CyberPeace Institute

Quarterly Analysis Report
Q3 July to September 2023

Cyber Dimensions
of the Armed Conflict in Ukraine

TABLE OF CONTENTS

Background

January 2022 - September 2023

Since the start of the armed invasion of Ukraine in February 2022, the CyberPeace Institute has been documenting cyberattacks against critical infrastructure and civilian objects in Ukraine and the Russian Federation and cyberattacks against targets beyond the two belligerent countries. Between January 2022 and September 2023, the CyberPeace Institute has documented a total of 2776 cyber incidents conducted by 106 different threat actors. The data is available through the Cyber Attacks in Times of Conflict Platform[1] #Ukraine.

574 incidents against entities in **Ukraine**

People's CyberArmy (217) has been the most active hacktivist collective threat actor, while *Sandworm (21)* has been the most active Russian state-sponsored threat actor since the start of the February 2022 military invasion of Ukraine.

Top 5 targeted sectors:

- Public administration (132)
- Financial (63)
- Media (61)
- ICT (59)
- Energy (31)

306 incidents against entities in the **Russian Federation**

Anonymous Italia (62) has been the most active hacktivist collective, while the *IT Army of Ukraine (75)* has been the most active Ukrainian state-sponsored threat actor since the start of the 2022 military invasion of Ukraine.

Top 5 targeted sectors:

- Public administration (50)
- Financial (44)
- ICT (31)
- Media (30)
- Transportation (25)

1896 incidents against entities in **other countries**

Top 5 targeted countries:

- Poland (315)
- Lithuania (157)
- Germany (136)
- United States (101)
- Estonia (93)

Top 5 targeted sectors:

- Public administration (575)
- Transportation (372)
- Financial (199)
- Manufacturing (122)
- Media (99)

The remainder of this report focuses on the incidents documented by the CyberPeace Institute in the third quarter of 2023; July 1 until September 30, 2023.

Trends and Emerging Issues Q3 2023

Ukraine

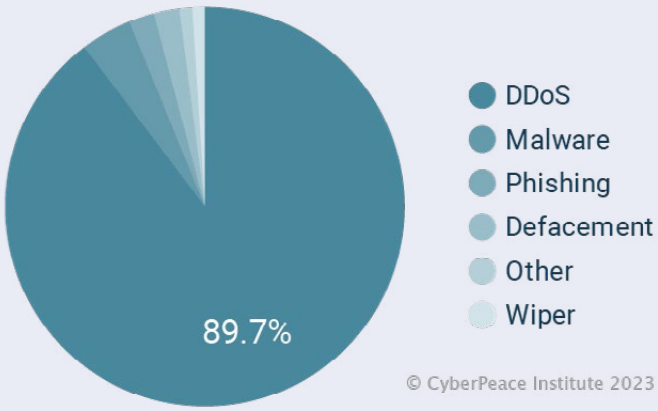
Incidents	Sectors	Threat Actors
97	16	15
↓ -14.1%	↓ -5.9%	↓ -6.3%

Daily evolution of cyber incidents impacting entities in Ukraine [July - September 2023]

Trends

- DDoS attacks account for 89% of all incidents. The most targeted sectors were the public administration (19), media (15), ICT (15), financial (10), and trade (8).
- One Ukrainian nonprofit organization was targeted by a possible DDoS attack.

Types of cyber incidents targeting entities in Ukraine



Five incidents, targeting Ukrainian entities, were attributed to state-sponsored actors:

- Two incidents have been attributed to *APT28*[2], a Russian state-sponsored actor[3]:
  - CERT-UA[4] reported on a phishing campaign to obtain authentication data for Ukrainian public mail services. The Ukrainian team discovered HTML files imitating the interface of mail services used to exfiltrate authentication data entered by the target using HTTP POST requests, transfering the stolen data by using previously compromised Ubiquiti devices.
  - CERT-UA[5] reported on a cyberattack targeting a critical energy infrastructure facility in Ukraine
- Two incidents have been attributed to *UNC-1151*[6], a Belarusian state-sponsored threat actor[7]:
  - CERT-UA[8] discovered a cyberattack against Ukrainian government agencies. Through a phishing campaign, the threat actor distributes the PicassoLoader malware. Once deployed, the malware downloads and runs njRAT remote access utility giving the threat actor access to the target's device and the capability to spread throughout the device's network.

- CERT-UA[9] reported on a cyberattack targeting Ukrainian entities, exploiting several vulnerabilities

- A campaign targeting at least 11 Ukrainian telecommunications providers has been attributed to the threat actor identified as *UAC-0165*. This attribution was made by CERT-UA, who, with a moderate level of confidence, assess *UAC-0165* to be the *Sandworm* group.[10] The campaign was discovered by CERT-UA.[11]
  - By using previously compromised systems, the threat actor was able to scan networks for open ports and gain remote control access. Once inside, the threat actor was able to gain remote access and interfere with the information and communication systems of 11 telecommunications providers of Ukraine by disabling active network and server equipment as well as data storage systems. This led to interruptions in the provision of services to consumers.

Notable threat actor activity

- According to the State Service of Special Communications and Information Protection of Ukraine[12] a cyberattack, claimed by the pro-Russian threat actor *SoIntsepek*[13], targeted a Ukrainian government service with wiper malware.

  This malware affected specific devices, while also enabling access to the service's official Facebook page. Using this platform, the attack was announced along with a claim of data theft. The SSSCIP of Ukraine stated that the corporate network had been disconnected and that the website was temporarily suspended, but that no harm was caused to the Service's resources.

- According to the State Service of Special Communications and Information Protection of Ukraine, as of late April, 2023, the Russian state-sponsored *Sandworm* began using SoIntsepek Telegram channel to publish information on their attacks.[14]

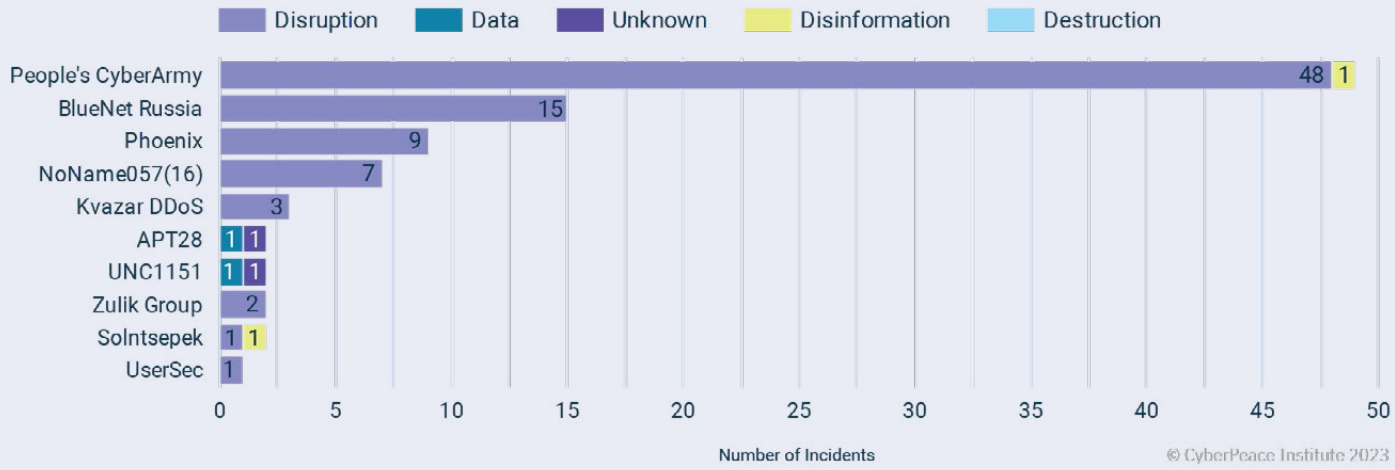
- BlackBerry Threat Research and Intelligence Team[15] and CERT-UA[16] have reported on a phishing campaign using Ukraine's attendance at a NATO Summit as a lure. The threat actor created a phishing website imitating the website of a legitimate nonprofit. The fake website is used to distribute malicious files allowing the threat actor to gain access to the target's device. The threat actor exploited the previously known Follinna vulnerability allowing the threat actor to conduct remote code execution. The threat actor could then gather information from the target's device such as the size of the computer memory, the username and information about the device's network adapter.

- A Ukrainian news media outlet confirmed a DDoS attack against their website. The cyberattack was claimed by the pro-Russian hacktivist collective *People's CyberArmy*.[17] [18] [19]

Latest malware

- CERT-UA reported on a SmokeLoader malware distribution through phishing emails posing as an invoice from compromised email accounts. If executed, this malware gives the threat actor access to the target's device. CERT-UA tracks the activity of this threat actor under the identifier *UAC-0006*.[20]

Top 10 threat actors targeting entities in Ukraine [April - June 2023]



In the third quarter of 2023, the CyberPeace Institute recorded a decline in malicious cyber activities perpetrated by pro-Russian threat actors targeting entities in Ukraine, in comparison to the preceding quarter, Q2 of 2023. The Institute's analysis suggests that *Sandworm*[21] is likely the most active pro-Russian state-sponsored threat actor conducting malicious operations against Ukrainian entities. Sandworm is a destructive Advanced Persistent Threat (APT), active since at least 2009, attributed to the Russian Federation's General Staff Main Intelligence Directorate.[22]

The group is responsible for several highly impactful cyberattacks, such as the widespread power outages in Ukraine in 2015,[23] and the NotPetya malware used in 2017.[24] As the group is known for its sabotaging and destructive activities, it is highly likely that their high activity in Ukraine is connected to an underlying Russian strategy to degrade, rather than establish control over, Ukraine's cyber domain.

Cyberattacks on Ukrainian entities [Q3 2023 vs Q2 2023]

+36.4 %
cyberattacks on the media and the ICT sector

+100 %
cyberattacks on the trade and the manufacturing sector

+25 %
cyberattacks on the education sector

A year of analyzing cyberattacks

When contrasting the activities of pro-Russian threat actors in Q3 of 2023 with those in Q3 of 2022, the number of attacks remain relatively consistent, with a slight increase of 11.49% in Q3 of 2023.

In contrast to the progressive increase observed in pro-Russian threat actors' activities from July to September in Q3 2022, their operations in Q3 2023 exhibited a distinct pattern. The peak of their activity occurred in July 2023, with 46 cyberattacks, followed by a gradual decline in August and September, with 23 and 28 cyberattacks recorded, respectively.

Furthermore, a consistent pattern emerged when comparing the targeted sectors in Q3 of 2023 with Q3 of 2022. The most frequently targeted sectors remain public administration, media, and information and communication technology (ICT). *The People's CyberArmy* remained the most active pro-Russian threat actor, consistently targeting Ukrainian entities since Q3 of 2022.

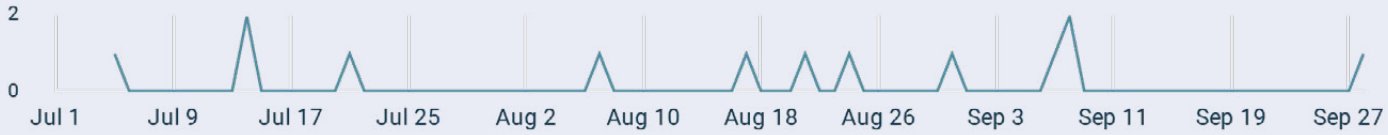
While there has been a shift in the threat actor landscape, with *Anonymous Russia* and the broader *KillNet* collective exhibiting reduced activity in Q3 of 2023, newer hacktivist collectives have filled the void. Notably, *BlueNet* Russia and Phoenix emerged as the second and third most active threat actors, respectively, in Q3 of 2023.

Trends and Emerging Issues Q3 2023

Russian Federation

Incidents	Sectors	Threat Actors
13	9	5
↓ -72.9%	↓ -43.8%	∞

Daily evolution of cyber incidents impacting entities in the Russian Federation [July - September 2023]



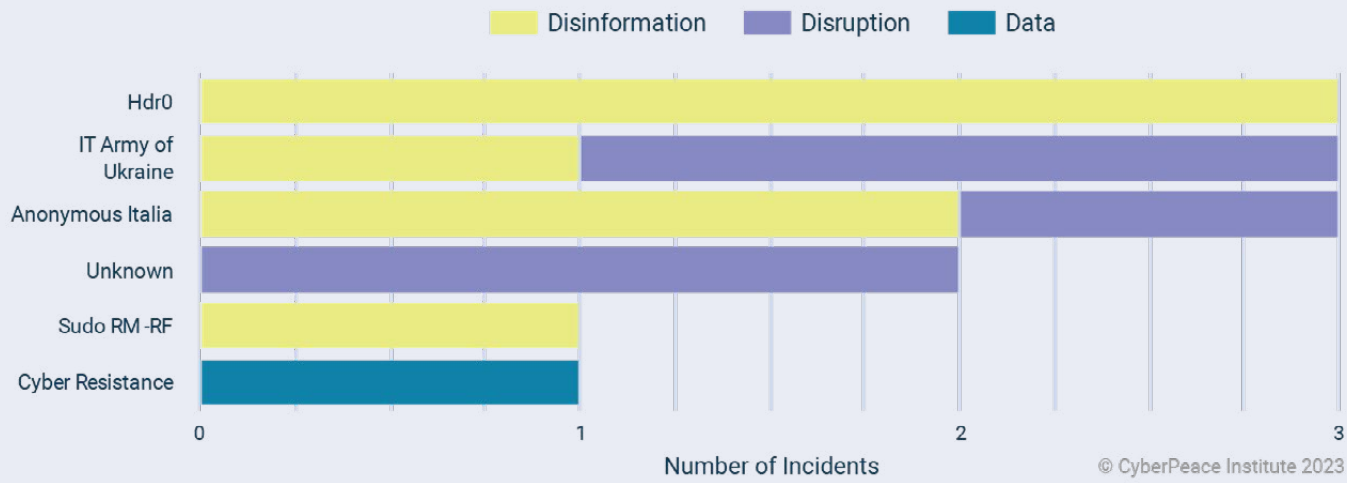
Trends

- Defacement operations account for 53.8% of all incidents, followed by DDoS attacks (30.8%).
- Second consecutive quarter showing a decrease in recorded malicious cyber activities, as well as a reduction in the number of threat actors identified as conducting these activities against entities in the Russian Federation.
- Two confirmed disruptive attacks against Russian Internet service providers operating in the illegally annexed territories of Ukraine.
- One confirmed defacement operation against the website of a Russian nonprofit organization.

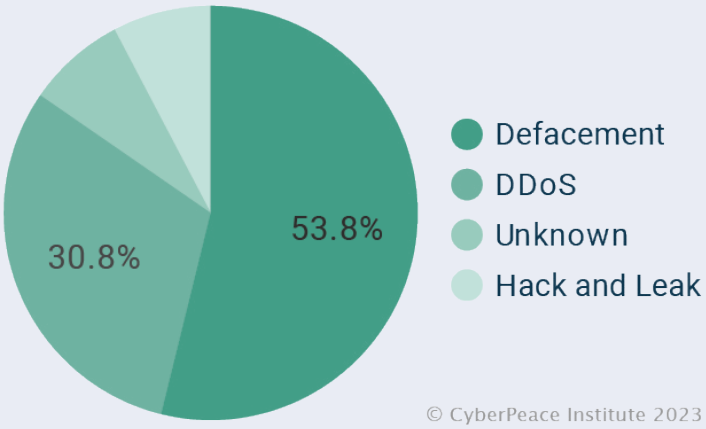
Notable threat actor activity

- *Hdr0* - A pro-Ukrainian hacktivist threat actor that is active on Telegram. The group's Telegram channel was initially created in February 2022, but has not been active since September 2022. The threat actor has conducted four confirmed defacement operations against Russian entities beginning in Q3 2023.

Threat actors targeting entities in the Russian Federation [July- September 2023]



Types of cyber incidents targeting entities in the Russian Federation [July- September 2023]



In alignment with the overall decline in malicious activities detected by the CyberPeace Institute in Q3 of 2023, the documented cyberattacks against entities in the Russian Federation have decreased by 72.9% compared to the previous quarter, Q2 of 2023.

Additionally, there has been a notable reduction of 43.8% in the number of targeted sectors and a 16.7% decrease in the number of active threat actors.

Notable incidents in Russian Federation

Disruption

July 10, 2023

Confirmed cyberattack against the information system of a Russian regional medicinal distributor. The cyberattack led to a disruption in sales of medicine.[25]

July 23, 2023

Confirmed DDoS attack claimed by the *IT Army of Ukraine* against the servers of a Russian Internet service provider operating in the illegally annexed territories of Luhansk.[26] [27]

August 9, 2023

Confirmed DDoS attack claimed by the *IT Army of Ukraine* against the servers of a Russian Internet service provider operating in the illegally annexed territories of Luhansk.[28] [29]

September 8, 2023

Confirmed DDoS attack against the servers of a Russian IT company assisting in online voting. The DDoS attack led to delays for voters in receiving SMS messages needed to vote.[30]

A year of analyzing cyberattacks

In comparison to the same quarter in the previous year (Q3, 2022), there has also been a decline of 72.9% of incidents.

A shift in the entities being targeted is evident when comparing Q3 of 2022 to Q3 of 2023. Pro-Ukrainian threat actors, during Q3 of 2022, predominantly targeted Russian media, financial, and administrative/support sectors. However, in Q3 of 2023, the focus shifted to Russian public administration, transportation, and ICT sectors.

For the first time since the CyberPeace Institute began documenting cyberattacks within the context of the conflict, defacement operations have become the most prevalent type of cyberattacks conducted against Russian entities.

The landscape of pro-Ukrainian threat actors targeting entities in the Russian Federation has undergone substantial changes since Q3 of 2022. During the initial analysis of malicious cyber operations within the ongoing conflict in Ukraine, the *IT Army of Ukraine* was notably active, peaking between August and October of 2022 with 25 claimed attacks throughout that period, compared to only 3 documented claims of attacks in the third quarter of 2023.

Trends and Emerging Issues Q3 2023

Other Countries

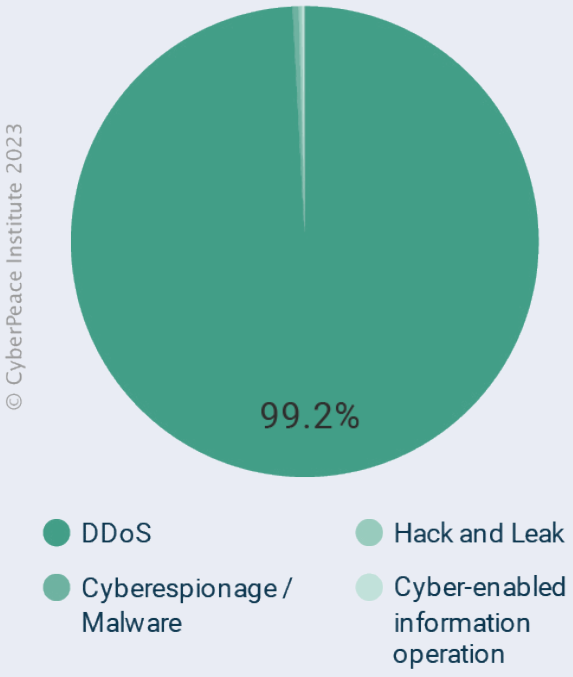
Incidents	Countries	Sectors	Threat Actors
472	37	19	18
↓ -3,5%	↓ -2,6%	↓ -13,6%	∞

Daily evolution of cyber incidents impacting entities in countries other than the the two belligerent states [July - September 2023]

Trends

- DDoS attacks account for 99.4% of all the incidents which were recorded in 37 countries globally, none of which are belligerents in this conflict.
- Most targeted sectors were the public administration (135), transportation (113), financial (67), media (34), and administrative / support (22).

Types of cyber incidents targeting entities outside the two belligerent states [July - September 2023]



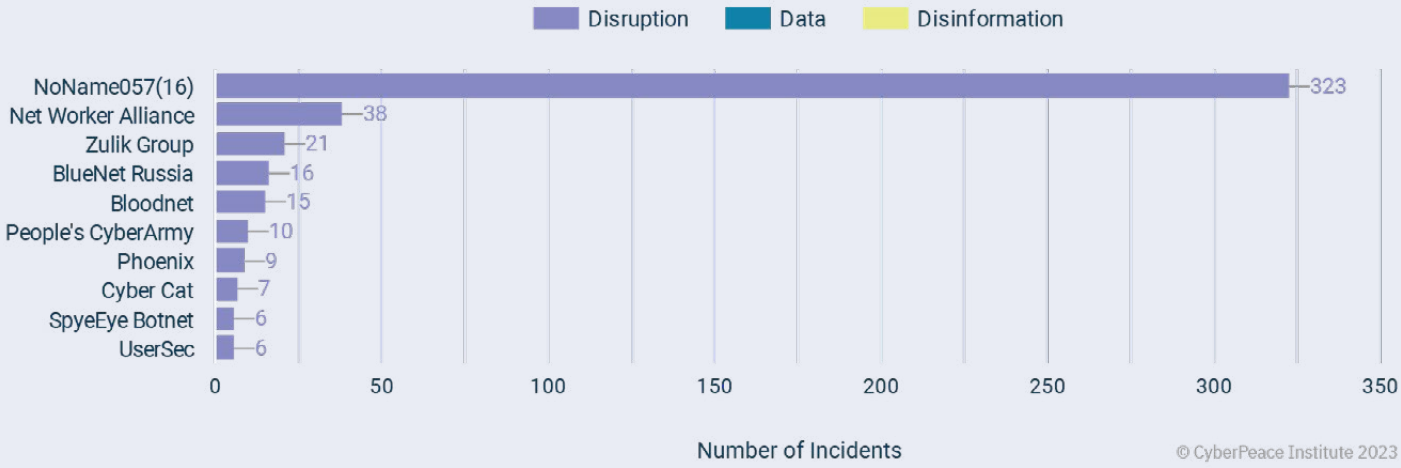
Top 10 targeted countries, outside the two belligerent states [July - September 2023]

	Country	Incidents ▾	%Δ
1.	POLAND	77	-19% ↑
2.	LITHUANIA	46	59% ↑
3.	SPAIN	30	50% ↑
4.	NETHERLANDS	25	79% ↑
5.	FRANCE	25	-32% ↓
6.	ITALY	25	-11% ↓
7.	GERMANY	23	-50% ↓
8.	ESTONIA	22	∞
9.	LATVIA	21	31% ↑
10.	MOLDOVA	19	1800% ↑

Notable threat actor (in)activity

- Continuous decrease in the activity of *KillNet* recorded in Q3, 2023, falling to only 3 attributed incidents.
- Two new threat actors - *Net Worker Alliance* and *Zulik Group* started operations during this quarter. Both threat actors are hacktivist collectives communicating their alleged cyber operations through Telegram channels. *Net Worker Alliance* and *Zulik Group* mainly target the non-belligerent countries with DDoS attacks. Estonia was targeted the most (9 incidents) by *Net Worker Alliance* and Poland the most (9) by *Zulik Group*. Both threat actors' Telegram channels have since been deleted.

Top 10 threat actors targeting entities outside the two belligerent states [July - September 2023]



The overall number of processed malicious cyber activities by the CyberPeace Institute against entities in non-belligerent countries to the ongoing conflict in Ukraine has seen a slight decrease of 3.7% when compared to the preceding quarter of 2023. However, it is noteworthy that the number of processed cyberattacks remains relatively high, especially in contrast to Q3 of 2022, reflecting a substantial increase of 234.1%. Pro-Russian threat actors, while experiencing a slight decrease in activities in July 2023, have consistently maintained a level of over 400 cyberattacks per quarter since the beginning of 2023. Notably, in Q3 of 2023, more than 99% of all processed incidents were identified as DDoS attacks.

The number of processed cyberattacks exhibited a steady increase throughout Q3 of 2023, escalating from 118 incidents in July to 155 in August and reaching 198 in September. This contrasts with the pattern observed in Q3 of 2022 when pro-Russian threat actors' activities peaked in August and declined by the end of September.

In July 2023, Spain and Poland emerged as the two most targeted countries, each experiencing 27 recorded incidents in the country, while Lithuania closely followed with 23 incidents. The notable 50% increase in targeting Spanish entities, compared to the preceding quarter, is likely associated with Spain's assumption of the presidency of the Council of the European Union from July 1st to December 31, 2023. Spain announced one of its priorities as providing continuous

support for Ukraine during its rotational presidency, which highly likely have led to this increased level of cyber incidents.[31]

On July 13, the European Parliament adopted the Act in Support of Ammunition Production (ASAP). This legislative action was a response to Ukraine's request for assistance, and provides for the supply of 155 mm-calibre artillery rounds, as agreed upon by the Council on March 20, 2023, through a three-track proposal on ammunition.[32]

Concurrently, pro-Russian threat actors intensified their malicious activities against Lithuanian entities in July 2023. This escalation is highly likely linked to NATO's annual summit, which occurred in Vilnius, Lithuania, during the first half of July.[33]

During August 2023, Poland, the Netherlands, and Italy ranked as the three most targeted countries, according to the CyberPeace Institute's research. Poland experienced 26 recorded cyber incidents, followed closely by the Netherlands with 24, and Italy with 20 incidents.

The significant 78.6% increase in targeting Dutch entities, compared to the preceding quarter, is likely attributed to the Netherlands' ongoing commitment to supporting Ukraine.[34] [35] This support extends to decisions made by the Dutch authorities to donate F16 fighter jets to Ukraine.[36]

The Danish authorities also agreed to provide fighter jets. Notably, despite the trend observed that pro-Russian threat actors target countries that announce military support for Ukraine, the CyberPeace Institute did not observe a corresponding increase in attacks against Danish entities during this period.

The increase of cyberattacks against Italian entities is almost certainly related to the senate vote held on July 26, 2023 to recognize the Holodomor famine in Ukraine as a genocide.[37] Pro-Russian threat actor, *NoName057(16)*, referenced the vote before a DDoS attack campaign against entities in Italy in late July.[38]

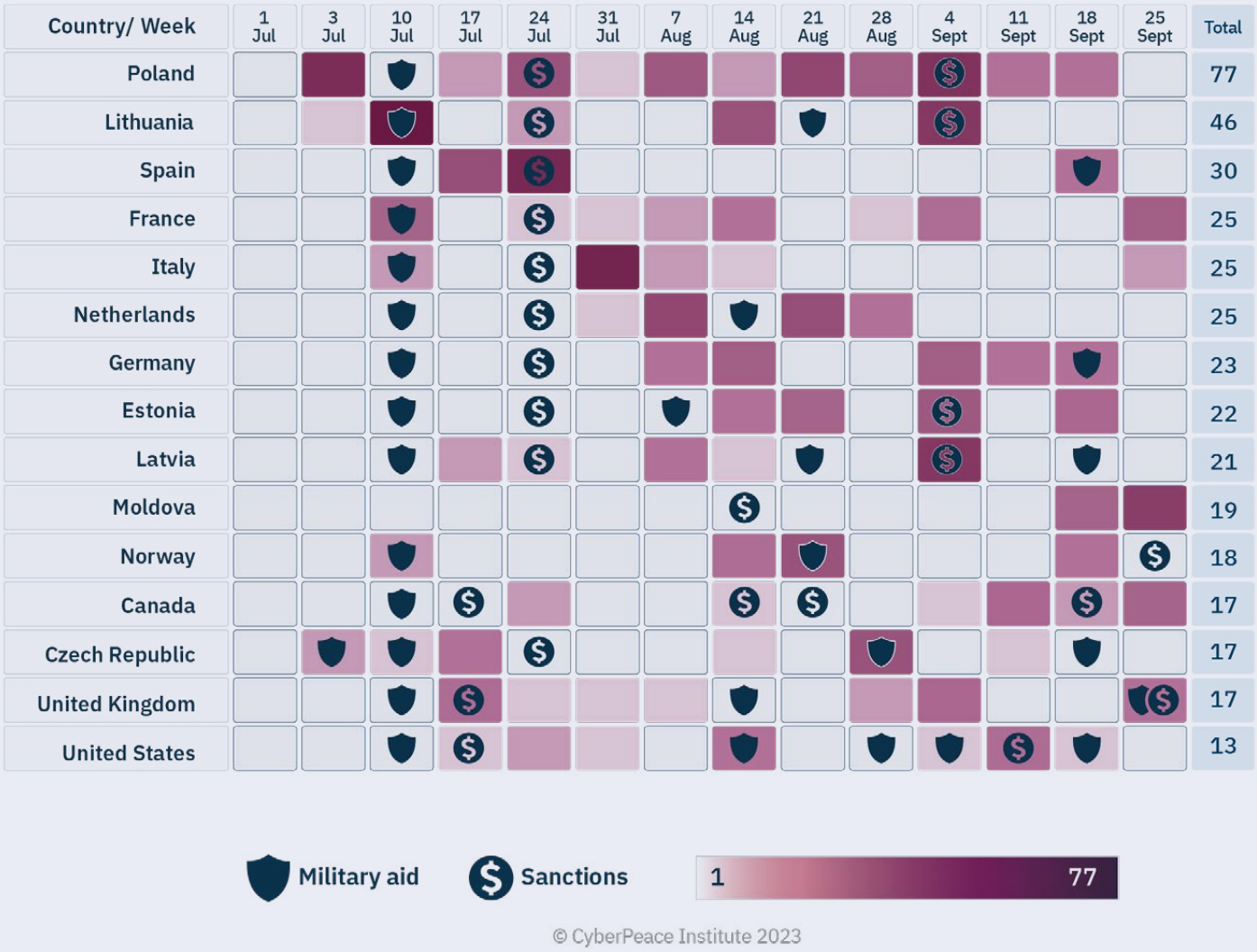
In September 2023, the CyberPeace Institute identified four countries as the most targeted with cyber attacks, with Poland experiencing 24 incidents, followed by Moldova with 19, and Italy and Canada both identifying 14 recorded incidents against entities within their borders. In early September, Poland, along with Estonia, Latvia, Lithuania and Finland put into place a ban on vehicles with Russian license plates. It is highly likely that this decision prompted Pro-Russian threat actors to target the countries involved with the ban, which can be supported by the rise in attacks against Poland, Lithuania, Latvia and Estonia during this period.[39]

The significant 1800% increase in attacks against Moldovan entities, compared to Q2 2023, is highly likely related to Moldova's recent actions to curb alleged Russian influence within the country. Notably, by the end of August, Moldova expelled 45 Russian diplomats and embassy staff as part of a comprehensive effort to garner support from European Union Member States for accession talks.[40] [41]

Similarly, the observed malicious cyber activities against Canadian entities are highly likely to be connected to the Canadian government's recent reaffirmation of unwavering support for Ukraine.[42]

In the heatmap depicted below, the CyberPeace Institute has documented instances of cyberattacks and incidents associated with geopolitical occurrences, specifically focusing on non-belligerent countries' actions in relation to sanctions, military assistance, and public statements on the armed conflict.[43]

Heat matrix indicating the number of incidents per week for all countries with more than 10 incidents in Q1 2023 overlaid with documented public announcements of new sanctions or military aid [Jan - Mar 2023]



Notable incidents

Disruption

September 13-14, 2023

A two-day confirmed DDoS campaign against the websites of 15 Canadian public administration entities, claimed by *NoName057(16)*.[44 45 46 47 48]

Disinformation

July 7, 2023

Confirmed cyber-enabled information operation conducted through the exploitation of the servers of a Lithuanian regional radio station and shopping center.

An unknown pro-Russian threat actor was able to disrupt a third-party music streaming service leading to the broadcast of pro-Russian disinformation.[49 50]

Harm and Impact

In the third quarter of 2023, the CyberPeace Institute collected and processed data on nearly 600 cyberattacks and operations within the context of the ongoing conflict. Despite the substantial volume of recorded incidents, the CyberPeace Institute's analysis indicates that the harm and impact on the general population was likely low. This is primarily due to the prevalence of DDoS attacks, which typically result in minor service disruptions, affecting the availability of online resources. While these operations may impact the reputation and finances of the targets, their direct impact on the general population is likely to be limited.

DDoS attacks, especially against the public administration sector, aim to undermine trust and influence the general population by eroding confidence in essential services and government functions. They also aim to create a sense of proximity to the conflict for the general population by intensifying their perceived involvement.

The overall decrease in incidents during Q3 of 2023 only partially aligns with the activity patterns of threat actors observed in Q3 of 2022. In 2022, pro-Russian threat actors increased activities in Q3 compared to Q2, while pro-Ukrainian threat actors experienced a decline in both periods during the summer months. Last year's decline was attributed to reduced documented activities by the *Anonymous* collective, whereas this year's decrease in incidents is linked to the reduced documented claims attacks by the *IT Army of Ukraine*. Consequently, the Institute observes a steady decline in cyber incidents against entities in the Russian Federation from quarter to quarter.

A Year of Analyzing the Impact and Harm of Cyberattacks

For the past year, the Institute has been producing an analytical report, discussing the findings of the data presented on our Cyber Attacks in Times of Conflict Platform #Ukraine platform which monitors incidents affecting critical infrastructure essential for the civilian population and other civilian objects.

Up until the end of September 2023, the Institute documented a total of 604 cyber incidents targeting entities within Ukraine.

The most active pro-Russian threat actors involved in attacks against Ukrainian entities were *People's CyberArmy* (237 incidents), *NoName057(16)* (60), and *Anonymous Russia* (30). The primary impact category observed was disruption (462 incidents), followed by data-related impacts (75).

Beyond Ukraine, pro-Russian threat actors conducted 1883 malicious cyber operations, with entities in Poland (315), Lithuania (157), and Germany (136) being the most targeted. The most active threat actors overall were *NoName057(16)* (1103 incidents), *Anonymous Russia* (104), and *KillNet* (99), with disruption being the most common type of impact (1801 incidents), followed by disinformation (51).

The prevailing conclusion drawn from the data suggests that the pro-Russian threat actor landscape is primarily dominated by hacktivist collectives. Their focus is on conducting cyber incidents with short-term and often negligible impacts. The primary objective of active pro-Russian hacktivist collectives is likely an attempt to sow chaos and amplify their specific narratives.

In Ukraine, given the prevalence of data weaponization as the second most common impact category, the primary objective is likely to gather as much data from Ukrainian entities and citizens as possible for later use by Russia. In non-belligerent countries, especially in the western hemisphere, disinformation is the second most prevalent impact category. Thus, it is highly probable that pro-Russian threat actors aim to create distrust and/or sow chaos amongst Ukrainian allies, possibly intending to weaken their support for Ukraine, including exacerbating war fatigue, as discussed by the Institute in Q2/2023.[51]

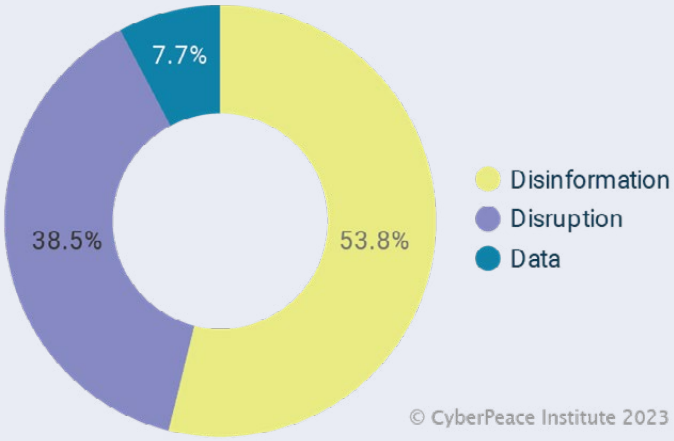
Up until the end of September, the Institute documented 308 malicious cyber operations against entities in the Russian Federation and an additional 14 malicious operations conducted by pro-Ukrainian threat actors against Belarusian entities. The most active threat actors in this context were the *IT Army of Ukraine* (75 incidents), *Anonymous Italia* (64), and *Anonymous* (53), with disruption being the most prevalent impact category (180 incidents), followed by data-related impacts (82).

The behavior and probable objectives of pro-Ukrainian threat actors likely underwent a change throughout the observed period.

In the first six months of the 2022 conflict, pro-Ukrainian threat actors, particularly the *Anonymous* hacktivist collective, focused on hack and leak operations, harvesting data from Russian entities and citizens. However, by Q3 of 2022, *Anonymous*' claimed activities decreased dramatically, marking a shift from data-centric impacts to disruption-centric impacts against Russian entities. This decline coincided with increased activity by the *IT Army of Ukraine*, a threat actor classified as state-sponsored by the Institute due to its close connections to Ukrainian state actors. Since the start of 2023, the Institute observed a decline in the claimed activities of the *IT Army of Ukraine* but noted a new trend - a shift from disruption-centric impact operations to disinformation-centric impact operations. This was evident through cyber-enabled information operations exploiting the networks of several Russian radio and television stations.[52]

In conclusion, despite DDoS attacks constituting the majority of incidents processed by the Institute and resulting in temporary disruption of online services, the main threat likely stems from the sheer number of threat actors operating within the context of the ongoing conflict.

Impact categories of cyber incidents in the Russian Federation [July - September 2023]



Threat actor landscape

As of the end of September 2023, the CyberPeace Institute has attributed cyber incidents to nearly 120 threat actors, with 90 aligning with the Russian Federation and the remainder to Ukraine. Among these, 23 are identified as state-sponsored, 64 as hacktivist collectives, and the remaining categorized as cybercriminal groups, individual threat actors, or unknown entities.

The predominant threat arises from the significant number of hacktivist collectives and their objectives of garnering support for their respective causes, and monetizing their malicious activities, within the context of the ongoing conflict in Ukraine. These threat actors disseminate their ideologies to the widest possible audience, and many hacktivist collectives actively contribute to lowering the knowledge threshold for engaging in cyber incidents. A recent example is the latest recruitment of hacktivists for the *KillNet*'s offensive wing - *Legion Cyber Spetznaz*.[53]

The pro-Russian forum "infinity[.]ink", purportedly moderated by *KillNet*'s founder *KillMilk*, operates on the clear web, offering resources and guidance to new members on conducting various malicious cyber incidents.

Simultaneously, it serves as a communication channel for several pro-Russian threat actors.

The pro-Russian forum, which became subscription-based in mid September[54], is not the only example of a threat actor aiming to increase wider participation in malicious cyber incidents and monetization of hacktivist collectives' activities. Various pro-Russian threat actors, including *KillNet*, have released paid online courses on hacking, DDoS-as-a-service tools[55], or advertising malicious software like the Titan malware or the alleged source code for the infamous Pegasus spyware.

Moreover, threat actors like *NoName057(16)* and the *IT Army of Ukraine* have embraced offensive and, in *IT Army of Ukraine*'s case, defensive crowdsourcing software. In such operations, participants do not require in-depth cybersecurity knowledge; they simply provide their machines to function as "zombies" in a large botnet controlled by the operators of the software.

The lowered threshold for participating in cyber incidents presents multiple threats, particularly the increased civilianization of the conflict. The accessibility of knowledge and guidance for conducting cyberattacks has never been as widespread as it is in the current threat landscape. These sources of information could likely be utilized to pursue political or military objectives, and/or criminal activities. Civilians who participate in cyberattacks may lose the legal protections afforded to them if they directly participate in the hostilities, and/or may be subject to prosecution for criminal acts.

Other Research

During the preceding months, spanning the third quarter of 2023, a confluence of noteworthy cyberattacks and incidents have been recorded, especially within the confines of the enduring conflict between Russia and Ukraine.

In July 2023, the "Cyber Operations during the Russo-Ukrainian War" analysis was published by the Center for Strategic & International Studies that discusses a variety of topics from strange patterns to alternative futures as a part of the war. The report states that though empirical evidence indicates a rise in cyberattacks during the conflict, these attacks did not exhibit an escalation in severity, a change in targets, or a shift in methods overall. Moreover, contrary to widespread expectations of a revolution in warfare, it mentions that Russia's behavior aligned with popular expectations. Finally, the study addresses future implications and affirms that cyber operations are expected to play a supporting, rather than decisive, role in major wars.[56]

The "APT Quarter Highlights of Q3 2023" report that was released by CYFIRMA has recorded a hike in the dynamic and continually evolving activities of Advanced Persistent Threat (APT) groups originating from a range of countries such as China, Iran, North Korea, and Russia. Alongside elaborating on its general observation about the APT collectives posing challenges to the global cybersecurity landscape, it details the activities of various Russian APTs.[57]

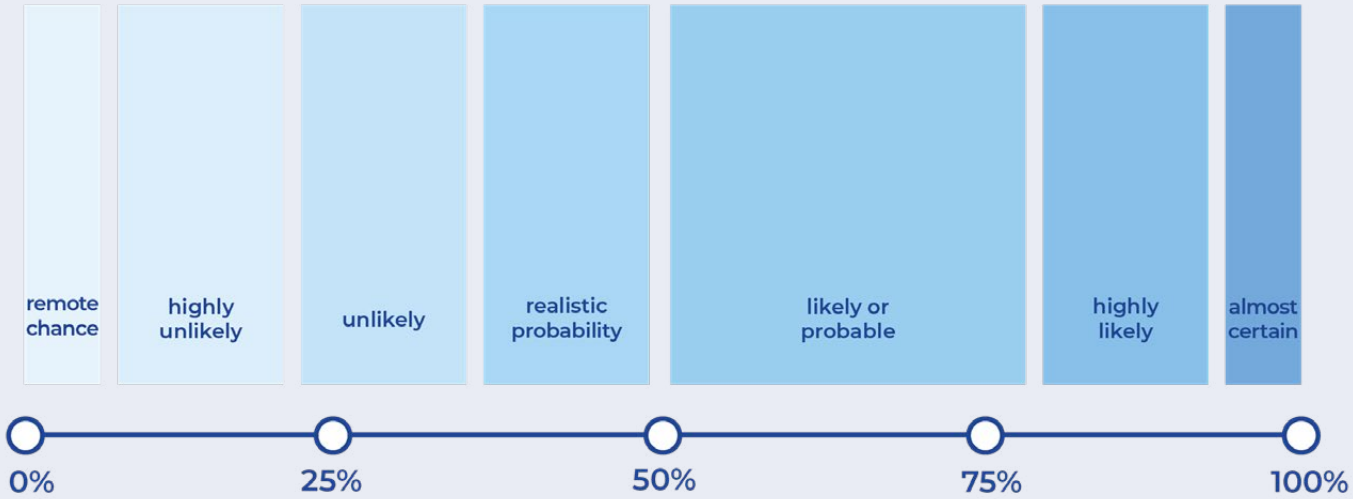
The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (SCPC SSSCIP) published their Q3 2023 report detailing cyber operations in Ukraine. Based on the insights from the "Q3 2023 Performance Report of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System", pro-Russian hacktivist groups continue to target entities in Ukraine belonging to predominantly the financial, public administration, telecommunications, education and civil society sectors in the country. By the end of the quarter, a total of 4 billion events were detected through active monitoring, analysis, and transfer of telemetric information regarding cyber incidents and attacks. Comparing the results from Q2 with Q3 of 2023, the number of registered cyber incidents is observed to have increased by 46%.[58]

The Regional Cyber Defense Centre, a subsidiary of the Ministry of National Defense of Lithuania, released a "Report on Cyber Lessons Learned during the War in Ukraine" in the Q3 of 2023. This report focuses on the cyber activities that took place during 2022 and details how Russian cyber operations have undermined Ukraine's economic and governmental sectors, gained access to critical infrastructure, and impeded the public's right of access to information.[59]

Report Methodology

This report focuses on the incidents documented by the CyberPeace Institute in the second quarter of 2023. Therefore, analysis only covers attacks and campaigns between April 1 and June 30, 2023. For trends-based analysis, the CyberPeace Institute may refer to numbers during a wider date range, in this case the dates are referenced accordingly in the report. Information within the report is generated from data collected by the CyberPeace Institute and made accessible through the Cyber Attacks in Times of Conflict Platform[61]#Ukraine. Specific details and sources of information regarding any individual cyber incidents referenced in this report can be found in the Attack Details[62] page.

As there is a reliance on publicly available data, the data on documented cyberattacks has been given a classification of certainty based on the reliability of the information source. The classification levels are Possible, Probable and Confirmed[63]. Additionally, the CyberPeace Institute distinguishes between singular incidents and campaigns.[64] When conducting analysis it is instrumental to accurately communicate probability in the assessment of our findings and inferences. The CyberPeace Institute uses the UK's Defence Intelligence standard for conveying probability; the 'Professional Head of Intelligence Assessment (PHIA) probability yardstick'.[110] This scale demonstrates broad ranges of certainty or uncertainty that can be translated into consistent language; this language is used throughout this report.



PHIA Probability Yardstick

Source: United Kingdom College of Policing

Disclaimer: Base maps are for graphical purposes only and there should be no inference of the borders of a country or territory. The CyberPeace Institute used the naming convention of countries and their categorization based on the United Nations Statistics Division.

References

[1] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: https://cyberconflicts.cyberpeaceinstitute.org/ (Accessed: 25 October 2023)

[2] Associated identifiers: Sofacy, Fancy Bear, Sednit, Group 74, Pawn Storm, TG-4127, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Forest Blizzard, BlueDelta

[3] United States District Court For The District Of Columbia. (2018). 'United States Of America Vs Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, And Aleksey Aleksandrovich Potemkin'. District Court For The District Of Columbia. Available At: https://Www.Justice.Gov/File/1080281/Download (Accessed: 7 August 2023)

[4] CERT-UA. (2023). 'Fishynhovi ataky hrupy APT28 (UAC-0028) z metoyu otrymannya avtentyfikacijnyx danyx do publichnyx poshtovyx servisiv (CERT-UA#6975)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5105791(Accessed: 1 October 2023).

[5] CERT-UA. (2023). 'Kiberataka APT28: msedge yak zavantazhuvach, TOR ta servisy mockbin.org/website.hook yak centr upravlinnya (CERT-UA#7469)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5702579 (Accessed: 1 October 2023).

[6] Cybersecurity companies use the following names as identifiers for operations and campaigns attributed to UNC1151: Ghostwriter, TA445, UAC-0051,PUSHCHA, Dev-0257, Storm-0257

[7] Huntley, S.(2023). 'An update on the threat landscape'. Google Threat Analysis Group. Available at: https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ (Accessed: 2 October 2023).

[8] CERT-UA. (2023). 'Cil"ova kiberataka UAC-0057 u vidnoshenni derzhavnyx orhaniv iz zastosuvannyam PicassoLoader/njRAT (CERT-UA#6948)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5098518 (Accessed: 31 July 2023).

[9] CERT-UA. (2023). 'Kiberataka UAC-0057: eksplojt dlya CVE-2023-38831, JavaScript-variaciya PicassoLoader, alhorytm Rabbit ta Cobalt Strike Beacon (CERT-UA#7435)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5661411 (Accessed: 31 August 2023).

[10] CERT-UA. (2023). WinRAR yak "kiberzbroya". Destruktyvna kiberataka UAC-0165 (jmovirno, Sandworm) na derzhsektor Ukrayiny iz zastosuvannyam RoarBat (CERT-UA#6550)'. Computer Emergency Response Team of Ukraine. Available at : https://cert.gov.ua/article/4501891 (Accessed: 1 October 2023).

[11] CERT-UA. (2023). 'Osoblyvosti destruktyvnyx kiberatak u vidnoshenni ukrayins"kyx provajderiv (CERT-UA#7627)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/6123309 (Accessed: 31 October 2023).

[12] SSSCIP. (2023). 'Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent "victory"'. State Service of Special Communications and Information Protection of Ukraine. Available at: https://cip.gov.ua/en/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo (Accessed: 1 October 2023).

[13] Solntsepek. (2023). [Telegram]. Available at: https://t.me/solntsepekZ/904 (Accessed: 31 July 2023).

[14] SSSCIP. (2023). 'Russia's Cyber Tactics H1' 2023'. State Service of Special Communications and Information Protection of Ukraine. Available at: https://cip.gov.ua/services/cm/api/attachment/download?id=60068 (Accessed: 31 October 2023).

[15] BlackBerry Research and Intelligence Team. (2023). 'RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit'. BlackBerry Blog. Available at: https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit (Accessed: 7 August 2023).

[16] CERT-UA. (2023). 'Cil"ova ataka z vykorystannyam tematyky chlenstva Ukrayiny v Orhanizaciyi Pivnichnoatlantychnoho dohovoru (CERT-UA#6940)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5077168 (Accessed: 31 July 2023).

[17] People's Cyber Army. (2023). [Telegram]. Available at: https://t.me/CyberArmyofRussia_Reborn/4228 (Accessed: 31 July 2023).

[18] People's Cyber Army. (2023).[Telegram]. Available at: https://t.me/CyberArmyofRussia_Reborn/4230 (Accessed: 31 July 2023).

[19] Kremenchuk operatyvnyj. (2023). [Telegram]. Available at: https://t.me/kremenkop/14684 (Accessed 31 July 2023).

[20] CERT-UA. 'Kiberataka UAC-0006: rozpovsyudzhennya SmokeLoader z vykorystannyam elektronnyx lystiv i tematyky "raxunkiv" (CERT-UA#6999)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/5158006 (Accessed: 31 July 2023).

[21] Associated identifiers: Iron Viking, CTG-7263, Voodoo Bear, Quedagh, TEMP.Noble, ATK 14, BE2, UAC-0082, UAC-0113, FROZENBARENTS, IRIDIUM, Seashell Blizzard, Electrum, Telebots, Black Energy (Group)

[22] Mitre. (2023). 'Sandworm Team'. Mitre. Available at: https://attack.mitre.org/groups/G0034/ (Accessed: 18 December 2023).

[23] Hultquist, J. (2023). 'Sandworm Team and the Ukrainian Power Authority Attacks'. Mandiant. Available at: https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team (Accessed: 18 December).

[24] Mitre. (2023). 'NotPetya, Software S0368'. Mitre. Available at: https://attack.mitre.org/software/S0368/ (Accessed: 18 December 2023).

[25] Xudchenko Ofycyal"no. (2023). [Telegram]. Available at: https://t.me/s/anastasiyahudchenko (Accessed: 30 September 2023).

[26] IT Army of Ukraine. (2023). [Telegram]. Available at: https://t.me/itarmyofukraine2022/1442 (Accessed: 31 July 2023).

[27] Luganetinternet-provajdervLNR. (2023).[VK[.]com]Availableat:https://vk.com/luga_net?w=wall-114493021_61957 (Accessed: 31 July 2023).

[28] IT Army of Ukraine. (2023). [Telegram]. Available at: https://t.me/itarmyofukraine2022/1520 (Accessed: 30 August 2023).

[29] Operator «MKS». (2023). [Telegram]. Available at: https://t.me/operator_mcs/226 (Accessed: 30 August 2023).

[30] TASS. (2023). 'DDoS-ataki stali prichinoj zaderzhki SMS dlja uchastnikov onlajn-golosovanija v Moskve'. TASS. Available at: https://tass.ru/politika/18683863 (Accessed: 30 September 2023).

[31] Spanish Presidency. (2023). Council of the European Union. 'The Spanish Presidency Programme'. Available at: https://spanish-presidency.consilium.europa.eu/en/programme/the-spanish-presidency-programme/ (Accessed: 31 October 2023).

[32] European Parliament. (2023). 'Act in support of ammunition production (ASAP)'. European Parliament Think Tank. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)749782 (Accessed: 31 October 2023).

[33] NATO. (2023). 'Vilnius Summit Communiqué'. NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (Accessed 31 October 2023).

[34] Meier, B., Van den Berg, S., Van der Wouw, P. (2023). 'Zelensky in Netherlands to boost Ukraine air defenses'. The West Australian. Available at: https://thewest.com.au/news/conflict/ukraine-says-russian-missile-kills-seven-hurts-129-c-11643928 (Accessed 31 August 2023).

[35] Koster, T. (2023). 'The Dutch are leading the way on military aid to Ukraine. Here's why'. Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/the-dutch-are-leading-the-way-on-military-aid-to-ukraine-heres-why/ (Accessed 30 August 2023).

[36] Walker, A., Lowe, Y., Fulton, A. (2023). 'Netherlands and Denmark to supply F-16 fighter jets to Ukraine, Dutch PM says- as it happened'. The Guardian. Available at: https://www.theguardian.com/world/live/2023/aug/20/russia-ukraine-war-live-zelenskiy-vows-revenge-over-chernihiv-terrorist-attack-drone-hits-russian-train-station (Accessed: 30 August 2023).

[37] RFE Ukrainian Service. (2023). 'Italy's Senate votes to recognize Holodomor Famine in Ukraine as genocide'. Radio Free Europe Radio Liberty. Available at: https://www.rferl.org/a/italy-senate-recognizes-holodomor-ukraine-genocide/32522340.html (Accessed: 31 October 2023).

[38] NoName057(16). (2023). [Telegram]. Available at: https://t.me/noname05716/4360 (Accessed: 31 July 2023).

[39] Nilsen, T. (2023). 'Last European entry point bans Russian cars'. The Barents Observer. Available at: https://thebarentsobserver.com/en/2023/09/last-european-entry-point-bans-russian-cars (Accessed: 31 October).

[40] Dermenji, D., Schreck, C. (2023). 'Moldova Kicked Out Most of Russia's Diplomats, But the Embassy in Chisinau Still Has Close Ties To Spies'. Radio Free Europe Radio Liberty. Available at: https://www.rferl.org/a/investigation-moldova-expels-russian-diplomats-spy-ties/32581071.html (Accessed: 31 October 2023).

[41] Gavin, G. (2023). 'Don't let Putin keep us out of the EU, Moldova implores'. Politico. Available at: https://www.politico.eu/article/nicu-popescu-moldova-foreign-minister-european-union-accession-membership-putin-russia/ (Accessed: 31 October 2023).

[42] Prime Minister of Canada Justin Trudeau. (2023). 'Canada reaffirms our unwavering support for Ukraine for as long as it takes'. Prime Minister of Canada Justin Trudeau. Available at: https://www.pm.gc.ca/en/news/news-releases/2023/09/22/canada-reaffirms-our-unwavering-support-ukraine-long-it-takes (Accessed: 30 October 2023).

[43] Heatmap sources:

- Bir, B. (2023). 'UK announces over $110M for Ukraine's air defense capability'. AA. Available at: https://www.aa.com.tr/en/europe/uk-announces-over-110m-for-ukraines-air-defense-capability/2971330 (Accessed: 30 November 2023).
- BNS. (2023). 'Lithuania announces new €41m military aid package to Ukraine'. LRT[.]lt. Available at:https://www.lrt.lt/en/news-in-english/19/2062185/lithuania-announces-new-eur41m-military-aid-package-to-ukraine (Accessed: 30 November 2023).
- Cabinet of Ministers. (2023). 'Latvia supports Ukraine'. Cabinet of Ministers Republic of Latvia. Available at: https://www.mk.gov.lv/en/latvia-supports-ukraine?utm_source=https%3A%2F%2Fwww.google.com%2F (Accessed: 30 November 2023).
- EER. (2023). 'Estonia to donate small arms to Ukraine'. ERR. Available at:https://news.err.ee/1609058315/estonia-to-donate-small-arms-to-ukraine (Accessed: 30 November 2023).
- European Council. (2023). Timeline - EU restrictive measures against Russia over Ukraine'. European Council. Available at: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/ (Accessed: 30 November 2023).
- European Pravda. (2023). 'Spain announces plans to send additional aid to Ukraine'. Ukrainska Pravda. Available at: https://www.pravda.com.ua/eng/news/2023/09/20/7420665/ (Accessed: 30 November 2023).
- Federal Ministry of Defense. (2023). 'New €400 million support package for Ukrainian armed forces'. Federal Ministry of Defense of Germany. Available at: https://www.bmvg.de/de/aktuelles/neues-400-millionen-euro-paket-fuer-ukrainische-streitkraefte-5679858 (Accessed: 30 November 2023).
- Fenbert, A. (2023). 'Latvia pledges more military aid to Ukraine'. The Kyiv Independent. Available at: https://kyivindependent.com/latvia-pledges-more-military-aid-to-ukraine/ (Accessed: 30 November 2023).
- Foreign, Commonwealth & Development Office, Cleverly, J. Rt Hon MP. (2023). 'UK announces new sanctions in response to Russian sham elections in Ukraine'. Gov[.]uk. Available at: https://www.gov.uk/government/news/uk-announces-new-sanctions-in-response-to-russian-sham-elections-in-ukraine (Accessed: 30 November 2023).
- Fornusek, M. (2023). 'Minister: Germany plans $5.5 billion in annual military aid for Ukraine until 2027'. The Kyiv Independent. Available at: https://kyivindependent.com/german-minister-germany-plans/ (Accessed: 30 November 2023).

· Government of the Netherlands. (2023). 'Dutch aid for Ukraine: from day to day'. Government of the Netherlands. Available at: https://www.government.nl/topics/russia-and-ukraine/dutch-aid-for-ukraine (Accessed: 30 November 2023).
· Government[.]no. (2023). 'Norway is tightening its restrictive measures against Russia'. Government[.]no. Available at:https://www.regjeringen.no/en/aktuelt/norway-is-tightening-its-restrictive-measures-against-russia/id2996416/ (Accessed: 30 November 2023).
· Government[.]no. (2023).' Norway plans to donate F-16 fighter jets to Ukraine'. Government[.]no. Available at: https://www.regjeringen.no/en/aktuelt/norway-plans-to-donate-f-16-fighter-jets-to-ukraine/id2992009/ (Accessed: 30 November 2023).
· Mills, C. (2023). 'Military assistance to Ukraine since the Russian invasion'. House of Commons Library UK Parliament. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9477/ (Accessed: 30 November 2023).
· Mills, C. (2023). 'Sanctions against Russia'. House of Commons Library UK Parliament. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9481/ (Accessed: 30 November 2023).
· Ministry of Defence & Armed Forces. (2023).' Czech Republic, Denmark and the Netherlands sealed an agreement in Ramstein on supplies of weapons to Ukraine'. Ministry of Defence & Armed Forces of the Czech Republic. Available at: https://www.army.cz/en/ministry-of-defence/newsroom/news/czech-republic--denmark-and-the-netherlands-sealed-an-agreement-in-ramstein-on-supplies-of-weapons-to-ukraine-246492/ (Accessed: 30 November 2023).
· Ministry of Defence & Armed Forces. (2023). 'Minister Cernochova in Toledo: Czech Republic to deliver additional Hinds to Ukraine'. Ministry of Defence & Armed Forces of the Czech Republic. Available at: https://www.army.cz/en/ministry-of-defence/newsroom/news/minister-cernochova-in-toledo:-czech-republic-to-deliver-additional-hinds-to-ukraine-246041/ (Accessed: 30 November 2023).
· Ministry of Defence, Shapps, G. Rt Hon MP. (2023). 'Further support for Ukraine promised as Defence Secretary meets President Zelenskyy in Kyiv'. Gov[.]uk. Available at: https://www.gov.uk/government/news/further-support-for-ukraine-promised-as-defence-secretary-meets-president-zelenskyy-in-kyiv#:~:text=The%20UK%20delivered%20%C2%A32.3,the%20coming%20weeks%20and%20months. (Accessed: 30 November 2023).
· Reuters. (2023). 'UK to provide Ukraine with ammo, vehicles and 65$ million for equipment repair'. Reuters. Available at: https://www.reuters.com/world/europe/uk-provide-65-mln-support-package-ukraine-2023-07-11/ (Accessed: 30 November 2023).
· U.S. Department of State. (2023). 'Additional U.S. Security Assistance for Ukraine'. Available at: https://www.state.gov/additional-u-s-security-assistance-for-ukraine-9/ (Accessed: 30 November 2023).
· U.S. Department of State. (2023). 'Biden Administration Announces Additional Security Assistance for Ukraine'. Available at: https://www.defense.gov/News/Releases/Release/Article/3534283/biden-administration-announces-additional-security-assistance-for-ukraine/(Accessed: 30 November 2023).
· U.S. Department of State. (2023). 'Imposing Additional Sanctions in Response on Those Supporting Russia's War against Ukraine'. U.S. Department of State. Available at: https://www.state.gov/imposing-additional-sanctions-on-those-supporting-russias-war-against-ukraine/ (Accessed: 30 November 2023).
· U.S. Department of State. (2023). 'Imposing Further Sanctions in Response to Russia's Illegal War against Ukraine'. U.S. Department of State. Available at: https://www.state.gov/imposing-further-sanctions-in-response-to-russias-illegal-war-against-ukraine-2/ (Accessed: 30 November 2023).
· U.S. Department of State. (2023). 'New Package of Additional U.S. Military Assistance for Ukraine'. U.S. Department of State. Available at: https://www.state.gov/new-package-of-additional-u-s-military-assistance-for-ukraine/ (Accessed: 30 November 2023).

[44] Canadian Centre for Cyber Security. (2023). 'Distributed Denial of Service campaign targeting multiple Canadian sectors'. Canadian Centre for Cyber Security. Available at: https://www.cyber.gc.ca/en/alerts-advisories/distributed-denial-service-campaign-targeting-multiple-canadian-sectors (Accessed: 30 September 2023).

[45] NoName057(16). (2023). [Telegram]. Available at: https://t.me/noname05716/4838 (Accessed: 30 September 2023).

[46] NoName057(16). (2023). [Telegram]. Available at: https://t.me/noname05716/4841 (Accessed: 30 September 2023).
[47] NoName057(16). (2023). [Telegram]. Available at: https://t.me/noname05716/4847 (Accessed: 30 September 2023).
[48] NoName057(16). (2023). [Telegram]. Available at: https://t.me/noname05716/4849 (Accessed: 30 September 2023).
[49] NKSC. (2023). 'NKSC fiksavo du kibernetinius incidentus, susijusius su muzikos transliacijomis'. National Cyber Security Centre of Lithuania. Available at: https://www.nksc.lt/naujienos/nksc_fiksavo_du_kibernetinius_incidentus_susijusiu.html (Accessed: 31 July 2023).
[50] BNS. (2023). 'Hackers stream anti-NATO broadcasts in Lithuania after cyber attacks'. LRT[.]lt. Available at: https://www.lrt.lt/en/news-in-english/19/2031082/hackers-stream-anti-nato-broadcasts-in-lithuania-after-cyber-attacks (Accessed: 31 July 2023).
[51] CyberPeace Institute. (2023). 'Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q2 April to June 2023'. CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/wp-content/uploads/2023/09/Ukraine-Report-Q2_4.09.pdf (Accessed: 1 October 2023).
[52] Ibid.
[53] Legion- Cyber Spetsnaz. (2023). [Telegram]. Available at: https://t.me/legion_ddos/5 (Accessed: 30 August 2023).
[54] KillNet. (2023). [Telegram]. Available at: https://t.me/killnet_reservs/7537 (Accessed: 30 September 2023).

[55] KillNet Order/ ZAKAZ.(2023). [Telegram]. Available at: https://t.me/killnet_order/4(Accessed: 30 September 2023).
[56] Mueller, G., et al. (2023). 'Cyber Operations during the Russo-Ukrainian war: From Strange Patterns to Alternative Futures'. Center for Strategic and International Studies. Available at: https://www.jstor.org/stable/resrep52130 (Accessed: 31 October 2023).
[57] Cyfirma. (2023). 'APT Quarterly Highlights - Q3 2023'. Cyfirma. Available at: https://www.cyfirma.com/outofband/apt-quarterly-highlights-q3-2023/ (Accessed: 31 October 2023).
[58] SCPC SSSCIP. (2023). 'Q3 2023 Performance Report'. State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine. Available at: https://scpc.gov.ua/api/files/6ce94c1b-0431-4187-b8e3-376457f9f8a2 (Accessed: 30 November 2023).
[59] NKSC. (2023). 'Report of Cyber Lessons Learned during the War in Ukraine.' Regional Cyber Defence Center of Lithuania. Available at: https://www.nksc.lt/doc/rkgc/report_on_cyber_lessons_learned_during_the_war_in_ukraine.pdf (Accessed: 30 September 2023).
[60] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 30 November 2023).
[61] Ibid.
[62] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 30 November 2023).
[63] Ibid.
[64] United Kingdom College of Policing (n.d.) Delivering effective analysis. Available at: https:// www.college.police.uk/app/intelligence-management/analysis/delivering-effective-analysis (Accessed: 6 December 2022)