TALLINN PAPERS

Nataliya Tkachuk, PhD

Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression

Tallinn Paper No. 15
2025

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Previously in This Series

No. 1 Kenneth Geers “Pandemonium: Nation States, National Security, and the Internet” (2014)

No. 2 Liis Vihul “The Liability of Software Manufacturers for Defective Products” (2014)

No. 3 Hannes Krause “NATO on Its Way Towards a Comfort Zone in Cyber Defence” (2014)

No. 4 Liina Areng “Lilliputian States in Digital Affairs and Cyber Security” (2014)

No. 5 Michael N. Schmitt and Liis Vihul “The Nature of International Law Cyber Norms” (2014)

No. 6 Jeffrey Carr “Responsible Attribution: A Prerequisite for Accountability” (2014)

No. 7 Michael N. Schmitt “The Law of Cyber Targeting” (2015)

No. 8 James A. Lewis “The Role of Offensive Cyber Operations in NATO’s Collective Defence” (2015)

No. 9 Wolff Heintschel von Heinegg “International Law and International Information Security: A Response to Krutskikh and Streltsov” (2015)

No. 10 Katrin Nyman Metcalf “A Legal View On Outer Space and Cyberspace: Similariteis and Differences” (2018)

No. 11 Elaine Korzak “Russia’s Cyber Policy Efforts in the United Nations” (2021)

No. 12 TALLINN PAPERS YOUNG SCHOLAR EDITION: Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe “Opportunities for Public and Private Attribution of Cyber Operations” (2021)

No. 13 Jeremy K. Davis “Developing Applicable Standards of Proof for Peacetime Cyber Attribution” (2022)

No. 14 George Christou “Cyber Diplomacy: From Concept to Practice” (2024)

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). The expressions reflected are those of the author(s) alone; publication by the Centre should not be interpreted as endorsement thereof by the Centre, its Sponsoring Nations or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

The Tallinn Papers

The NATO CCD COE's Tallinn Papers are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarization of cyberspace, and technical. Focusing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by invitation, proposals dealing with issues of strategic importance and acuteness will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

Abstract

The article explores Ukraine's journey toward the development of its national cybersecurity system, building cyber resilience and cyber defence capabilities in countering Russian cyber aggression, and the lessons learned that may be valuable for other European nations. It analyses Russia's tactics in cyber warfare and their gradual transformation, and examines the growing Russian cyber threat to EU countries. This Tallinn Paper aims to propose ways to strengthen Europe's collective cyber defence based on Ukraine's experience. The study is based on scientific articles, analytical materials and statistical data from open sources, as well as open public information created and used by the main entities of the national cybersecurity system of Ukraine when ensuring cybersecurity. It delivers twelve key and context-specific recommendations on building effective national cyber defence capabilities and proposes the creation of a Cyber Alliance to prevent and counter Russian cyber threats.

Keywords: *Ukraine, cyber war, Russia, cyber aggression, cyberattack, cyber operations, IT Army*

Introduction

Since February 24, 2022, Europe has been witnessing the largest conventional war in Europe since the World War II. A terrorist state – Russia, once believed to have the world's second most powerful military – launched a treacherous attack on Ukraine, a country with significantly fewer human and military resources. The full-scale invasion was a continuation of the crime of aggression that Russia has been carrying out against Ukraine since February 2014, temporarily occupying the Autonomous Republic of Crimea, the city of Sevastopol, and certain areas of the Donetsk and Luhansk regions.[1] In 2022, the Russian Federation openly and cynically escalated the war into a new phase without any provocation, no longer attempting to conceal its true nature or intentions.

Unexpectedly for the entire world, Ukraine has demonstrated extraordinary resilience, bravery and endurance in this war. It has managed to awaken Europe, which had recognised the obvious threats, but without taking the required actions and decisions to rally nations to stand together against the aggressor.

Cyberspace has become another domain of this war. Every day, Russia carries out dozens of sophisticated cyberattacks on Ukraine's critical infrastructure, government agencies and military and civilian systems, coordinating these attacks with conventional weapons and information-

[1] Ministry of Foreign Affairs of Ukraine, Statement on a Year Since the Start of Russia's Full-Scale Military Invasion of Ukraine (24 February 2023) https://mfa.gov.ua/en/news/zayava-mzs-ukrayini-do-roku-z-pochatku-povnomasshtabnogo-vijskovogo-vtorgnennya-rosiyi-v-ukrayinu.

psychological operations.[2] However, Ukraine has shown remarkable cyber resilience built in a short time and the maturity of its national cybersecurity system, which has been developed over the past decade. It has also proven its ability to strike back in cyberspace through offensive cyber operations.[3]

Yet, Russia's war is no longer just against Ukraine. In reality, it has declared cyber war against the entire democratic world, the EU and NATO.[4] Russia conducts unlawful cyber and information operations targeting Western populations, undermines the functioning of critical infrastructure, steals citizens' personal data and attempts to influence electoral processes.[5]

This makes it crucial to study and apply Ukraine's experience gained from its prolonged cyber war with Russia and to thoroughly understand the adversary in order to develop collective defence mechanisms for all of Europe. The EU must recognise that, without a strong, proactive cyber defence system, it will be impossible to provide an advantage in the face of current and future cyber threats. Any future war, as history has already shown, will begin and be accompanied by a cyber component.

The Beginning of the Cyber War

Russia's launching its military aggression against Ukraine in 2014 can also be considered the beginning of the world's first cyber war. At present, the term has no common definition. In this article, it is used to describe cyberattacks and operations which, for the first time, accompanied an open military invasion.

The first documented case of a cyberattack as a tool of military aggression occurred in December 2015.[6] Russian hackers, using the BlackEnergy malware, carried out a cyberattack against multiple energy facilities in Ukraine. The attack on Prykarpattyaoblenergo was particularly successful, leaving approximately 80,000 households, businesses and enterprises without electricity for several hours.

---

[2] Oleksandr Topchii, 'Rosiia za dopomohoiu kiberatak namahaietsia teroryzuvaty ukraintsiv' (*UNIAN*,12 January 2023) https://www.unian.ua/techno/communications/rossiya-pri-pomoshchi-kiberatak-pytaetsya-terrorizirovat-ukraincev-politico-12106917.html; Dmytro Kazantsev, 'Cybersecurity during war: challenges, trends, startups' (*MEZHA*, 20 March 2025) https://mezha.media/articles/vid-diversiy-do-shpigunstva-vikliki-ta-trendi-kiberviyni-300559/.

[3] Maksym Butchenko, 'Zahaniaiut voroha do «cheburnetu». Ukrainska rozvidka provela vzhe bilshe pivsotni znachnykh kiberoperatsii proty rosiian' (*NV.UA* , 11 June 2024) https://nv.ua/ukr/ukraine/events/ukrajinska-rozvidka-rozkrila-svoji-hakerski-ataki-po-rf-tipi-cili-ta-dosyagnennya-novini-ukrajini-50426113.html.

[4] Council of the European Union, *Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation* (3 May 2024) https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/; NATO, Statement by the North Atlantic Council on recent Russian hybrid activities (2 May 2024), https://www.nato.int/cps/uk/natohq/official_texts_225230.html.

[5] Lukasz Olejnik, *Russian cyber and information warfare and its impact on the EU and UK* (15 April 2025) https://www.kcl.ac.uk/russian-cyber-and-information-warfare-and-its-impact-on-the-eu-and-uk.

[6] Dustin Volz and Jim Finkle, 'U.S. Helping Ukraine Investigate Power Grid Hack' (*Reuters*, 12 January 2016) https://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112/.

This cyberattack specifically targeted the civilian population and was accompanied by Russian military actions in eastern Ukraine. It bore some of the characteristics of a war crime.[7] At that time, Ukraine was unprepared to counter such threats, just as most Western nations were likely unprepared as well. However, the realisation that Russian aggression against Ukraine, particularly in cyberspace, would only intensify catalysed Ukraine to launch an active process of strengthening its cybersecurity capabilities. Previously, the state lacked the political will and understanding of the need to develop cybersecurity as an important component of national security and defence.

Development of Ukraine's National Cybersecurity Capabilities

The first step was to establish a regulatory and legal framework. In 2016, Ukraine adopted its first National Cybersecurity Strategy,[8] followed by the Cybersecurity Law[9] in 2017. These acts laid the foundation for the national cybersecurity system, set key priorities for its development and defined the responsibilities of each government entity involved in cybersecurity.

Structure of the National Cybersecurity System

The **National Cybersecurity Coordination Centre (NCSCC)**, as a working body of the National Security and Defence Council of Ukraine, is responsible for coordinating and overseeing the activities of security and defence sector entities that ensure cybersecurity. The NCSCC also develops and oversees the implementation of Ukraine's **Cybersecurity Strategy**.

The main entities within Ukraine's **National Cybersecurity System** include:

- **The State Service of Special Communications and Information Protection of Ukraine (SSSCIP)** – Responsible for developing and implementing state policy on cyber protection of government systems and critical information infrastructure. It conducts state oversight in these areas, ensures the operation of the **State Cyber Protection Centre**, the **Centre for Active Cyber Defence Against Aggression**, and **Ukraine's Government Computer Emergency Response Team (CERT-UA)**.
- **The National Police of Ukraine** – Conducts activities to prevent, detect, stop and investigate cybercrimes while also raising public awareness of cybersecurity.

[7] Yola Verbruggen, 'Cyberattacks as War Crimes' (10 January 2024) *International Bar Association* https://www.ibanet.org/Cyberattacks-as-war-crimes.
[8] Ukaz Prezydenta Ukrainy №96/2016, Pro rishennia RNBO vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy", (15 March 2016) https://www.president.gov.ua/documents/962016-19836.
[9] Law of Ukraine, *On the Basic Principles of Cybersecurity in Ukraine*, 5 October 2017, № 2163-VIII https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.

- **The Security Service of Ukraine (SBU)** – Counteracts cyberterrorism, cyber espionage and the most serious cybercrimes. It responds to and investigates cyber incidents related to state security, such as cyberattacks on government systems and critical infrastructure. The SBU also conducts covert assessments of critical infrastructure readiness against potential cyberattacks and incidents.
- **The Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine** – Prepare the state for cyber defence against military aggression, conduct cyber defence operations and engage in military cooperation with NATO and other defence entities to ensure collective protection against cyber threats.
- **Ukraine's Intelligence Agencies** – Conduct intelligence operations related to cybersecurity threats to national security and other cyber-related events.
- **The National Bank of Ukraine (NBU)** – Develops cybersecurity policies for Ukraine's banking and financial sector, oversees compliance and ensures the functioning of a cybersecurity system for banks.
- **The Cabinet of Ministers of Ukraine** – Responsible for shaping and implementing state policy in the field of cybersecurity.

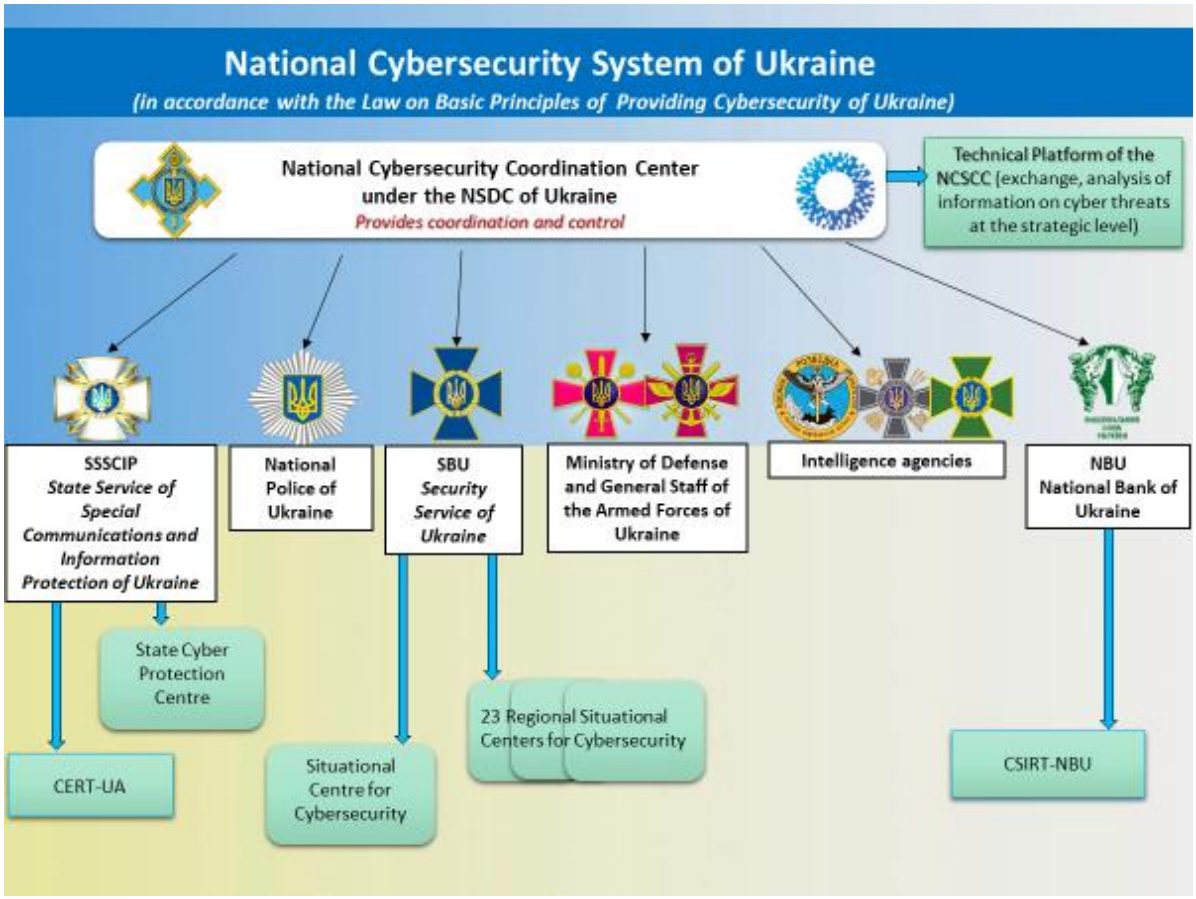

Figure 1. Structure of Ukraine's National Cybersecurity System

Alongside the development of the regulatory and legal framework, Ukraine has also strengthened the institutional, personnel and technical capabilities of key entities responsible for responding to cyber threats and ensuring cybersecurity.

The Security Service of Ukraine (SBU) established the Cybersecurity Situational Centre in Kyiv,[10] later expanding it with several regional branches and significantly increasing the capacity of units responsible for countering cyber threats.

The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) initiated the deployment of sensor infrastructure across government institutions and expanded the capabilities of the State Cyber Protection Centre (SCPC) and CERT-UA.[11]

The Cyber Police Department of the National Police of Ukraine underwent significant development, introducing new tools for citizens to report cybercrimes more efficiently.

[10] 'V Ukraini ziavyvsia Sytuatsiinyi tsentr, shcho vidbyvatyme kiberataky', (*UKRINFORM*, 25 January 2018) https://www.ukrinform.ua/rubric-technology/2389847-v-ukraini-zavivsa-situacijnij-centr-so-vidbivatime-kiberataki.html; SBU, 'Sytuatsiinyi tsentr zabezpechennia kiberbezpeky SBU' https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky.

[11] SSSCIP, 'SSSCIP's State Cyber Protection Center expands sensor system for government agencies to enhance cyber incident response' (29 January 2025) https://cip.gov.ua/ua/news/dckz-prodovzhuye-rozbudovu-sistemi-sensoriv-u-derzhavnikh-organakh-dlya-shvidkogo-reaguvannya-na-kiberincidenti; SSSCIP, 'Cabinet of Ministers of Ukraine restores SSSCIP's authority to oversee cryptographic and technical protection of information resources, and cyber defense of CII' (25 January 2025) https://cip.gov.ua/en/news/kabmin-vidnoviv-povnovazhennya-derzhspeczv-yazku-z-kontrolyu-kriptografichnogo-ta-tekhnichnogo-zakhistu-informaciinikh-resursiv-a-takozh-kiberzakhistu-oki.

Additionally, the Cyber Police intensified its participation in international investigations and operations to combat transnational cybercrime.[12]

The National Bank of Ukraine (NBU) established CSIRT-NBU,[13] a specialised Computer Security Incident Response Team for the banking sector, to enhance the financial system's cybersecurity resilience.

Since 2018, Ukraine has initiated processes for cyber incident information sharing. The SBU launched the first Ukrainian MISP (Malware Information Sharing Platform), enabling cyber threat intelligence exchange among various national entities.[14]

With the support of international partners, Ukrainian specialists began actively participating in leading training programmes, workshops and other practical exercises to enhance their skills in cybersecurity and cyber incident investigation.[15]

To ensure effective coordination and oversight in the field of cybersecurity, the NCSCC was established under the National Security and Defence Council of Ukraine in 2016.[16]
Unlike specialists in other European countries, Ukrainian cybersecurity professionals had unparalleled opportunities to apply their knowledge and skills in real-world cyber warfare against the aggressor. As Russian cyberattacks against Ukraine grew increasingly complex, large-scale and dangerous over time, Ukrainian experts continuously improved their response capabilities.

This continuous real-world experience forced on Ukraine by the enemy became one of the key factors behind the country's cyber resilience both before and during the full-scale invasion.

Escalation of Russia's Cyber Aggression Before the Invasion

The escalation of Russia's cyber aggression against Ukraine began in November 2021, with a significant increase in both the number and intensity of already familiar cyberattacks. On 14 January 2022, Russian hackers carried out a cyberattack on more than 70 Ukrainian government websites. As a result of the defacement, a message appeared on these sites in Ukrainian, broken Polish and Russian, stating:

[12] Kiberpolitsiia Ukrainy, Zvit pro diialnist Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy u 2024 rotsi (31 January 2025) https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/.
[13] NBU, 'NBU Team Joins Global Cybersecurity Community' (8 February 2022) https://bank.gov.ua/en/news/all/komanda-nbu-stala-chastinoyu-mijnarodnoyi-spilnoti-z-protidiyi-kiberzagrozam.
[14] SBU, 'Dlia protydii kiberzahrozam SBU vvodyt v diiu onovlenu versiiu platformy MISP-UA' (16 July 2020) https://ssu.gov.ua/novyny/7800.
[15] PlayUA, 'U Kyievi provely masshtabni navchannia z kiberzakhystu obiektiv krytychnoi infrastruktury' (8 December 2021) https://playua.net/u-kyyevi-provely-masshtabni-navchannya-z-kiberzahystu-ob-yektiv-krytychnoyi-infrastruktury/.
[16] Prezydent Ukrainy, Ukaz 'Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky', No 242/2016 (7 July 2016).https://zakon.rada.gov.ua/laws/show/242/2016#Text.
.

> "*Ukrainian! All your personal data has been uploaded to the public network. All data on your computer is being destroyed and cannot be restored. All information about you has become public, fear and expect the worst. This is for your past, present and future. For Volhynia, for OUN-UPA, for Galicia, for Polissia and for the historical lands.*"[17]

Thanks to the coordinated efforts of Ukrainian cybersecurity specialists, the websites were quickly restored. However, the motives of the attackers remain unclear, but the attack served as a warning about the upcoming escalation, giving Ukraine time to strengthen its cyber defences and remove the Russian hacker presence from the affected systems. Thus, the attack only had an insignificant psychological effect on the population. Had this attack been executed on the day of the invasion and combined with open military actions of Russian troops, its impact would have been far more severe.

On 27 June 2024, the US Department of Justice put a Russian citizen on the wanted list who, together with the GRU, participated in cyberattacks on Ukrainian websites in January 2022, thereby confirming attribution of these attacks to Russian special services.[18]

[17] Olena Bohdaniok, '"Pidnyaly za tryvohoiu o 4 ranku". Shcho vidomo pro kiberataku na ukrainski derzhavni saity' (*SUSPILNE*, 14 January 2022) https://suspilne.media/197659-vnoci-hakeri-atakuvali-uradovi-sajti-i-diu/.
[18] US Department of Justice, *Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data* (26 June 2024) https://www.justice.gov/archives/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian.

Preparatory Measures in Ukraine

Intelligence reports, including information provided by international partners, open-source data analysis and assessments of the adversary's activities in cyberspace, indicated the inevitability of a cyber escalation that could be combined with a direct Russian military invasion.

Under the coordination of the NCSCC, Ukraine urgently began preparing its national cybersecurity system for the full-scale military invasion. This involved refining mechanisms for cooperation across all entities responsible for cybersecurity, developing strategic and operational response plans and making key political and managerial decisions to strengthen national cyber resilience.

In December 2021, two months before the invasion, the NCSCC conducted its first strategic-level command and staff exercise, National Cyber Readiness 2021. The exercise, attended by senior and mid-level officials from key cybersecurity agencies, focused on improving coordination in the event of a cyber escalation by Russia. The scenario was developed using intelligence and analytical data on Russian plans and intentions. In practice, approximately 80% of the exercise scenario materialised, and the exercise proved instrumental in preparing Ukraine and refining interagency cooperation mechanisms.[19]

As part of the National Cyber Readiness of Ukraine initiative, large-scale practical exercises – the GridNetwars cyber competition – were also held.[20] The event brought together 250 specialists from across Ukraine, including representatives of critical infrastructure, government agencies, private sector companies and academic institutions. Participants developed and tested practical skills to counter massive Russian cyberattacks.

In January 2022, the NCSCC convened an urgent meeting attended by the heads of all security and defence sector entities responsible for cybersecurity, including the Security Service of Ukraine, State Service of Special Communications and Information Protection, National Police, intelligence agencies and other NCSCC members, as well as the Deputy Prime Minister for Innovation, Education, Science and Technology – the Minister for Digital Transformation in Ukraine.[21] The closed-door meeting resulted in several critical decisions to protect Ukraine's critical systems and infrastructure ahead of the invasion and anticipated cyber escalation. An emergency strategic cyber defence action plan was approved.

To coordinate cybersecurity efforts, the NCSCC established an operational headquarters, where technical experts and representatives of all government agencies responsible for cybersecurity

[19] US Cybersecurity Activity in Ukraine, Facebook video (uploaded by US Embassy Kyiv, 2024) https://www.facebook.com/share/v/14bCUA7afY/.
[20] National Security and Defense Council of Ukraine, 'Ukraine's First Grid NetWars Cyber Training Has Started in Kyiv' (2 December 2021) https://www.rnbo.gov.ua/en/Diialnist/5170.html.
[21] National Security and Defense Council of Ukraine, 'O. Danilov proviv zasidannia NKTsK' (20 January 2022) https://www.rnbo.gov.ua/ua/Diialnist/5218.html.

provided 24-hour coverage. In collaboration with representatives from critical infrastructure and the private sector, the team monitored threats, made joint decisions and took proactive measures to mitigate risks. International partners also provided crucial intelligence, allowing Ukraine to take pre-emptive measures against threats. Additionally, governments and leading cybersecurity companies from around the world provided urgent support in the form of free licences, hardware and software to enhance the cyber resilience of Ukraine's state systems and critical infrastructure, bypassing bureaucratic delays.

These measures, along with the coordinated efforts and professionalism of key cybersecurity institutions, support from the private sector and international assistance, enabled Ukraine to effectively counter cyberattacks before and during the early days of the invasion, detecting and blocking most threats at an early stage.[22]

The Eve of the Invasion

From 23 to 24 February 2022, just before the full-scale invasion, massive cyberattacks targeted the telecommunications sector, satellite communications, the banking sector, transportation systems, energy infrastructure and official government websites.[23] Had these attacks been successful as a prelude to the invasion, they would have caused chaos among the population and given the enemy an informational advantage.

Despite the adversary's intentions, these attacks did not have significant consequences for Ukraine's defence capabilities or the daily lives of its citizens. The swift and effective response to these threats was due to several factors, including Ukraine's robust countermeasures, the maturity of its national cybersecurity and cyber defence system and the country's unique strategic decisions in this cyber war.

Lessons Learned: Cybersecurity Matters

The events of February 2022 in Ukraine provide a clear assessment of the role of cyber operations in modern armed conflicts. While the consequences of Russian cyberattacks cannot be compared to the widespread destruction and civilian casualties in places like Bucha[24] or Irpin,[25] their

[22] 'Ukrainski saity vytrymaly naipotuzhnishi kiberataky voroha' (*UKRINFORM*, 6 September 2022) https://www.ukrinform.ua/rubric-technology/3565926-ukrainski-sajti-vitrimali-najpotuznisi-kiberataki-voroga-zelenskij.html.
[23] Mitchell Orenstein, 'Russia's Use of Cyberattacks: Lessons from the Second Ukraine War' (*Foreign Policy Research Institute*, 7 June 2022) https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/.
[24] Viacheslav Shramovych, 'Skilky liudei zahynulo u Buchi pid chas rosiiskoi okupatsii: onovleni dani' (*BBC Ukraine*, 21 March 2025) https://www.bbc.com/ukrainian/articles/c3w13v8z6z1o.
[25] 'Ubytykh rozdavliuvaly tankamy y zakatuvaly v asfalt': v Irpeni zahynulo do 300 myrnykh zhyteliv' (*ZN.UA*, 30 March 2022) https://zn.ua/ukr/UKRAINE/ubitikh-rozdavljuvali-tankami-j-zakatuvali-v-asfalt-v-irpeni-zahinulo-do-300-mirnikh-zhiteliv-mer-mista.html.

potential impact should not be underestimated. If Ukraine's cybersecurity system had not been prepared and in the first days of the invasion its citizens had lost access to communication and the internet due to successful attacks on the telecom sector, had been unable to buy food or medicine due to disruptions in payment systems, or had faced power and heating outages caused by cyberattacks on the energy sector, the enemy would have had a significant advantage.

Ukraine's experience has shown that a well-structured cyber defence, the implementation of proper security practices and continuous personnel training have a tangible effect. Cyber operations ultimately failed to become a decisive factor in the conflict. The only cyberattack with a noticeable impact was the successful breach of the Viasat satellite communication system[26] which supported Ukraine's Armed Forces. However, this system was outside Ukraine's cybersecurity perimeter and not directly under national protection.

Creation of the IT Army

An unprecedented phenomenon in Ukraine's cyber resistance during the full-scale Russian invasion was the establishment of the IT Army and the rapid involvement of private sector specialists (cyber volunteers) in the country's cyber defence efforts.

The foundation for this initiative was laid by the Decision of the National Security and Defence Council of Ukraine, 'On Urgent Measures for the Cyber Defence of the State', enacted by the Presidential Decree on 26 August 2021,[27] which provided for the creation of cyber forces in the system of the Ministry of Defence of Ukraine. This meant that six months before the war, discussions had already begun on forming cyber forces and engaging volunteers. Cybersecurity specialists began reaching out to state authorities, primarily the NCSCC, which had initiated this Decision of the NSDC of Ukraine, expressing their willingness to join the effort. Their information was collected and stored for potential mobilisation.[28]

On 26 February 2022, the Ministry of Digital Transformation announced the formation of the IT Army, which, according to published data, included around 300,000 participants.[29] There were not only Ukrainian citizens, but also individuals from other countries who supported Ukraine and were willing to contribute to its cyber defence.

[26] Nadiia Sobenko, 'YeS zvynuvatyv Rosiiu u zlami suputnykiv Viasat za hodynu do vtorhnennia v Ukrainu', (*SUSPILNE*, 10 May 2022) https://suspilne.media/237923-es-zvinuvativ-rosiu-u-zlami-suputnikiv-viasat-za-godinu-do-vtorgnenna-v-ukrainu/.
[27] Rada natsionalnoi bezpeky i oborony Ukrainy, Pro nevidkladni zakhody z kiberoborony derzhavy, 14 travnia 2021 roku, https://zakon.rada.gov.ua/laws/show/n0053525-21#Text.
[28] UKRINFORM, 'Ukrainskykh fakhivtsiv zaproshuiut do kiberviisk – yak doluchytys' (15 February 2022) https://www.ukrinform.ua/rubric-technology/3405510-ukrainskih-fahivciv-zaprosuut-do-kibervijsk-ak-dolucitis.html.
[29] Yuliia Kozina, «Aktyvno atakuiemo RF». Ukrainska IT-armiia nalichuie 300 tysiach spetsialistiv — Mintsyfry (18 March 2022) https://biz.nv.ua/ukr/tech/it-viyska-ukrajini-atakuyut-rosiyski-sayti-mincifra-ostanni-novini-50226311.html.

Cyber volunteers began launching cyberattacks against the enemy. Their activities demonstrated that Ukraine could not only defend itself but also conduct offensive cyber operations. These included large-scale DDoS attacks, defacing of Russian websites, attacks aiming at causing maximum damage to the Russian economy and reducing the aggressor's military and financial resources, and blocking hostile media propaganda.[30]

Pro-Ukrainian hacktivism played a crucial role, especially in the early stages of the conflict, helping to tie up Russian Cyber Forces that could have otherwise been deployed in offensive operations. The creation of this cyber army was unique to Ukraine in this war, as despite the lack of centralised coordination, pre-established mechanisms and a clear legal framework, the self-organised, sometimes chaotic efforts of the cyber volunteers significantly contributed to Ukraine's cyber resistance and debunked the myth of Russia's invincible hackers.

Some experts argue that the IT Army mainly served as a distraction, creating 'white noise' to cover for high-level cyber operations conducted by Ukraine's key cybersecurity institutions, including the Security Service of Ukraine, the State Service of Special Communications, intelligence agencies and the National Police. In some cases, volunteer actions may have even interfered with complex cyber operations.

Over time, many of the most skilled hacktivists officially joined military and security institutions as part of Ukraine's national cybersecurity system through voluntary mobilisation.

The existence of regular cyber forces as a part of Ukraine's army before the invasion greatly increased Ukraine's strategic capacities for cyber defence, including offensive and defensive cyber operations. Unfortunately, in the absence of the relevant law, the task of creating Ukraine's Cyber Forces has not yet been implemented.

Features of the Activities of Key Entities in the National Cybersecurity System

Despite the assistance of cyber volunteers and international partners, the primary burden of cyber defence in the early weeks of the war was borne by Ukraine's key cybersecurity institutions, including the Security Service of Ukraine, the State Service of Special Communications and Information Protection, the General Staff of the Armed Forces, the Ministry of Defence, military intelligence, foreign intelligence, border security, the National Police and the National Bank of Ukraine.

[30] Anna Nahorna, Naizhorstkishi kiberataky, deanon khaktyvistiv ta spivpratsia z HUR. Interviu z kuratorom IT ARMY of Ukraine, (*SPEKA*, 31 January 2024) https://speka.media/intervyu-z-kuratorom-it-army-of-ukraine-v7ylqy.

One distinctive feature of Ukraine's national cybersecurity system is that most of its key entities are military structures, with the exception of the National Bank. Such militarisation of national cybersecurity could have raised some concerns in terms of democratic civilian control. However, in practice, this military-driven structure played a crucial role in ensuring coordination and efficiency. The personnel of these institutions upheld their military duty during the critical first weeks of the war, while some civilian employees, including government officials, fled their workplaces or even the country to protect themselves and their families.[31]

From the first days of the full-scaled invasion, interagency cooperation and coordination between key cybersecurity entities significantly intensified. Traditional institutional competition was set aside in favour of the collective priority of countering Russian cyber aggression and protecting the country.

The National Cybersecurity Coordination Centre established a Joint Cyber Incident Response Group, comprising representatives from all NCSCC member institutions. Specific mechanisms for practical cooperation in responding to cyber threats were defined, and the group was led by the Deputy Head of the NCSCC.

Developing a Human Cyber Force Through Promoting the Role of Women

As a result of the ongoing cyber war, Ukraine has gained a unique asset that no other European country currently possesses – specialists with practical experience in cyber warfare, including both defensive and offensive cyber operations conducted in real combat conditions.

However, despite this advantage, the shortage of IT and cybersecurity professionals remains a pressing issue. A significant number of these specialists, most of whom are men, have been mobilised into the Armed Forces of Ukraine. Under martial law, Ukrainian men are fulfilling their constitutional duty by defending the country on the front lines and resisting the aggressor. This situation makes the increased involvement of women in cybersecurity more important than ever.

In Ukraine's current circumstances, gender equality is not just a matter of social justice and human rights but a critical necessity for the survival of the state and the continued operation of key economic and national security sectors, including cybersecurity and IT. Therefore, promoting women's participation in these fields has become an integral part of Ukraine's cybersecurity policy. To implement this, in September 2024, the NCSCC, in collaboration with the Foundation for Women's Leadership and Strategic Initiatives, launched a national initiative to enhance the

[31] Slovo i Dilo, U NADS rozpovily, skilky chynovnykiv vtratyly robotu cherez viinu, (11 May 2022), https://www.slovoidilo.ua/2022/05/11/novyna/suspilstvo/nads-rozpovily-skilky-chynovnykiv-vtratyly-robotu-cherez-vijnu.

role of women in cybersecurity.[32] This initiative brings together government cybersecurity entities, civil society, educational institutions and the private sector to support and expand women's involvement in cybersecurity.[33]

Cyber Threat Landscape

Since the invasion, Russian cyber aggression against Ukraine has been carried out exclusively by hacker groups that are either structural units of or controlled by Russian intelligence services. There are no independent 'hacktivists' in Russia and any illegal activity in cyberspace is strictly controlled by the state.[34]

At the start of the invasion, Russian hacker attacks were primarily destructive, aimed at data destruction, system disruptions, and high-profile defacements that spread Russian propaganda. However, the activities of Russian hacker groups have shifted predominantly toward intelligence gathering and cyber espionage, although destructive cyber influence remains one of their aims. If cyberattacks primarily targeted the military sector and government institutions at the beginning of the invasion, over time, the enemy has shifted its focus toward inflicting maximum damage on the civilian population.[35]

The most active APT groups include: **Armageddon (FSB Russia)**, primarily targeting government agencies; **Sandworm (GRU Russia)** focusing on energy sector enterprises; and **Turla (FSB Russia)** targeting defence sector enterprises and organisations to gain access to situational awareness systems.[36]

Cyberattacks on Ukraine's infrastructure involve not only Russian intelligence agencies but also financially motivated criminal groups under their control, including ransomware groups. To enhance these cybercriminal groups' capabilities, Russian intelligence services provide access to advanced technologies, vulnerabilities and cyberattack tools, including those targeting mobile devices. This raises the risk of the uncontrolled proliferation of cyber weapons that were previously accessible only to state actors.[37]

[32] NCCC, The NCCC has decided to restrict the use of Telegram in government agencies, military formations, and critical infrastructure facilities, 20 September 2024, https://www.rnbo.gov.ua/en/Diialnist/6994.html.
[33] NCCC, The role of women in strengthening Ukraine's cyber resilience was the main topic of the meeting of the National Cybersecurity Cluster, 18 December 2024, https://www.rnbo.gov.ua/en/Diialnist/7087.html.
[34] AJ Vicens, Pro-Russian hacktivism isn't real, top Ukrainian cyber official says, (*CYBERSCOOP*, 27 April 2023), https://cyberscoop.com/pro-russia-hacktivism-ukraine/.
[35] SSSCIP, Russian Cyber Operations: Attack Automation, Espionage Against Defense Sector, and New Tactics. Analysis for the Second Half of 2024 (30 April 2025) https://cip.gov.ua/en/news/russian-cyber-operations-attack-automation-espionage-against-defense-sector-and-new-tactics-analysis-for-the-second-half-of-2024.
[36] SSSCIP, Russian Cyber Operations: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups (September 2023) https://cip.gov.ua/services/cm/api/attachment/download?id=60201.
[37] NCCC, Landshaft kiberzahroz Ukrainy v 2023 rotsi (2024) https://ua.understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_ua.pdf.

A common tactic involves phishing emails and messages aimed at gaining unauthorised access to the personal accounts of Ukrainian military personnel and law enforcement officers in messaging platforms such as Telegram, Signal and WhatsApp.[38]

The enemy also conducts large-scale, destructive cyber operations aimed at disabling infrastructure and erasing data. There have been several notable cyberattacks since the invasion. The December 2023 attack on Kyivstar, one of Ukraine's three largest mobile operators, left 10 million users without communication and internet access and prevented them from receiving air raid alerts.[39] In January 2024, there was a cyberattack on one of the country's largest data centres in Kyiv, which provided services to government institutions.[40] Later that year, in December 2024, there was an attack on Ukraine's state registries, leading to the suspension of around 60 registries of the Ministry of Justice of Ukraine, disrupting essential public services.[41]

Russian intelligence-controlled pseudo-hacktivist groups such as NoName057(16), UserSec, 22C and CyberArmy of Russia continuously carry out DDoS attacks on government institutions, financial enterprises, transportation, the defence sector and other Ukrainian organisations.[42]

Compared to 2022, there is now greater coordination between Russian cyberattacks and its military and information operations. The intensity of cyberattacks and the selection of priority targets, whether specific facilities, regions or sectors, are increasingly synchronised with military actions and kinetic strikes on Ukrainian infrastructure.[43] Compromised information systems, including operational technology (OT) devices such as surveillance cameras in targeted areas, are used to analyse the effect of missile and drone strikes.[44] Data stolen in cyberattacks and defacements of government websites and media outlets are also exploited in influence operations.

An analysis of cybercrime trends reveals the widespread increase of attacks targeting user accounts on social networks and messaging apps, particularly through phishing links designed to steal personal data. Every day in Ukraine, an average of 10,000 to 15,000 people click on phishing links, making them potential fraud victims. In 2023 alone, there were over 1.9 million recorded

[38] SSSCIP, Russian Cyber Operations: Attack Automation, Espionage Against Defense Sector, and New Tactics. Analysis for the Second Half of 2024 (30 April 2025) https://cip.gov.ua/en/news/russian-cyber-operations-attack-automation-espionage-against-defense-sector-and-new-tactics-analysis-for-the-second-half-of-2024.
[39] Yurii Tarasovskyi, 'Khakery perebuvaly v systemi «Kyivstaru» z travnia 2023 roku. SBU rozkryla detali kiberataky' (*Forbes*, 4 January 2024) https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307.
[40] Yurii Tarasovskyi, 'Kiberataka na data-tsentr «Parkovyi». Kompaniia obitsiaie vidnovyty povnyi dostup do danykh protiahom 48 hodyn' (*Forbes*, 26 January 2024) https://forbes.ua/news/kiberataka-na-data-tsentr-parkoviy-kompaniya-obitsyae-vidnoviti-povniy-dostup-do-danikh-protyagom-48-godin-26012024-18812.
[41] Diana Kuryshko, 'Reiestry vidnovyly. Yaki naslidky kiberataky dlia Ukrainy', (*BBC Ukraine*, 24 January 2025) https://www.bbc.com/ukrainian/articles/c5ye75y8415o.
[42] SSSCIP, Russian Cyber Operations: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups(September 2023) https://cip.gov.ua/services/cm/api/attachment/download?id=60201.
[43] SSSCIP, 'Cyber, Artillery, Propaganda. General Overview of the Dimensions of Russian Aggression' (17 January 2023) https://cip.gov.ua/en/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.
[44] IQ Trading, 'rosiia vykorystala zlamani kamery videosposterezhennia pid chas povitrianoi ataky na Kyiv' (*IQ Trading*, 2024) https://iqtrading.ua/materials/moy_iq/press-centr/news/iq_trading_ipvm_shinese_cameras_hacking_by_russia.html.

phishing link visits.[45] Russian cybercriminals not only steal money from Ukrainian citizens, but also transfer all collected personal data to the Russian intelligence services for use in reconnaissance and subversive activities. Russian intelligence services are using cybercriminals' tools to keep their cash-strapped operations running. There is likely to be no independent cybercriminal groups in Russia, as such activities are under the control of law enforcement and intelligence agencies.[46] [47]

To counter cyber fraud, particularly phishing scams, in 2023, the NCSCC, in collaboration with the National Bank of Ukraine and the National Centre for Operational and Technical Management of Telecommunications Networks under the State Service of Special Communications, implemented a Protective Domain Name System. This tool has proven to be an effective measure against cyber fraud. Protective domain name system (DNS) redirects users to a webpage with a threat warning and cyber hygiene recommendations when attempting to visit a phishing site. The system analyses only sites that have signs of financial phishing. More than 300 Ukrainian providers with a responsible attitude towards their customers have already joined the system.[48]

Russian intelligence agencies have also increased their control over pseudo-hacktivist groups. Since late 2022, Russian intelligence has taken full command of all pro-Russian hacktivist groups, directing their activities toward achieving Russia's military and political objectives. Russia has developed a 'turnkey' methodology for creating, disguising and managing these pseudo-hacktivist groups, deploying them strategically based on geopolitical goals. For example, following the 7 October 2023 terrorist attack in Israel, dozens of new pseudo-hacktivist groups were launched to attack Israeli infrastructure. During this period, Ukraine saw its lowest number of cyber incidents in years. By late 2023, a trend had emerged where some pseudo-hacktivist groups, still controlled by Russian intelligence, began monetising their cyberattack services.[49]

One of Russia's primary tools for cyber and information operations, including the discrediting of political figures, election interference, malware distribution, fraud coordination, illicit substance trafficking and the mobilisation of pro-Russian hacktivist communities, is the Telegram online platform.

Given its extensive use in malicious activities, and due to its potential impact on the EU's digital space, Telegram should be designated as a Very Large Online Platform (VLOP) under the EU's Digital Services Act (DSA) regulations. Designation as a VLOP would trigger stricter DSA

[45] Oleksii Shaban, 'Finansove shakhraistvo. Yak protydiiaty kibershakhraistvu u finansovomu sektori', (*delo.ua*, 26 May 2023) https://delo.ua/opinions/finansove-saxraistvo-yak-protidiyati-kibersaxraistvu-u-finansovomu-sektori-418081/.
[46] Antoaneta Roussi, 'Russia taps cybercriminals to keep military pressure on Ukraine', (*Politico*, 12 February 2025) https://www.politico.eu/article/russia-cybercriminal-military-pressure-ukraine/.
[47] Adam Janofsky, 'From the front lines of "the first real cyberwar"', (*The Record*, 20 April 2022) https://therecord.media/from-the-front-lines-of-the-first-real-cyberwar.
[48] NCCC, During the first month of operation of the Protective DNS system, losses of Ukrainians from financial phishing decreased by more than 30%, (16 March 2023), https://www.rnbo.gov.ua/en/Diialnist/6184.html.
[49] SSSCIP, Russian Cyber Operations: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups (September 2023) https://cip.gov.ua/services/cm/api/attachment/download?id=60201.

obligations, including enhanced content moderation, transparency measures, and risk assessments, particularly concerning disinformation, illegal content, and potential harm to users.

Russian special services have access to Telegram users' private correspondence, even deleted messages, and to their personal data. Telegram is actively used by Russia for cyberattacks, spreading phishing and malware, establishing users' geolocation and adjusting missile strikes against military objectives.

Because of these threats, on 19 September 2024, the NCSCC issued official recommendation for state bodies, military personnel and critical infrastructure facilities do not use Telegram for work activities or the transmission of official information.[50]

Russia's Cyber War Against the EU: Cyberattacks, Information Operations and GPS Disruptions

Russia is now waging a full-scale information and cyber war not only against Ukraine but also against EU countries, continuously expanding its capabilities for special information and cyber operations while deploying new methods and tactics.[51] The number of Russian cyberattacks targeting EU and NATO countries is steadily increasing.[52] These attacks focus on national government institutions, critical infrastructure operators, politicians and the logistics, defence, aerospace, energy and IT sectors.

Russia has also developed a new tactic involving combined attacks on EU satellite systems, which will likely continue to expand if European countries fail to respond adequately. This tactic includes blocking satellite signals through hacking tools and jamming broadcast signals using electronic warfare systems. This destructive activity indicates Russia's efforts to master new hybrid tactics aimed at testing sabotage operations in the information domain, particularly by disrupting European satellite communications systems. The increasing duration of Russian signal jamming demonstrates its growing capabilities to disrupt global satellite networks. As a result of this malicious activity, significant disruptions have been observed in the Global Navigation Satellite System especially affecting safety of civil aviation flights in EU.[53]

[50] NCCC, The NCCC has decided to restrict the use of Telegram in government agencies, military formations, and critical infrastructure facilities, (20 September 2024), https://www.rnbo.gov.ua/en/Diialnist/6994.html.
[51] EBU Investigative Journalism Network, Playing With Fire: Are Russia's hybrid attacks the new European war?, (12 March 2025), https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/.
[52] Derek Gatopoulos, 'Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many', (APNews, 29 May 2024) https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd458df77a60440c.
[53] Vitaly Shevchenko, 'Russia blamed for GPS interference affecting flights in Europe ' (*BBC*, 2 May 2024)https://www.bbc.com/news/articles/cne900k4wvjo.

Russia may have been carrying out these operations by interfering with the Hot Bird 13 (France) and Astra-4A (Luxembourg) satellite networks, using the capabilities of the Medvezhi Ozera Space Communications Centre, a facility controlled by the Moscow Power Engineering Institute[54] in combination with cyberattacks. This activity suggests that Russian intelligence services are actively testing technical tools to block EU satellite communications, potentially as a preparation for future operations against Ukraine's partner countries and a trial run for an attack scenario on EU nations.

On 3 May 2024, the EU, NATO and several European countries, including Germany and the Czech Republic, issued an official public statement condemning Russian cyber aggression against the Euro-Atlantic community, warning of the full range of measures to prevent, deter and respond to such threats.[55] However, this had no deterrent effect on the aggressor.

Just a few days later, on 9 May 2024, Russia conducted a special information operation aimed at demonstrating its military superiority and psychologically influencing the populations of Ukraine and the Baltic states. This operation involved interference with the Astra 4A (Luxembourg) and Hot Bird 13E (France) satellites, along with a cyberattack on the Latvian telecommunications provider, Balticom.[56] As a result, national television channels in both Ukraine and Latvia simultaneously broadcast footage of Russia's Victory Day military parade on Red Square, replacing their regular programming.

This was Russia's first large-scale operation of its kind in which hostile content replacement occurred simultaneously in both Ukraine and an EU country. This attack could also be interpreted as a political signal to the Baltic states regarding the Kremlin's geopolitical ambitions. By forcibly broadcasting the 9 May military parade, Russia effectively subjected the population of a Baltic country to an aggressive propaganda event, demonstrating its ability to manipulate satellite communications beyond Ukraine and raising concerns about potential future hybrid operations in the region.

Russia's Election Interference and the Potential Consequences of US Policy Changes on Countering Disinformation

Russia is waging a full-scale war not only against Ukraine but also against the European Union in cyberspace. Its primary objective is not just to disable critical systems, block government

[54] *UKRINFORM*, RF atakuvala suputnykove movlennia Ukrainy - pryzupynena transliatsiia maizhe 40 kanaliv, (17 April 2024) https://www.ukrinform.ua/rubric-society/3853679-rf-atakuvala-suputnikove-movlenna-ukraini-prizupinena-translacia-majze-40-kanaliv.html.
[55] Alexander Martin, 'NATO and EU condemn 'intensifying' Russian sabotage and hybrid operations' (*The Record*, 3 May 2024) https://therecord.media/nato-eu-condemn-russian-sabotage-hybrid-operations.
[56] *BalticTimes*, 'Kremlin propaganda aired on Balticom TV as a result of cyberattack', (9 May 2024) https://www.baltictimes.com/kremlin_propaganda_aired_on_balticom_tv_as_a_result_of_cyberattack/.

websites or steal personal data, but to influence EU populations through intimidation, destabilisation and discrediting the ability of governments to ensure security. The ultimate goal is to interfere in electoral processes to bring to power individuals who can once again promote Russian interests within the EU.

The election interference and situation in Romania has already demonstrated that Russia possesses such capabilities,[57] which will only continue to grow. Unfortunately, this is further facilitated by shifts in US policy on countering disinformation.[58] Major internet platforms such as META (Facebook/Instagram), Alphabet (Google/YouTube) and X, all of which fall under US regulatory jurisdiction, are stopping the use of fact-checking mechanisms, content moderation and measures against manipulative content and disinformation. Current data indicates that Russian influence operations are increasing exponentially. This suggests that in the future, Russia will not be limited to using TikTok to interfere in European elections.

Regarding the policy of the new US administration, which has publicly stated that content moderation is an infringement on free speech, it is worth recalling one of the first offensive operations conducted by US Cyber Command under President Trump's first term. On 5 November 2018, just before the US midterm elections, USCYBERCOM, acting on intelligence about potential Russian election interference, disabled the operations of Russia's Internet Research Agency (the 'troll factory' in St. Petersburg) for several days.[59] According to the then-head of US Cyber Command, Paul Nakasone, demonstrating offensive cyber capabilities served as a deterrent to adversaries.[60] As a result, in the following years, the level of cyberattacks and unlawful interference in the US electoral process significantly declined.

This was the first publicly acknowledged offensive cyber operation by the US government, marking a significant expansion of USCYBERCOM's mandate. During Trump's presidency, in 2018, the US broadened its authorisation for offensive cyber operations, granting permission to conduct disruptive cyber activities in enemy cyberspace pre-emptively,[61] even short of full-scale military conflict.

While freedom of speech is a core democratic value, the US remains the only country in the Euro-Atlantic community with the capability to neutralise Russia's technical means of spreading disinformation. As a result, the US may no longer feel the need to moderate online content. This

[57] Eliza Gkritsi, 'EU opens investigation into TikTok and the Romanian election' (*Politico*, 17 December 2024) https://www.politico.eu/article/eu-opens-investigation-into-tiktok-over-romanian-election/.
[58] Clare Duffy, 'Meta is getting rid of fact checkers. Zuckerberg acknowledged more harmful content will appear on the platforms now' (*CNN*, 7 January 2025) https://edition.cnn.com/2025/01/07/tech/meta-censorship-moderation/index.html.
[59] Ellen Nakashima, 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms' (*WashingtonPost*, 27 February 2019) https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
[60] Julian E. Barnes, 'U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections' (*NYT*, 18 October 2018) https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.
[61] Ellen Nakashima, 'White House authorizes 'offensive cyber operations' to deter foreign adversaries' , (*WashingtonPost*, 20 September 2018), https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

certainly has an impact on European countries, which are most likely facing complex dilemmas as a result.

The discontinuation of US funding for international assistance programmes, including grants for media projects, educational programmes on critical thinking and fact-checking platforms, has also significantly weakened efforts to counter Russian influence. In many Eastern European countries, including Ukraine and Moldova, the majority of disinformation countermeasures in the private sector, NGOs and even government institutions have been funded through US support.[62]

This means that there is no longer disinformation moderation on major internet platforms (the US has even lifted its previous ban on TikTok) and there is no financial support for young democracies to counter Russian disinformation, despite the fact that these countries remain the most vulnerable and primary targets of Russian influence. As a result, the adversary is expected to gain even greater opportunities, and this threat is not just relevant to Ukraine but is even more pressing for EU countries.

This emphasises the importance of international cooperation and the necessity to take proactive measures. Within the framework of cooperation between Ukraine and the EU, new joint proactive mechanisms of countering Russian aggression in cyberspace and the information domain should be implemented, drawing on Ukraine's experience.

Both Ukrainian and European cybersecurity would benefit from the establishment of a Cyber Alliance comprising EU nations, the United Kingdom and Ukraine. This alliance would combine Ukraine's battlefield expertise with the technological capabilities and resources of partner nations to enhance intelligence sharing, cybersecurity resilience for networks and critical infrastructure and the ability to conduct both defensive and offensive cyber operations when national and collective security is at risk. Such an alliance would also play a crucial role in deterring hostile actors, including combating disinformation.

Cyber Operations and International Law

Practical examples of Russian cyberattacks against Ukraine demonstrate that cyber operations are an integral part of modern warfare and that attacks on critical infrastructure directly threaten the safety and livelihoods of civilians. Russia's cyberattacks against Ukraine and the EU will likely continue beyond direct military actions in Ukraine, also taking the form of hybrid operations below

[62] Anita Prasad, 'Maizhe 60% zhurnalistiv ochikuiut katastrofichnykh naslidkiv dlia media vid zupynky dopomohy SShA – opytuvannia IMI', (*Forbes*, 4 February 2025), https://forbes.ua/news/mayzhe-60-zhurnalistiv-ochikuyut-katastrofichnikh-naslidkiv-dlya-media-vid-zupinki-inozemnoi-dopomogi-ssha-opituvannya-imi-04022025-26868.

the threshold of use of force. One of the key tasks for both Ukraine and EU countries is thus to ensure their own offensive capabilities to pre-empt potential threats and protect national interests.

Conducting offensive cyber operations to gain covert control over enemy military systems, with the ability to disable them in case of an escalation and neutralising technical capabilities that could be used by malicious actors against national and collective EU interests could become an effective element of collective cyber defence and deterrence. International dialogue on the challenges posed to international law in modern realities, ways to address them and the formation of a common baseline approach to these issues is therefore needed.

There is a global consensus that existing international law, including international humanitarian law, fully applies in the cyber domain; however, the question is how these rules apply. Most of the existing legal frameworks were created long before cyberspace was even thought of, and there is no specific international treaty governing state behaviour in cyberspace. While international armed conflict arises when there is a resort to armed force between states and there is no minimum intensity requirement, this has typically involved the use of violence and tangible weapons, resulting in casualties or physical destruction of objects and infrastructure.

Now that societies heavily rely on critical information infrastructures, cyberattacks can have a significant impact and cause great harm, but the governing rules were developed focusing on physical domains and kinetic effects, which are not always simple to apply in the cyber realm. For example, the drafters of the Geneva Conventions could not have foreseen that cyberspace would emerge and become a domain of conflict, so there are no specific provisions about the protection of digital assets, even though they can be critically important, for example, for hospitals or for the survival of the civilian population. Neither is there any judicial practice of the International Criminal Court (ICC) in this sphere, although the concept of cyber war crimes has already emerged in expert discussions,[63] and recently, the ICC's Office of the Prosecutor has launched a public consultation on policy on cyber-enabled crimes under the Rome Statute.[64]

Such uncertainty and lack of judicial guidance have led to divergent interpretations of certain aspects of IHL by states. This is reflected in national positions on how international law applies to cyber activities, and there are different approaches as to what conduct would be considered unlawful, forming a grey zone within which the militarisation of cyberspace has rapidly advanced over the past decade. Many countries have created cyber forces, and their doctrinal documents

[63] Yola Verbruggen, 'Cyberattacks as War Crimes' (10 January 2024) *International Bar Association* https://www.ibanet.org/Cyberattacks-as-war-crimes.
; David P. Fidler, 'CyberWar Crimes: Islamic State Atrocity Videos and the Laws of War,' *Computer Law Review International*, vol. 16, no. 6, 2015, pp. 161–165. https://doi.org/10.9785/cri-2015-0603.
[64] The Office of the Prosecutor, 'ICC Office of the Prosecutor launches public consultation on policy on cyber-enabled crimes under the Rome Statute' (7 March 2025) https://www.icc-cpi.int/news/icc-office-prosecutor-launches-public-consultation-policy-cyber-enabled-crimes-under-rome.

now include the term ‘cyber operations’.[65] However, uncertainties persist about how international rules apply to these and when legal thresholds are crossed.

It is clear that Ukraine has the legal right to respond to Russia’s armed aggression also by using force in self-defence in accordance with Article 51 of the UN Charter, and therefore it may conduct cyber operations that cross the threshold of use of force. However, other European countries cannot (and do not) conduct cyberattacks above the use of force threshold (as it would be violation of Art 2(4) UN Charter in the absence of an armed attack against them), despite being victims of Russia’s hybrid aggression. There is also insufficient clarity on what lawful response options are at the disposal of these countries in such cases. Despite the murky picture, an increasing number of countries are developing their own cyber forces, already have offensive cyber capabilities and the ability to respond, but the boundaries of their conduct remain unsettled. Recently, the President of the European Commission stated that the EU should establish cyber forces with offensive capabilities.[66] This, and similar initiatives make it important to clarify how existing international rules apply to cyber operations, as international law must serve as the legal foundation for the activities of democratic nations.

Based on Ukraine’s experience, there are many pressing questions remaining with regard to the legal and ethical frameworks applicable to state conduct in cyberspace. While espionage is considered illegal under the national laws of most countries, it is not outlawed under international law. Thus, it would be counterproductive and short-sighted to equate all cyber operations with intelligence activities regardless of their effects, as it would create an essentially lawless sphere and allow states to evade accountability for wrongdoing and intentionally harming others. These issues require attention because interstate cyber conflicts will only intensify. Cyber operations, including those leveraging artificial intelligence, will not be limited to intelligence agencies and military structures but will increasingly affect civilian populations. It is important to develop a shared understanding and reach international baseline consensus on these matters in accordance with the existing international legal frameworks**.**

Conclusions

Ukraine’s experience has highlighted the crucial role of cyber defence as an integral component of national security, particularly under conditions of hybrid aggression and following full-scale invasion. The rapid evolution of emerging technologies, including artificial intelligence, combined

[65] Bondarenko I.D and Shestakov V.I, ’Russian Cyberattack on Ukraine – A War Crime’m Yurydychnyi naukovyi elektronnyi zhurnal, No 11, 2023, pp. 614 – 619. I https://doi.org/10.32782/2524-0374/2023-11/152.
[66] Alexander Martin, ’EU Council president proposes ‘European cyber force’ with ‘offensive capabilities’’, (*The Record*, 1 December 2023) https://therecord.media/offensive-cyber-force-proposal-european-council-president.

with the global digitalisation and the growing militarisation of cyberspace, has only increased its importance.

Ukraine has demonstrated a high level of cyber resilience and maturity in the face of Russian cyber aggression, setting an example for Western countries and offering valuable lessons for partner nations seeking to enhance their own cybersecurity postures. Drawing from Ukraine's experience, the following twelve elements appear to be especially relevant for building effective national cyber defence capabilities:

1. Establishment of cyber forces as a regular military structure responsible for cyber defence;
2. Clarification, and establishment where appropriate, of legal and organisational frameworks for conducting defensive and offensive cyber operations both in peacetime and during a war;
3. Proven mechanisms for urgent involvement of private sector specialists in cyber defence activities in case of necessity;
4. Policy and organisational mechanisms for providing physical protection of critical information systems in case of a military threat, including procedures for its relocation;
5. Ensuring obligatory data back-ups for all critical information systems;
6. Constant strengthening of cyber protection of state bodies, armed forces and critical infrastructure and raising the cyber hygiene level of their employees and military personnel;
7. Persistent development of human cyber force, including through promoting the role of women;
8. Development of public-private partnerships, defining the role and responsibilities of large private IT businesses in cyber defence in case of a serious threat to national security and military aggression;
9. Ensuring effective coordination mechanisms between state structures, the private sector and international partners in times of crisis;
10. Restricting the use of Russian software products and messengers, in particular Telegram;
11. Implementing a national DNS; and
12. Development of international cooperation that would that would provide for the creation of joint practical mechanisms to prevent and counter Russian cyber threats.

Ukraine's experience underscores the strategic value of preparedness, adaptability and multilateral collaboration in the cyber domain. However, Russia is waging an open and cynical cyber war not only against Ukraine but also against the EU, whose member states are even more vulnerable. Unlike Ukraine, which has experience, skilled personnel, technical capabilities, a deep understanding of enemy tactics and the legal grounds under wartime conditions to conduct offensive cyber operations, EU countries lack these advantages.

Russia's cyber aggression against both Ukraine and other European countries will persist even after the active phase of the war in Ukraine ends, which presumably will stipulate and give the aggressor further possibilities to relocate resources from providing for open military actions on the battlefield toward intensified arms build-ups in the cyber domain.

In light of evolving cyber threats, consideration could be given to the formation of a Cyber Alliance comprising EU member states, the United Kingdom and Ukraine. Such an initiative might benefit from integrating Ukraine's operational experience and skilled personnel with the technological capabilities and resources of its European partners.

This form of cooperation could contribute to enhanced intelligence sharing, increased resilience of digital networks and critical infrastructure and the development of coordinated approaches to both defensive and, where appropriate, offensive cyber operations in situations that pose a threat to national or collective security. Additionally, the establishment of such an alliance may serve a deterrent function, signalling a shared commitment to cybersecurity, international peace and stability, while remaining grounded in the principles of international law.