, N., and Quatresols, X.C. (2021). Cyberspace: EU and Ukraine launch a dialogue on cyber security. *European Union External Action.*

Statista. (February 2023). *'Timeline of cyber events involved in Russia's war in Ukraine from February to November 2022'.* https://www.statista.com/statistics/1428613/russia-cyber-incidents-war/

Stilwell, B. (7 February 2024). Polish filmmaker deepfaked an entire movie starring Vladimir Putin and screened it for Ukrainian troops. *Military.com.* https://www.military.com/off-duty/movies/2024/02/07/polish-filmmaker-deepfaked-entire-movie-starring-vladimir-putin-and-screened-it-ukrainian-troops.html

The Economist. (22 February 2023). *'How a chatbot has turned Ukrainian civilians into digital resistance fighters'.* https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters

The State Cyber Protection Centre. (8 January 2025). *'The Vulnerability Detection and Cyber Incidents / Cyber Attacks Response System helped to detect and process 1,042 cyber incidents in 2024'.* https://scpc.gov.ua/en/articles/383

The Telegraph. (17 March 2022). Deepfake video of Volodymyr Zelensky surrendering surfaces on social media. *YouTube. https://www.youtube.com/watch?v=X17yrEV5sl4*

Tidy, J. (15 April 2023). Meet the hacker armies on Ukraine's cyber front line. *BBC.* https://www.bbc.com/news/technology-65250356

Tidy, J. (2022). Ukraine cyber-attack: Russia to blame for hack, says Kyiv. *BBC.* https://bbc.com/news/world-europe-59992531

Tracking Exposed. (10 August 2022). 'Shadow-promotion: TikTok's algorithmic recommendation of banned content in Russia'. https://tracking.exposed/pdf/tiktok-russia-ShadowPromotion.pdf

Twomey, J.J., Linehan, C., and Murphy, G. (26 October 2023). Deepfakes in warfare: New concerns emerge from their use around the Russian invasion of Ukraine. *The Conversation.*

https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393

US Department of Defence. (2025). *'Joint Cybersecurity Advisory: Russian GRU Targeting Western Logistics Entities and Technology Companies'.* https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF

Vazquez, M., Judd, D., Lyngaas, S., and Cohen, Z. (21 March 2022). Biden warns business leaders to prepare for Russian cyber-attacks. *CNN.* https://www.cnn.com/2022/03/21/politics/biden-russia-cyber-activity

Watts, C. (2024). *'How Russia is trying to disrupt the 2024 Paris Olympic Games'.* Microsoft. https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/