CyberPeace Institute

Quarterly Analysis Report
Q4 October to December 2022

Cyber Dimensions
of the Armed Conflict in Ukraine

TABLE OF CONTENTS

Report Methodology 3

Trends and Emerging Issues 4

Ukraine 4

Facts & Figures 6

Russian Federation 7

Facts & Figures 11

Other Countries 12

Facts & Figures 15

Harm and Impact on Civilians and People 16

Wider Contextual Considerations 18

References 20

Report Methodology

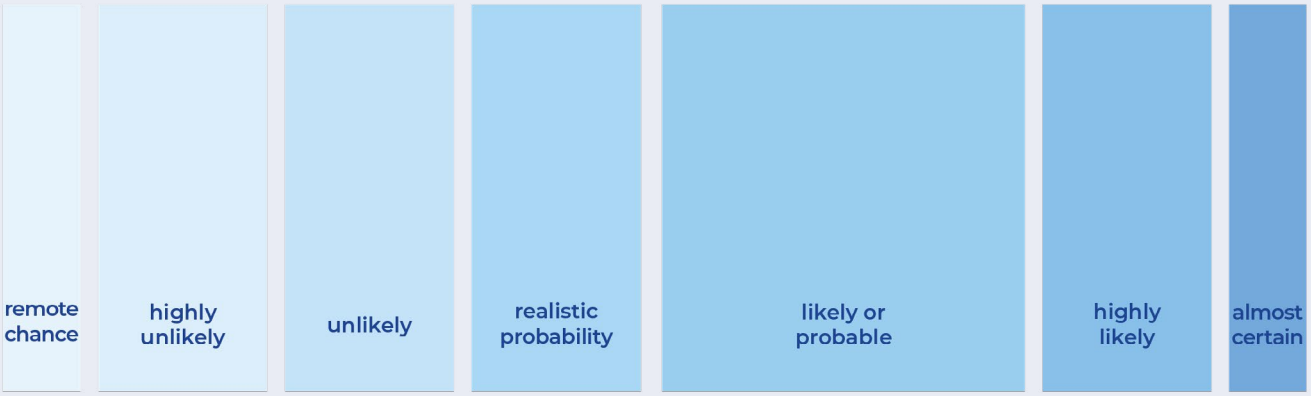
This report focuses on the incidents documented by the CyberPeace Institute in the fourth quarter of 2022. Therefore, analysis will only cover attacks and campaigns between October 1 and December 31, 2022. For trends-based analysis, the Institute may refer to numbers during a wider date range, in this case the dates will be 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[1] #Ukraine. Specific details and sources of information regarding any individual cyber incidents referenced in this report can be found in the Attack Details[2] 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[3]. Additionally, the CyberPeace Institute distinguishes between singular incidents and campaigns.[4]

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'.[5] 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

Trends and Emerging Issues

Ukraine

The CyberPeace Institute documented 249 cyber incidents against entities in Ukraine between January and December 2022. With **71 incidents impacting 16 sectors in Q4**, there has been a **18.4% decrease** in incidents compared to the previous quarter. This decrease is driven by a decline in substantiated incidents targeting Ukrainian entities by pro-Russian hacktivist collectives.

Trends

DDoS attacks account for 87.3% of all incidents.

Hacktivist collectives account for 91.4% of all incidents targeting entities in Ukraine.

The most targeted sector in Ukraine was the **Financial sector which saw a 116.7% increase** compared to Q3.

Two campaigns were attributed to Russian state-sponsored threat actors:

- *Gamaredon*, attributed to Russia's Federal Security Services,[6] conducted a phishing campaign[7] emulating the State Special Communication Service of Ukraine. It distributed malware, including an info-stealer.
- *Sandworm*, attributed to Russia's foreign military intelligence,[8] distributed "Prestige" ransomware,[9] targeting Ukrainian organizations in the Transportation sector.

Emerging Issues

New malware

- The Microsoft Threat Intelligence Center has identified a campaign by *Sandworm* using **"Prestige" ransomware** to target organizations in the Transportation sector.
- The author(s) of the **"Azov"data wiper malware**[11] [12] falsely claim the malware was created by well-known security researchers, which they deny. It directs the targets to these researchers for the decryption keys. The malware is distributed through pirated software, key generators, and adware bundles.
- **"Somnia" malware** attributed to the threat actor *From Russia with Love (FRwL)*[13] steals Telegram session data to access users' accounts. The account is then used to transfer VPN connection configuration files to users and gain access to corporate networks.

Notable threat actor activity

- A 71.7% decrease in incidents attributed to the *People's CyberArmy*.
- An 88.9% increase in incidents attributed to *Anonymous Russia* and a 240% increase in incidents attributed to *NoName057(16)*.
- *KillNet* announced the creation of a forum that would unite all pro-Russian threat actors.

The Financial sector was targeted the most in Q4, with Ukraine's Public administration seeing a 52.2% decrease in attacks. The CyberPeace Institute noted increased attacks against the Transportation, Trade, and Administrative/Support sectors.

Media coverage of pro-Russian threat actors continued in Q4, with the leader of *Zarya,* a hacking collective, giving two interviews to a Russian news outlet[15] and a Russian radio station.[16] Furthermore, Russian government officials continued drawing attention to Russian threat actors by declaring the need to create a state-sponsored Russian "People's Cyber Front"[17] or simply uniting the already-active Russian threat actors under one umbrella[18]. Lastly, the Deputy of the Russian State Duma, Dmitry Gusev, announced that Russian threat actors must be assigned military ranks due to their performance.[19]

Notable incidents in Ukraine

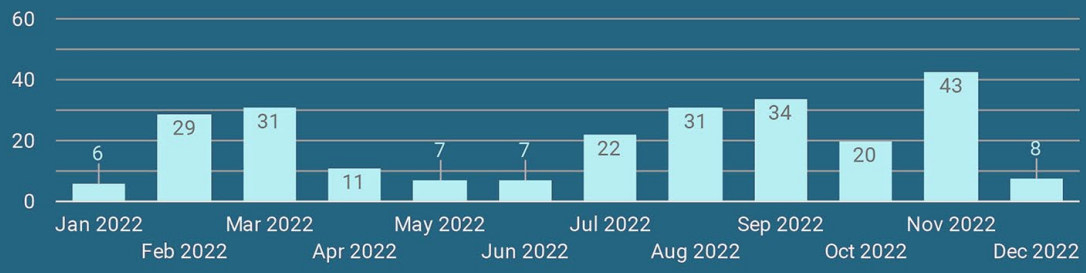
Disruption

December 3, 2022

Possible three-day-long DDoS campaign against the servers of a Ukrainian telecommunication company. *NoName057(16)* claimed responsibility for the campaign. The impact included disrupted accessibility to the online resources of the targeted organization.[20] [21] [22] [23] [24]

Facts & Figures

Ukraine



Incidents Jan-Dec 2022

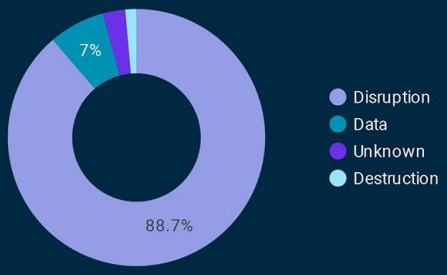
249

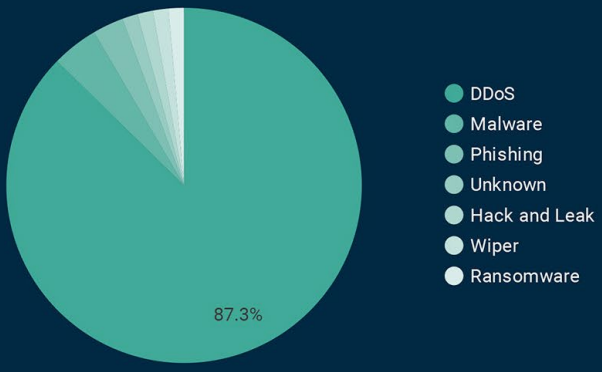
Sectors Jan-Dec 2022

21

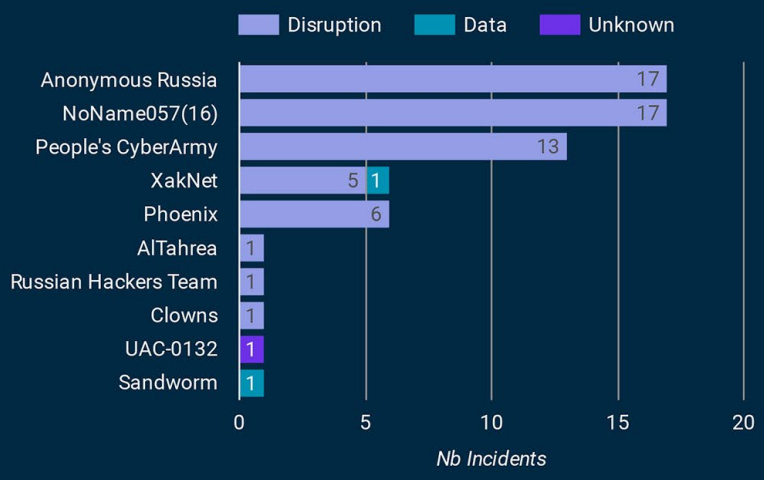
Q4 October - December 2022

Incidents	Sectors	Threat Actors
71	16	15
-18.4%	-5.9%	-11.8%





	Sector	Incidents	% Δ
1.	Financial	13	116.7%
2.	Public administration	11	-52.2%
3.	Transportation	9	125.0%
4.	ICT	6	0.0%
5.	Trade	5	25.0%
6.	Administrative / Supp...	5	66.7%
7.	Media	4	-71.4%
8.	Unknown	4	0.0%
9.	Energy	3	-25.0%
10.	Health	3	-
11.	Manufacturing	2	-60.0%
12.	Education	2	100.0%
13.	Professional / scientific	1	-
14.	Other service	1	-66.7%
15.	Agriculture	1	-
16.	Arts	1	-50.0%



Trends and Emerging Issues

Russian Federation

The CyberPeace Institute documented 178 cyber incidents against entities in the Russian Federation between January and December 2022. With **26 incidents impacting 11 sectors in Q4**, there has been a **45.8% decrease** in incidents compared to the previous quarter, marking a second consecutive quarter of declining incidents against entities in the Russian Federation.

Trends

The **ICT sector** was targeted the most in Q4 with six incidents.

The Public administration was the second most targeted sector, with four incidents; attacks against the Financial sector continue to persist with four incidents detected in Q4, down from 10 in Q3.

For the first time since the start of the conflict, the CyberPeace Institute has detected several attacks claimed by pro-Russian threat actors against Russian entities.

Emerging Issues

New Malware

Kaspersky Lab detected a cyberespionage campaign against major Russian companies. An unknown threat actor conducted the campaign through phishing emails targeting the companies' employees. The emails included a Word file titled "deferment from mobilization". A macro was activated upon opening the Word file, downloading malware on the target's device.[25]

Notable threat actor activity

The *National Republican Army*, a Russian-based collective opposing the government of President Putin, has been active both in the physical and digital world and published their manifesto in August 2022.[26] In the physical world, they have taken credit for sabotaging activities, such as setting cars and mobilization centers on fire. In Q4, the threat actor took credit for two significant cyberattacks, both reported by a Ukrainian newspaper with no further corroborating information. These incidents were a ransomware attack against a major Russian software development company;[27] [28] [29] and an alleged supply-chain cyberattack against Russian ICT companies, providing services in the area of national security to the government of the Russian Federation.[30]

While **cyberattacks against Russian entities decreased by 45.8%, the impact of the incidents was more pronounced than those in other countries**. The personal information of more than three million Russian citizens and millions of lines of additional personal information emerged in the public domain due to several hack and leak operations.

There is a realistic probability that pro-Ukrainian threat actors mostly targeted Russian ICT organizations because of the impact international sanctions have had on Russia's ICT sector. According to one article, "sanctions and the mass exodus of multinational corporations have eroded the industry's access to foreign capital and technology."[31] Russia's Minister of Digital Development, Communications and Mass Media stated that about 100,000 Russian IT specialists have left the country since the start of the conflict.[32] Furthermore, Western countries have banned the export of Western-made software to Russia.[33] To mitigate the impact of those sanctions, the Russian government announced a plan to finance the transition[34] to Russian-made software while also creating a department for the trade of pirated content.[35]

Among the incidents against entities in the Russian Federation, the CyberPeace Institute discovered for the first time several attacks claimed by pro-Russian threat actors. *KillNet* targeted SecurityLab, an online Russian cybersecurity news outlet, which shared a report arguing that *KillNet* has limited DDoS capabilities. This attack caused a dispute between pro-Russian threat actors *XakNet* and *KillNet,* resulting in DDoS[36] attacks being conducted by both threat actors against each other.

Mirai, a threat actor operating within the *KillNet* collective, claims to have targeted a Russian technology giant, referred to as Russia's alternative to Google. It is realistically probable that the attack occurred due to media information about the company's intentions of restructuring its business independently of Russia.[37] Lastly, citizens of the Republic of Dagestan protested the partial mobilization, which caused *PHOENIX*, a pro-Russian threat actor, to conduct DDoS attacks against their government's website.[38] [39]

Notable incidents in Russian Federation

Disruption

October 7, 2022

A Russian banking and financial services company headquartered in Moscow repelled a DDoS attack that lasted 24 hours.[40]

October 11, 2022

The *IT Army of Ukraine* conducted a cyberattack against a regional electric grid company, servicing the power grids of St Petersburg and Leningrad.[41] [42] [43] [44] According to the *IT Army of Ukraine*, the attack caused a power outage in St Petersburg and Leningrad whilst according to Russian news sources, the attack was neutralized, only causing minor disruptions to the operability of some of the target's online resources.

November 18, 2022

The Belarusian collective *Cyber Partisan* claims to have conducted a cyberattack against the Russian federal executive agency responsible for monitoring and controlling Russian mass media, including its internal network. The impact of the cyberattack is disputed. According to the threat actor, they allegedly stole 2 terabytes (TB) of information and encrypted the employees' workstations. According to a press release by the targeted organization the cyberattack was manageable, the perpetrators did not gain access to classified information, nor critical infrastructure, and the employees' workstations were not encrypted.[45] [46] [47]

November 29, 2022

Probable week-long DDoS campaign against a Russian bank. The *IT Army of Ukraine* claimed responsibility for the attack, which reportedly caused temporary difficulties in the performance of banking applications. Impacted applications allegedly included payments for fines and taxes, currency transfers and the bank's mobile application.[48] [49] [50]

Data

December 15, 2022

NLB, a pro-Ukrainian threat actor, leaked information of 1.5 million clients of a Russian online platform providing travel services.[51] *NLB* allegedly published three files containing information on 1.5 million clients, 400 000 orders, and the personal information of 900 000 tourists, including full names, passport details, phone numbers, IP addresses of users, and other personal and sensitive information.

October 2, 2022

The *National Republican Army* threat actor claimed to have stolen copies of all of the targeted ICT organization's data following a ransomware attack, including but not limited to credentials for bank accounts and personal accounts, sensitive employee information, phone numbers, addresses, contracts, and proprietary code for the target's clients and software.[52] [53]

October 18, 2022

The *National Republican Army* threat actor claimed to have committed a supply chain attack against an ICT organization. An unconfirmed media report indicated the hackers had "access to the architecture networks, databases, cloud solutions, and other information that is of key importance to the Russian Government".[54]

November 8, 2022

Pro-Ukrainian threat actors allegedly conducted a hack and leak operation against a Russian social media video service. Four files consisting of tables with 2 million rows were published in the public domain, containing data such as mobile phone and the registration date of users, information about the device from which they logged in, the type of connection, associated third-party service identifiers, such as the VKontakte ID, and other information. The leaked data includes data up to July 1, 2022.[55] [56]

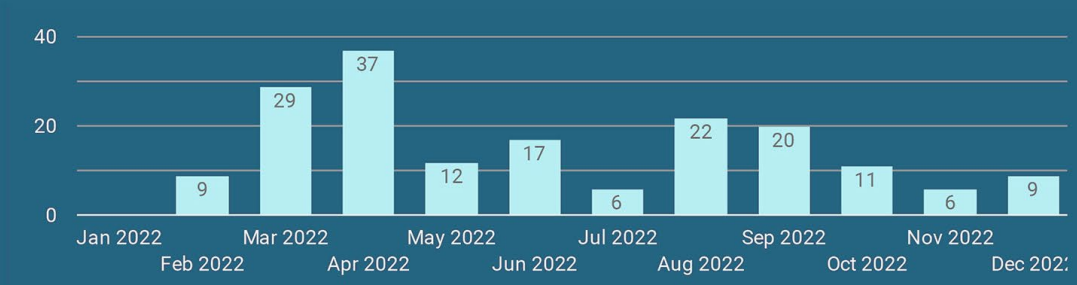
Disinformation and Propaganda

December 31, 2022

The *IT Army of Ukraine* claimed responsibility for an alleged campaign resulting in the defacement of the websites of at least seven Russian district administrations. The impacted websites displayed the New Year's speech of the President of Ukraine.[57]

Facts & Figures

Russian Federation

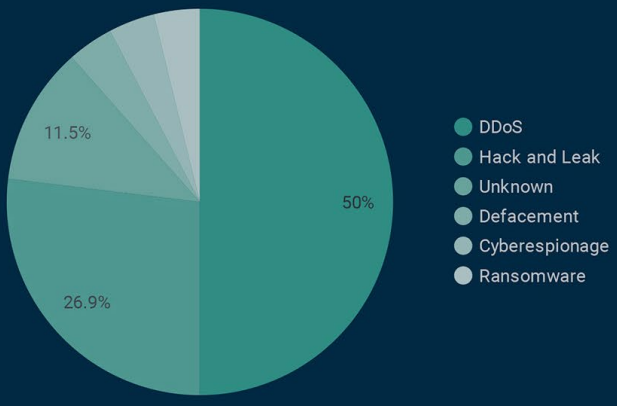


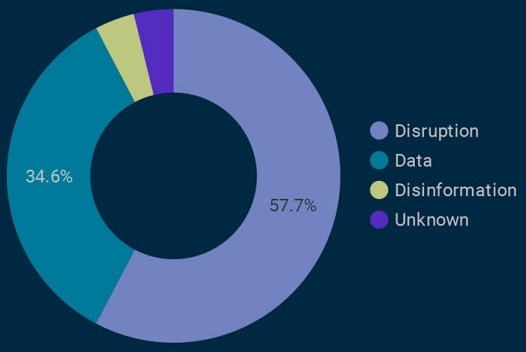
Incidents Jan-Dec 2022
178

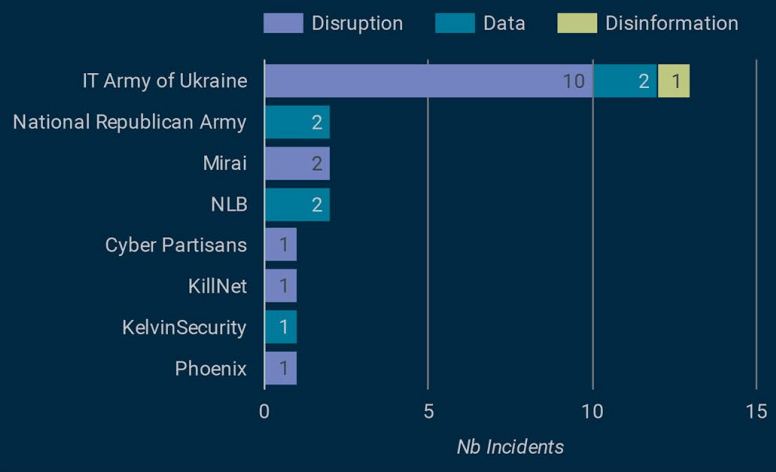
Sectors Jan-Dec 2022
21

Q4 October - December 2022

Incidents	Sectors	Threat Actors
26	11	8
-45.8%	-8.3%	-20.0%







	Sector	Incidents ▾	% Δ
1.	ICT	6	20.0%
2.	Public administra...	4	33.3%
3.	Financial	4	-50.0%
4.	Professional / sci...	4	-
5.	Energy	2	100.0%
6.	Trade	1	-66.7%
7.	Unknown	1	-
8.	Media	1	-90.9%
9.	Education	1	-
10.	Transportation	1	-75.0%
11.	Arts	1	-

Trends and Emerging Issues

Other Countries

The CyberPeace Institute documented 464 cyber incidents between January and December 2022 against entities in nation-states that are not the two belligerent states. With **239 incidents impacting 16 sectors in Q4**, the CyberPeace Institute notes a **368.6% increase in attacks** against states outside the two belligerent states compared to the previous quarter.

Trends

DDoS attacks account for 98.7% of all incidents.

Entities in **27 different countries** were targeted in Q4, **an increase of 42.1 %** compared to Q3.

In Q4, the most targeted entities by pro-Russian threat actors were in Poland (70 incidents), Latvia (32 incidents), and the United States of America (22 incidents).

The **Public administration** is the most targeted sector in Q4, with a **203.6% increase** compared to Q3, continuing the trend set in Q1 and Q2 of 2022.

The **Transportation sector remains a high-priority target for pro-Russian threat actors, with an increase of 31.3%** in the incidents compared to Q3.

The third most targeted sector was the Administrative/Support sector, with a 200% increase in attacks against it. The Financial sector saw a 20% decrease in attacks compared to Q3.

Emerging Issues

New malware

As per attacks against entities in Ukraine, entities in the Polish Transportation sector were also targeted by the "Prestige" ransomware.

Notable threat actor activity

The CyberPeace Institute notes an increase in the activities of pro-Russian threat actors, with *NoName057(16)*[59] being the most active threat actor for the second consecutive quarter, with 46.6% attributed attacks out of all incidents. *Anonymous Russia* has also increased their activities by 472.7% compared to Q3.

Anonymous Russia is a pro-Russian threat actor allegedly founded[60] by individuals who left the *KillNet* collective. The Telegram channel of the threat actor was created on July 10, 2022, and has been consistently active ever since. *Anonymous Russia* specializes in DDoS attacks against entities outside the two belligerent states.

Anonymous Russia has a DDoS-as-a-sevice tool advertised in the threat actor's Telegram channel. On September 29, *Anonymous Russia* announced they had joined the *KillNet* collective. Nevertheless, *Anonymous Russia* continues to claim responsibility for incidents on its Telegram channels, so the CyberPeace Institute tracks them under their name.

The CyberPeace Institute noted a 368.6% increase compared to Q3 in the activities of pro-Russian threat actors against entities outside the two belligerent states. The increase in attacks is likely associated with increased collaboration between pro-Russian threat actors.[61]

After the noted decrease in the activities of pro-Russian threat actors, and their announcement for the preparations of more complex actions in Q3, the CyberPeace Institute noted a 46.6% increase compared to Q3 in the activities of *NoName057(16)*, and 472.7% increase in the activities of *Anonymous Russia*. In Q3, *Anonymous Russia* and more than a dozen other pro-Russian threat actors joined the *KillNet* collective.[69] Nevertheless, the CyberPeace Institute continues to document the attribution of incidents according to the ownership of the channels the incidents were announced on.

Attacks against entities in **Poland, Latvia, and the United States of America increased significantly**, by 169.2%, 113.3%, and 266.7% respectively, compared to Q3. In contrast, **attacks against Lithuanian entities decreased by 46.7%** in Q4, compared to Q3 when pro-Russian threat actors targeted Lithuanian organizations the most.

Cyber incidents targeting entities in Poland

Incidents targeting Polish entities represented 29.3% of all recorded incidents in Q4 against non-belligerent states. Furthermore, 40% of all incidents recorded against the Public administration sector were conducted against the Polish state administration. Nearly half of the incidents against Polish entities occurred in the first two weeks of November, which is highly likely connected to the increased geopolitical tensions between the governments of Poland and the Russian Federation:

- Firstly, on October 30, TASS published an announcement by a Russian representative of the occupied region of Luhansk stating that Poland will soon annex the Western parts of Ukraine.[62]
- On November 2, the Polish Defense Minister announced that Poland has begun building a wall on the border with Kaliningrad, Russia's European enclave.[63]
- On November 4, during the commemoration of Russia's National Unity Day, celebrating a Russian uprising that freed Moscow from Polish-Lithuanian occupation forces on November 4, 1612, President Putin repeated the announcement made by TASS, emphasizing Polish expansionism into Ukraine as a threat.[64]

Cyber incidents targeting entities in Latvia

As in Q3, Latvian organizations were amongst the most targeted by pro-Russian threat actors, highly likely caused by the continued support of the Latvian government towards Ukraine. Latvia's Minister of Foreign Affairs tweeted on October 11 that the country provides the most significant monetary support for Ukraine's military, proportionate to its GDP, amongst all of Ukraine's allies.[65] Additionally, on November 29, Latvia's foreign minister spoke in favor of NATO allowing Ukraine to attack military targets inside Russian territory[66]. Latvia has also supported Ukraine's media[67] while banning a Russian TV channel operating within Latvia's territory.[68]

Notable incidents

Disruption

October 5, 2022

KillNet claimed responsibility for a confirmed DDoS campaign targeting the websites of 12 states in the United States of America. The impact resulted in a temporary inaccessibility to the websites.[70]

October 10, 2022

KillNet claimed responsibility for a probable DDoS campaign targeting the websites of 48 American airports. According to news media reports, the campaign successfully disrupted the operability of 14 websites.[71]

October 15, 2022

KillNet and *Anonymous Russia* claimed responsibility for a confirmed DDoS campaign targeting the websites of 24 Bulgarian entities operating in six sectors, including the ICT, Transportation, and Financial sectors in Bulgaria. The impact was temporary inaccessibility to the websites.[72]

November 11, 2022

KillNet claimed responsibility for a possible DDoS campaign targeting two Greek ministries, allegedly impacting the operability of 800 websites. According to Greek media, the campaign blocked the online system for medical prescriptions during the weekend. As a result, doctors and pharmacies could not provide medication via that system.[73]

November 23, 2022

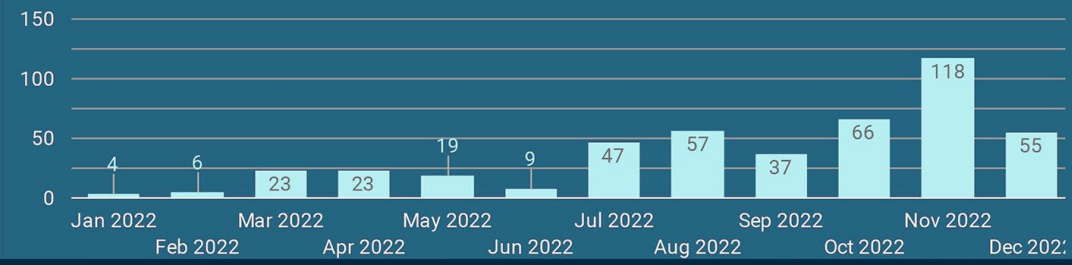
Anonymous Russia claimed responsibility for a confirmed DDoS attack against the servers of the European Parliament.
The impact was inaccessibility to the website of the European Parliament for several hours.[74]

December 15, 2022

NoName057(16) claimed responsibility for a confirmed DDoS attack against the website of the lower house of Poland's parliament. The impact was temporary inaccessibility to the website.[75]

Facts & Figures

Other Countries



Incidents Jan - Dec 2022

464

Sectors Jan - Dec 2022

23

Q4 October - December 2022

Incidents

239

368.6%

Countries

27

42.1%

Sectors

16

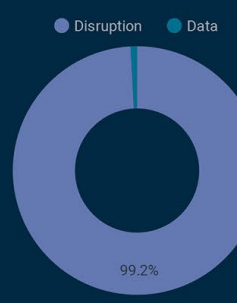
-15.8%

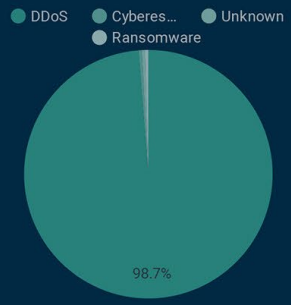
Threat Actors

13

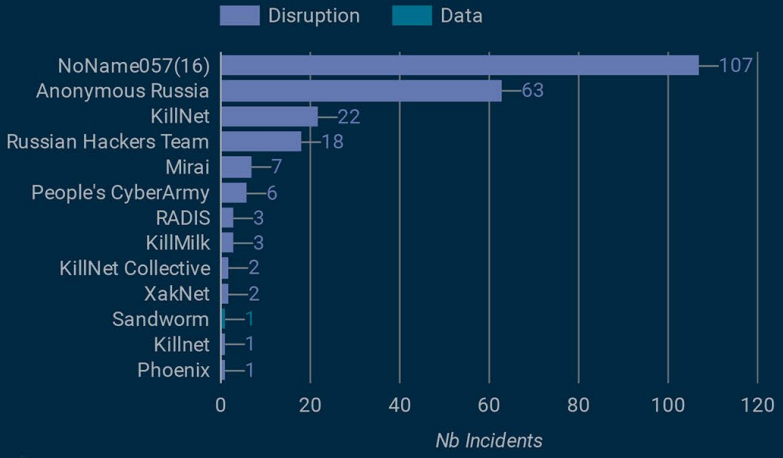
8.3%

	Country	Incid...	% Δ
1.	POLAND	70	169.2%
2.	LATVIA	32	113.3%
3.	UNITED STATES	22	266.7%
4.	LITHUANIA	16	-46.7%
5.	CZECH REPUBLIC	15	1,400.0%
6.	UNITED KINGDOM	11	266.7%
7.	ESTONIA	11	-15.4%
8.	REPUBLIC of MOLDOVA	11	1,000.0%
9.	BULGARIA	9	-
10.	FINLAND	6	500.0%
11.	GREECE	5	-
12.	KAZAKHSTAN	3	-
13.	ROMANIA	3	-
14.	CANADA	3	-
15.	FRANCE	3	200.0%





	Sector	Nb Incidents	% Δ
1.	Public administration	85	203.6%
2.	Transportation	42	31.3%
3.	Administrative / Support	21	200.0%
4.	Financial	19	-20.8%
5.	ICT	16	100.0%
6.	Energy	13	160.0%
7.	Manufacturing	12	100.0%
8.	Media	12	100.0%
9.	Other service	5	-16.7%
10.	Trade	3	200.0%



Harm and Impact on Civilians and People

The CyberPeace Institute documented 34.8% more DDoS attacks in Q4 compared to Q3. Apart from singular incidents with a more noticeable impact, DDoS attacks conducted by pro-Russian threat actors have had a relatively low impact, temporarily blocking the connectivity to the targets' websites. As noted by the EclecticIQ Threat Research Team,[76] the pro-Russian collective *KillNet* has limited DDoS capabilities, stemming from the highly probable lack of experience of its members. Nevertheless, *KillNet*, through its attacks, actively amplifies the Russian narrative set by Russian government officials. According to the OECD, "Russia's disinformation campaigns purposefully confuse and undermine information environments. Their efforts seek to cause confusion, complicate efforts to reach consensus, and build support for Russia's goals, while undermining the legitimacy of Ukraine's response."[77]

Evolving cyber threats of pro-Russian threat actors

There have already been some signs of the preparation for more complex cyberattacks. In a security alert, Microsoft warned of a future intensification of cyberattacks by pro-Russian threat actors.[78] The head of Microsoft's Digital Threat Analysis Center suggests that due to a lack of military success, pro-Russian and state-sponsored threat actors will intensify their activities against Ukrainian and European critical infrastructure, which can directly impact civilians and people. The "Prestige" ransomware attack against entities in the Transportation sector in Ukraine and Poland[79] is an example of Russia's willingness "to use its cyberweapons against organizations outside Ukraine in support of its ongoing war".[80] According to media reports, Dragos, an American cybersecurity company, Russian-affiliated threat actors *Xenotime* and *Kamacite* have been conducting exploratory research into the systems of Dutch liquified natural gas (LNG) terminals in Rotterdam.[81] Furthermore, Microsoft's security alert aligns with a recent report by Finland's security services[82], warning of an intensification of malicious cyber activities, more specifically, cyberespionage campaigns, by pro-Russian actors.

The CyberPeace Institute documented several DDoS attacks conducted by pro-Russian threat actors against entities in the Russian Federation. The likely reason for those attacks was either the distribution of news deemed hostile to the Russian Federation, such as the reporting of EclecticIQ research into *KillNet*'s low DDoS capabilities by a Russian news media[83]; or anti-conflict protests in Russian Republics, such as the DDoS attacks against Dagestan's main website.

The impact of incidents conducted by pro-Ukrainian threat actors

Although the attacks attributed to pro-Ukrainian threat actors were fewer than those attributed to pro-Russian threat actors, the impact of attacks against entities in the Russian Federation was more pronounced. It is likely that the reason for the higher impact of cyberattacks allegedly committed by pro-Ukraine threat actors, mainly the *IT Army*

of Ukraine, is the latter's status as a state-backed collective that also uses DDoS crowdsourcing offensive tools.[84]

In Q4, pro-Ukrainian threat actors conducted several hack and leak operations, releasing the personal data of nearly three million Russian citizens into the public domain. As noted in the previous report for Q3, hack and leak operations pose a multitude of risks to governments, civilians and the general population.

According to a recent announcement for the media by the Russian service for intelligence of data leaks and monitoring of the darknet DLBI (Data Leakage & Breach Intelligence), the data of around three-quarters of Russia's citizens was leaked into the public domain throughout 2022, including 99.8 million unique email addresses and 109.7 million unique phone numbers.[85] [86] As stated by the head of DLBI : "password reuse attacks are becoming a real headache for information security services. Logins and passwords that comply with password strength guidelines get leaked, and then collected by hackers and used to attack corporate and government resources. In particular, a similar scheme was used by Ukrainian "Hacktivists" in several recent attacks on the websites of Russian departments".[87]

Wider Contextual Considerations

Other research

During Q4, several entities researched and investigated one of the most active pro-Russian threat actors, *KillNet*. Some of the investigations[88] [89] focused on their founder: an unknown person going by the pseudonym *"KillMilk"*. Whilst other research focused on *KillNet*'s structure, development, and targeting such as research by SocRadar,[90] EclecticIQ,[91] Groupsense[92] and SingCert.[93]

Carnegie Endowment for International Peace published three reports on the cyber conflict within the context of the conflict in Ukraine:

- A report into the mismatch between expectations and reality of Russian cyber operations,[94]
- An evaluation of the International cyber support for Ukraine,[95]
- An evaluation of the impact of Russia's Wartime Cyber Operations.[96]

The European Union Agency for Cybersecurity published its annual report on the status of the cybersecurity threat landscape in 2022, in which it discusses the consequences stemming from the conflict in Ukraine.[97]

Research conducted by the cybersecurity company Positive Technologies discovered that the large majority (96%) of Russian companies that formed part of their research sample are vulnerable to intrusions from an external attacker. Furthermore, the research found that 86% of the sample's Local Area Network was vulnerable to even low-skilled attackers.[98]

Lastly, the non-profit organization Access Now published a report on Internet shutdowns in Ukraine[99]. The report argues that Internet shutdowns in Ukraine are part of the broader Russian military strategy and have been implemented in four stages:

1. Destroying civilian telecommunication infrastructure.
2. Rerouting[100] internet traffic and seizing communication equipment.
3. Imposing censorship and surveillance.
4. Using shutdowns and blackouts as retaliation.

Events

One of the most important events in Q4 was a change in the leadership of the Russian army in Ukraine.[101] After General Surovikin took the lead, aerial bombardment became a key tactic in Russia's offensive, resulting in several Internet shutdowns caused by power outages or the targeting of the Internet infrastructure.[102] [103] [104]

The attention of the Russian media and government officials towards pro-Russian threat actors has increased in Q4. The head of the State Duma Committee on Information Policy of the Russian Federation argued in favor of Russia opening a full-fledged IT front against Ukraine, targeting Ukraine's critical infrastructure, albeit clarifying that he is not talking about targeting civilian infrastructure.[105] After that, **the State Duma deputy proposed the creation of a "People's Cyber Front"**, highly likely suggesting the creation of an entity

similar to Ukraine's IT Army of Ukraine.[106] The Duma's deputy also proposed the assigning of military ranks to Russian hackers.[107] Lastly, in December, the Deputy Chairman of the State Duma Committee on Information Policy, Information Technology, and Communications declared the need for creating a cyber army within the structures of Russia's military.[108]

Economic sanctions, military aid, and public statements

Sanctions and statements

Along with the Eighth and Ninth EU packages of sanctions against Russia,[109] [110] several other countries implemented additional sanctions in Q4. A more thorough timeline of sanctions is available at S&P Global.[111]

Several statements increased tensions between non-belligerent states and the Russian Federation. The Latvian Foreign Minister urged the supply of offensive weapons to Ukraine and called for a greenlight for Ukrainian strikes against Russian military infrastructure within the territories of the Russian Federation. The European Parliament declared Russia a state-sponsor of terrorism.[113]

Other countries announced their continued support for Ukraine, such as Greece.[114] Moldova[115] announced a new agreement of cooperation with Ukraine in air defense and improved border control. In early November, NATO announced that their next leaders' summit would be in Lithuania in July 2023.[116]

Military aid

Several countries announced additional military aid to Ukraine, including the United States of America,[117] Bulgaria,[118] Finland,[119] Slovakia,[120] Canada,[121] Denmark,[122] Netherlands,[123] Japan,[124] and the Czech Republic.[125]

In Q4 incidents were documented against entities in all of the aforementioned countries except the Netherlands, Denmark and Japan. It is worth noting that entities in both Denmark and Japan were targeted by cyberattacks related to the conflict in Q3 2022.

References

[1] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 17 January 2023)

[2] Ibid.

[3] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 17 January 2023).

[4] Ibid.

[5] 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)

[6] SSU. (2021) 'Gamaredon/Armageddon Group'. Security Service of Ukraine. Available at: https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf (Accessed: 6 December 2022)

[7] CERT-UA. (2022). 'Kiberataka hrupy UAC-0010: rozsylannia elektronnykh lystiv, nachebto, vid imeni Derzhspetszviazku (CERT-UA#5570)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/2681855 (accessed: 11 November 2022).

[8] United States District Court (2020) 'United States of America vs Yuriy Sergeyevich Andrenko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin. Western District of Pennsylvania. Available at: https://www.justice.gov/opa/press-release/file/1328521/download (Accessed: 2 December 2022).

[9] Microsoft. (2022) 'New "Prestige" ransomware impacts organizations in Ukraine and Poland". Microsoft Security Threat Intelligence. Available at: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (Accessed: 11 October 2022).

[10] Ibid.

[11] Abrams, L. (2022) 'New Azov data wiper tries to frame researchers and BleepingComputer'. BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/new-azov-data-wiper-tries-to-frame-researchers-and-bleepingcomputer/ (Accessed: 30 October 2022).

[12] Vinopal, J. (2022) 'Pulling the curtains on Azov ransomware: not a skidsware but polymorphic wiper'. CheckPoint Research. Available at: https://research.checkpoint.com/2022/pulling-the-curtains-on-azov-ransomware-not-a-skidsware-but-polymorphic-wiper/ (Accessed: December 15 2022).

[13] CERT-UA. (2022) 'Informatsiia shchodo kiberatak hrupy UAC-0118 (FRwL) z vykorystanniam shkidlyvoi prohramy Somnia (CERT-UA#5185)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/2724253 (Accessed: 12 November 2022).

[14] KillNet_Reservs (2022) [Telegram] 23 December. Available at: https://t.me/killnet_reservs/4507 (Accessed: 23 December 2022).

[15] Kil'djushkin R. (2022) '«My voiny, a ne terroristy». Interv'ju s osnovatelem hakerskoj gruppy Zarja'. Gazeta. Available at: https://m.gazeta.ru/tech/2022/11/06/15734689.shtml?utm_source=yxnews&utm_medium=mobile&utm_referrer=https%3A%2F%2Fdzen.ru%2Fnews%2Fsearch%3Ftext%3D (Accessed: 10 November 2022).

[16] Shaulina, L. and Belousov, V. (2022) '"My ne ob"javljali kibervojnu, jeto otvet na kiberagressiju Ukrainy"'. Smotrim. Available at: https://smotrim.ru/video/2506836?utm_source=internal&utm_medium=special-radiorus&utm_campaign=special-radiorus-videos (Accessed: 10 November 2022).

[17] Gusev, D. (2022) 'Kiberbezopasnost' Rossii i cifrovaja jekonomika. Kruglyj stol v Gosudarstvennoj Dume'. VKontakte. Available at: https://vk.com/dg_prav?w=wall3726796_8362 (Accessed: 26 November 2022).

[18] Mal'ceva, E. (2022) 'Deputat Gosdumy Matvejchev prizval sozdat' v Rossii kibervojska'. Ura. Available at: https://ura.news/news/1052608382 (Accessed: 9 December 2022).

[19] Gusev, D. (2022) [Telegram] 22 November. Available at: https://t.me/gusev_tg/1466 (Accessed: 22 November 2022).

[20] NoName057(16) (2022) [Telegram] 3 December. Available at: https://t.me/noname05716/1169 (Accessed 5 December 2022).

[21] NoName057(16) (2022) [Telegram] 5 December. Available at: https://t.me/noname05716/1206 (Accessed 5 December 2022).

[22] NoName057(16) (2022) [Telegram] 5 December. Available at: https://t.me/noname05716/1221 (Accessed 5 December 2022).

[23] NoName057(16) (2022) [Telegram] 6 December. Available at: https://t.me/noname05716/1223 (Accessed 6 December 2022).

[24] NoName057(16) (2022) [Telegram] 7 December. Available at: https://t.me/noname05716/1232 (Accessed 7 December 2022).

[25] Kaspersky. (2022) 'Zloumyshlenniki obeshhajut otsrochku ot sluzhby sotrudnikam krupnyh rossijskih kompanij'. Kaspersky Lab. Available at: https://www.kaspersky.ru/about/press-releases/2022_zloumyshlenniki-obeshayut-otsrochku-ot-sluzhby-sotrudnikam-krupnyh-rossijskih-kompanij?ysclid=l9pbcvqyb760749947 (Accessed: 31 October 2022).

[26] Nacional'naja Respublikanskaja Armija | Rospartizan (2022) [Telegram] 21 August. Available at: https://t.me/nationalrepublicanarmy/9 (Accessed: 3 November 2022).

[27] Smart, J.J. (2022) 'Russian Citizens Wage Cyberwar From Within'. Kyiv Post. Available at: https://www.kyivpost.com/world/russian-citizens-wage-cyberwar-from-within.html (Accessed: 3 October 2022).

[28] Zelealem, F. (2022) 'Kremlin targeted by Russian cyber-attack as citizens aim to overthrow Putin'. Daily Star. Available at: https://www.dailystar.co.uk/news/world-news/kremlin-targeted-russian-cyber-attack-28138654 (Accessed: 3 October 2022).

[29] Nacional'naja Respublikanskaja Armija | Rospartizan (2022) [Telegram] 2 October. Available at: https://t.me/rospartizan/1125 (Accessed: 3 October 2022).

[30] Smart, J.J. (2022) 'Russians Against Putin: NRA Claims Massive Hack of Russian Government Contractors' Computers'. Kyiv Post. Available at: https://www.kyivpost.com/russias-war/russians-against-putin-nra-claims-massive-hack-of-russian-government-contractors-computers.html (Accessed: 19 October 2022).

[31] AlJazeera. (2022) 'Shunned by the West, Russia's IT sector goes on the defensive'. AlJazeera. Available at: https://www.aljazeera.com/news/2022/11/21/russias-it-sector-facing-ctrl-alt-delete-moment-in-midst-of-war (Accessed: 13 January 2023).

[32] Interfax (2022) 'About 100,000 IT specialists left Russia in 2022 - digital development minister'. Available at: https://interfax.com/newsroom/top-stories/86316/ (Accessed: 25 January 2023).

[33] US Department of State (20220 'The Impact of Sanctions and Export Controls on the Russian Federation. Office of the Spokesperson. Available at: https://www.state.gov/the-impact-of-sanctions-and-export-controls-on-the-russian-federation/ (Accessed: 25 January 2023).

[34] SecurityLab. (2022) 'Gosudarstvo gotovo sofinansirovat' do 80% zatrat po perehodu na rossijskoe PO'. Available at: https://www.securitylab.ru/news/534246.php (Accessed: 10 January, 2023).

[35] Dzen. (2022) 'Nelicenzionnoe PO v Rossii — polnyj zapret ili legalizacija?' Dzen. Available at: https://dzen.ru/a/Y6YDuaLdIm_ebLdD (Accessed: 10 January 2023)

[36] XakNet Team (2022) [Telegram] 14 November. Available at: https://t.me/xaknet_team/409 (Accessed: 14 November 2022)

[37] Chan, B. (2022) 'Russia's ongoing invasion of Ukraine is pushing out one of Russia's biggest tech giants'. Insider. Available at: https://www.insider.com/russian-tech-giant-wants-out-of-country-ukraine-war-rages-2022-11 (Accessed: 17 January 2022).

[38] PHOENIX (2022) [Telegram] 6 October. Available at: https://tgstat.ru/en/channel/@phoenixinform/811 (Accessed: 7 October 2022).

[39] PHOENIX (2022) [Telegram] 6 October. Available at: https://tgstat.ru/en/channel/@phoenixinform/818 (Accessed: 7 October 2022).

[40] TASS. (2022) 'Sberbank v nachale oktjabrja otrazil krupnuju kiberataku s uchastiem bolee 100 tys. hakerov'. TASS. Available at: https://tass.ru/ekonomika/16146055?ysclid=l9xxzlpre8520120210 (Accessed: 26 October 2022)

[41] IT Army of Ukraine (2022) [Telegram] 16 October. Available at: https://t.me/s/itarmyofukraine2022/809 (Accessed: 17 October 2022).

[42] Kommersant (2022) 'Jelektroseti Sankt-Peterburga i Leningradskoj oblasti podverglis' kiberatake'. Kommersant. Available at: https://www.kommersant.ru/doc/5608338?ysclid=l9dzvb9xvo515155712 (Accessed: 17 October 2022).

[43] Kommersant (2022) 'V LOJeSK zajavili o kiberatake na svoju setevuju infrastrukturu'. Kommersant. Available at: https://www.kommersant.ru/doc/5608331?ysclid=l9dzvymuje836775500 (Accessed: 17 October 2022).

[44] ABnews (2022) 'TEHNIKI AO «LOJeSK» OTRAZILI MASSIROVANNUJu KIBERATAKU NA INFRASTRUKTURU KOMPANII'. ABnews. Available at: https://abnews.ru/2022/10/13/tehniki-ao-loesk-otrazili-massirovannuyu-kiberataku-na-infrastrukturu-kompanii?ysclid=l9dzwehjf805949655 (Accessed: 17 October 2022).

[45] KiberPartizany (2022) [Telegram] 18 November. Available at: https://t.me/cpartisans/960 (Accessed: 21 November 2022).

[46] TASS (2022) 'Hakery atakovali Glavnyj radiochastotnyj centr Roskomnadzora'. TASS. Available at: https://tass.ru/obschestvo/16372881 (Accessed: 21 November 2022).

[47] Dmitrova, D. (2022) 'Glavnyj radiochastotnyj centr Roskomnadzora podvergsja hakkerskoj atake'. Gazeta. Available at: https://www.gazeta.ru/tech/news/2022/11/19/19071901.shtml?ysclid=latske26y2372604293 (Accessed: 21 November 2022).

[48] IT Army of Ukraine (2022) [Telegram] 29 November. Available at: https://t.me/itarmyofukraine2022/902 (Accessed: 8 December 2022).

[49] IT Army of Ukraine (2022) [Telegram] 6 December. Available at: https://t.me/itarmyofukraine2022/927 (Accessed: 8 December 2022).

[50] FrankMedia (2022) 'V VTB nabljudaetsja sboj pri perevodah i zachislenijah denezhnyh sredstv'. FrankMedia. Available at: https://frankrg.com/104253 (Accessed: 8 December 2022).

[51] SecurityLab (2022) 'Proizoshla utechka dannyh pol'zovatelej Level.travel'. SecurityLab. Available at: https://www.securitylab.ru/news/535272.php?r=2 (Accessed: 14 December 2022).

[52] Nacional'naja Respublikanskaja Armija | Rospartizan (2022) [Telegram] 2 October. Available at: https://t.me/rospartizan/1125 (Accessed: 3 October 2022).

[53] Smart, J.J. (2022) 'Russian Citizens Wage Cyberwar From Within'. Kyiv Post. Available at: https://www.kyivpost.com/world/russian-citizens-wage-cyberwar-from-within.html (Accessed: 3 October 2022).

[54] Smart, J.J. (2022) 'Russians Against Putin: NRA Claims Massive Hack of Russian Government Contractors' Computers'. Kyiv Post. Available at: https://www.kyivpost.com/russias-war/russians-against-putin-nra-claims-massive-hack-of-russian-government-contractors-computers.html (Accessed: 19 October 2022).

[55] In2security (2022) [Telegram] 8 November. Available at: https://t.me/in4security/939 (Accessed: Accessed 14 November 2022).

[56] Kommersant (2022) 'Yappy poshel po stopam Rutube'. Kommersant. Available at: https://www.kommersant.ru/doc/5653066 (Accessed: 14 November 2022).

[57] IT Army of Ukraine (2022) [Telegram] 31 December. Available at: https://t.me/itarmyofukraine2022/943 (Accessed: 9 January 2023).

[58] Microsoft. (2022) 'New "Prestige" ransomware impacts organizations in Ukraine and Poland". Microsoft Security Threat Intelligence. Available at: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (Accessed: 11 October 2022).

[59] CyberPeace Institute (2022) 'Cyber Dimensions of the Armed Conflict in Ukraine'. Quarterly Analysis Report - Q3 July to September 2022. Available at: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/ (Accessed: 25 January 2023).

[60] SOCRadar Research (2022) 'Dark Web Profile: Killnet - Russian Hacktivist Group'. SOCRadar. Available at: https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/ (Accessed: 18 December 2022

[61] CyberPeace Institute (2022) 'Cyber Dimensions of the Armed Conflict in Ukraine'. Quarterly Analysis Report - Q3 July to September 2022. Available at: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/ (Accessed: 25 January 2023).

[62] TASS (2022) 'Poland begins 'quiet annexation' of Ukraine with West's consent - diplomat'. TASS. Available at: https://tass.com/politics/1529677 (Accessed: 16 January 2023).

[63] Euronews (2022) 'Poland begins building new wall along border with Russia's Kaliningrad'. Euronews. Available at: https://www.euronews.com/2022/11/02/poland-begins-building-new-wall-along-border-with-russias-kaliningrad (Accessed: 16 January 2023).

[64] TheFirstNews (2022) 'Poland accuses Putin of spreading disinformation'. TheFirstNews. Available at: https://www.thefirstnews.com/article/poland-accuses-putin-of-spreading-disinformation-34216 (Accessed: 16 January 2023).

[65] Rinkēvičs, E (2022) [Twitter] 12 October. Available at: https://twitter.com/edgarsrinkevics/status/1580079436170682370?ref_src=twsrc%5Etfw (Accessed: 13 January 2023).

[66] Anzalone, K. (2022) 'Latvian FM: NATO 'SHOULD NOT FEAR' MOSCOW'S RESPONSE TO STRIKES INSIDE RUSSIA'. The Libertarian Institute. Available at: https://libertarianinstitute.org/news/latvian-fm-nato-should-not-fear-moscows-response-to-strikes-inside-russia/ (Accessed: 13 January 2023).

[67] Delfi (2022) 'Latvija vydelit 550 tysjach evro na pokupku generatorov dlja ukrainskih mass-media'. Delfi. Available at: https://rus.delfi.lv/news/daily/latvia/latviya-vydelit-550-tysyach-evro-na-pokupku-generatorov-dlya-ukrainskih-mass-media.d?id=55050546 (Accessed: 13 January 2023).

[68] Financial Times (2022) 'Latvia bans exiled Russian news channel over 'threat to national security''. Financial Times. Available at: https://www.ft.com/content/c6617435-aaef-47da-aaea-d6d868f10ed8 (Accessed: 11 January 2023).

[69] KillNet_Reservs (2022) [Telegram] 29 September. Available at: https://t.me/killnet_reservs/2900 (Accessed: 29 September 2022)

[70] Lyngaas, S. (2022) 'Russian-speaking hackers knock US state government websites'. CNN. Available at: https://edition.cnn.com/2022/10/05/politics/russian-hackers-state-government-websites/index.html (Accessed: 5 October 2022).

[71] Wallace G., Lyngaas, S., Muntean P., and Watson, M. (2022) 'Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported'. CNN. Available at: https://edition.cnn.com/2022/10/10/us/airport-websites-russia-hackers/index.html) (Accessed: 10 October 2022).

[72] PRB (2022) 'Sofijska gradska prokuratura se samosezira po medijni publikacii za hakerski ataki sreshtu b"lgarski sajtove'. PRB. Available at: https://prb.bg/sgp/bg/news/60700-sofiyska-gradska-prokuratura-se-samosezira-po-mediyni-publikatsii-za-hakerski-at (Accessed: 15 October 2022).

[73] Tovima (2022) 'Epίthesh chάker sto yp. PShfiakής Diakyvérnhshς: Epicheírhsan na «ríksoyn» 800 istότopoyς toy Dhmosίoy'. Tovima. Available at: https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/ (Accessed: 15 November 2022)

[74] Metsola, R. (2022) [Twitter] 23 November. Available at: https://twitter.com/EP_President/status/1595443471518777345?cxt=HHwWgoC-sczYk6QsAAAA (Accessed: 23 November 2022)

[75] Government of Poland (2022) 'Russian cyberattacks'. Government of Poland. Available at: https://www.gov.pl/web/special-services/russian-cyberattacks (Accessed: 9 January 2022)

[76] EclecticIQ Threat Research Team (2022) 'Killnet Effectively Amplifies Russian Narratives but has Limited DDoS Capabilities'. SecurityBoulevard. Available at: https://securityboulevard.com/2022/10/killnet-effectively-amplifies-russian-narratives-but-has-limited-ddos-capabilities (Accessed: 13 October 2022).

[77] OECD (2022) 'Disinformation and Russia's war of aggression against Ukraine'. OECD. Available at: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/) (Accessed: 17 January 2022)

[78] Watts, C. (2022) 'Preparing for a Russian cyber offensive against Ukraine this winter'. Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/ (Accessed: 5 December 2022).

[79] Microsoft. (2022) 'New "Prestige" ransomware impacts organizations in Ukraine and Poland". Microsoft Security Threat Intelligence. Available at: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (Accessed: 11 October 2022).

[80] Watts, C. (2022) 'Preparing for a Russian cyber offensive against Ukraine this winter'. Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/ (Accessed: 5 December 2022).

[81] Yahoo (2022) 'Russian Hackers Target Dutch LNG Terminal'. Yahoo. Available at: https://finance.yahoo.com/news/russian-hackers-target-dutch-lng-170000151.html?&web_view=true&guccounter=1 (Accessed: November 28, 2022).

[82] SUPO (2022) 'Foreign intelligence and influence operations'. Finnish Security and Intelligence Service. Available at: https://supo.fi/en/intelligence-and-influence-operations (Accessed: 16 January 2023).

[83] SecurityLab. Available at: https://www.securitylab.ru/

[84] CyberPeace Institute (2022) 'Cyber Dimensions of the Armed Conflict in Ukraine'. Quarterly Analysis Report - Q3 July to September 2022. Available at: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine/ (Accessed: 25 January 2023).

[85] Interfax (2023) 'Jeksperty DLBI soobshhili ob utechke v set' dannyh 75% rossijan v 2022 godu'. Interfax. Available at: https://www.interfax.ru/russia/881264 (Accessed: 23 January 2023).

[86] DLBI (n.d.) 'Blog'. Data Leak & Breach Intelligence. Available at: https://dlbi.ru/ (Accessed: 25 January 2023).

[87] Tadviser (2022) '2022: Otkrytie API k sisteme monitoring a Data Leakage & Breach Intelligence'. Tadviser. Available at: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:DLBI:_Data_Leakage_&_Breach_Intelligence (Accessed: 25 January 2023).

[88] Krokford, T.P., Hansen, N., and Frigård, T. (2022) 'Hacker-pengene leder til ektepar'. Dagbladet. Available at: https://www.dagbladet.no/nyheter/hacker-pengene-leder-til-ektepar/77632007 (Accessed: 20 November 2022).

[89] News.bg (2022) 'Ustanoviha izv"rshitelJa na kiberatakata sreshtu pravitelstveni sajtove'. News.bg. Available at: https://news.bg/crime/ustanoviha-izvarshitelya-na-kiberatakata-sreshtu-pravitelstveni-saytove.html (Accessed: 16 October 2022).

[90] SOCRadar Research (2022) 'Dark Web Profile: Killnet - Russian Hacktivist Group'. SOCRadar. Available at: https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/ (Accessed: 18 December 2022).

[91] EclecticIQ Threat Research Team (2022) 'Killnet Effectively Amplifies Russian Narratives but has Limited DDoS Capabilities'. EclecticIQ. Available at: https://blog.eclecticiq.com/killnet-effectively-amplifies-russian-narratives-but-has-limited-ddos-capabilities (Accessed: 13 October 2022).

[92] Groupsense (2022) 'Killnet Increases Attacks on US Organizations'. Groupsense. Available at: https://www.groupsense.io/resources/killnet-increases-attacks-on-us-organizations?utm_campaign=Blogs&utm_content=232313653&utm_medium=social&utm_source=twitter&hss_channel=tw-2578641014 (Accessed: 9 January 2023).

[93] SingCERT (2022) 'Killnet- From Cybercriminals to Cyber-Partisans'. Singapore Computer Emergency Response Team. Available at: https://www.csa.gov.sg/singcert/Publications/killnet---from-cybercriminals-to-cyberpartisans (Accessed: 18 November 2022).

[94] Wilde, G. (2022) 'Cyber Operations in Ukraine: Russia's Unmet Expectations'. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607 (Accessed: 17 January 2023).

[95] Beecroft, N. (2022) 'Evaluating the International Support to Ukrainian Cyber Defense'. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (Accessed: 21 November , 2022).

[96] Bateman, J. (2022) 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications'. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 (Accessed: 10 January , 2023).

[97] ENISA (2022) 'ENISA Threat Landscape 2022'. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed: 9 January 2023).

[98] Positive technologies. (2022) 'Itogi pentestov — 2022'. Positive technologies. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/ (17 January 2023).

[99] Zhyrmont, A. (2022) '#KeepItOn: Who is shutting down the internet in Ukraine?'. AccessNow. Available at: https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/ (Accessed: 16 January 2023).

[100] Millochau G. and Raffray, E. (2022) 'Guerre en Ukraine: la lutte contre le contrôle du réseau informatique et son impact sur les civils. CyberPeace Institute. Available at: https://fr.cyberpeaceinstitute.org/actualites/guerre-en-ukraine-la-lutte-pour-le-controle-du-reseau-informatique-et-son-impact-sur-les-civils/ (Accessed: 26 January 2023).

[101] AlJazeera (2022) ''Shrinking operation': Russia names new Ukraine war commander'. AlJazeera. Available at: https://www.aljazeera.com/news/2022/10/8/russia-names-new-general-to-lead-ukraine-offensive-after-setbacks (Accessed: 18 January 2023).

[102] Chatterjee, M. (2022) 'Ukraine scrambles to keep internet up amid blackouts'. Politico. Available at: https://subscriber.politicopro.com/article/2022/10/ukraine-internet-blackouts-00063004 (Accessed: 18 January 2023)

[103] MaxNet (2022) 'How rolling blackouts in Ukraine affect the Internet'. MaxNet. Available at https://maxnet.ua/en/blog/yak-viyalovi-vidklyuchennya-elektroenergiyi-v-ukrayini-vidobrazhayutsya-na-roboti-internetu/ (Accessed: 18 January 2023).

[104] Ilyushina, M. (2022) 'Russia's new commander in Ukraine was decorated after brutality in Syria'. The Washington Post. Available at: https://www.washingtonpost.com/world/2022/10/12/sergei-surovikin-russia-ukraine-war/ (Accessed: 27 January 2023).

[105] SecurityLab (2022) 'Hinshtejn prizval k kiberudaram po IT-infrastrukture Ukrainy'. SecurityLab. Available at: https://www.securitylab.ru/news/534439.php (Accessed: 1 November 2022).

[106] Gusev, D. (2022) 'Kiberbezopasnost' Rossii i cifrovaja jekonomika. Kruglyj stol v Gosudarstvennoj Dume'. VKontakte. Available at: https://vk.com/dg_prav?w=wall3726796_8362 (Accessed: 26 November 2022).

[107] Gusev, D. (2022) [Telegram] 22 November. Available at: https://t.me/gusev_tg/1466 (Accessed: 22 November 2022).

[108] Mal'ceva, E. (2022) 'Deputat Gosdumy Matvejchev prizval sozdat' v Rossii kibervojska'. Ura. Available at: https://ura.news/news/1052608382 (Accessed: 9 December 2022).

[109] European Commission (2022) 'Ukraine: EU agrees on eighth package of sanctions against Russia'. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5989 (Accessed: 6 October 2022).

[110] European Commission (2022) 'Ukraine: EU agrees ninth package of sanctions against Russia'. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7652 (Accessed: 16 December 2022).

[111] S&P Global (2022) 'Sanctions against Russia - a timeline'. S&P Global Market Intelligence. Available at: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/sanctions-against-russia-8211-a-timeline-69602559 (Accessed: 16 January 2023).

[112] RFERL (2022) 'Latvia Says Ukraine Should Be Free To Strike Targets Inside Russia'. RadioFreeEuropeRadioLiberty. Available at: https://www.rferl.org/a/ukraine-strike-russia-targets/32155673.html (Accessed: 30 November 2022).

[113] European Parliament (2022) 'European Parliament declares Russia to be a state sponsor of terrorism'. European Parliament. Available at: https://www.europarl.europa.eu/news/en/press-room/20221118IPR55707/european-parliament-declares-russia-to-be-a-state-sponsor-of-terrorism (Accessed: 23 November 2022).

[114] President of Ukraine (2022) 'President of Ukraine had a meeting with the President of Greece'. President of Ukraine Official website. Available at: https://www.president.gov.ua/en/news/prezident-ukrayini-proviv-zustrich-z-prezidentom-greciyi-78913 (Accessed: 16 January 2023).

[115] Government portal (2022) 'Ukraine and Moldova agreed to cooperate in air defense and improve border control'. Government Portal of Ukraine. Available at: https://www.kmu.gov.ua/en/news/ukraina-ta-moldova-domovylysia-spivpratsiuvaty-v-pytanniakh-ppo-ta-pokrashchyty-prykordonnyi-kontrol-denys-shmyhal (Accessed: 19 January 2023).

[116] AP News (2022) 'NATO announces next leaders' summit will be in Lithuania'. Associated Press. Available at: https://apnews.com/article/putin-biden-nato-vilnius-lithuania-192552c306ac6b3c9ecb204539d92c68 (Accessed: 14 November 2022).

[117] Singh, K. (2022) 'U.S. announces additional $1.85 billion military aid for Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/us-announces-185-billion-additional-military-assistance-ukraine-2022-12-21/ (Accessed: 9 January 2023).

[118] Reuters (2022) 'Bulgaria to send its first military aid to Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/bulgaria-send-its-first-military-aid-ukraine-2022-12-09/ (Accessed: 9 December 2022).

[119] Vanttinen, P. (2022) 'Finland sends 11th military aid package to Ukraine'. Euractive. Available at: https://www.euractiv.com/section/politics/news/finland-sends-11th-military-aid-package-to-ukraine/ (Accessed: 18 January 2023).

[120] Ukrainian World Congress (2022) 'Slovakia approves a new package of military aid to Ukraine'. Ukrainian World Congress. Available at: https://www.ukrainianworldcongress.org/slovakia-approves-a-new-package-of-military-aid-to-ukraine/ (Accessed: 18 January 2023).

[121] Zimonjic, P. (2022) 'Canada announces additional $500M in military aid to Ukraine, adds 23 names to sanctions list'. CBC. Available at: https://www.cbc.ca/news/politics/canada-announces-military-aid-ukraine-1.6650616 (Accessed: 18 January 2023).

[122] Forsvarsministeriet (2022) 'Danmark donerer 300 mio. kr. til fond til indkøb af våben til Ukraine'. Forsvarsministeriet. Available at: https://www.fmn.dk/da/nyheder/2022/danmark-donerer-300-mio.-kr.-til-fond-til-indkob-af-vaben-til-ukraine/ (Accessed: 18 January 2023).

[123] Government of the Netherlands (2022) 'Netherlands earmarks €2.5 billion for support to Ukraine in 2023'. Government of the Netherlands. Available at: https://www.government.nl/latest/news/2022/12/23/netherlands-support-ukraine-2023-news (Accessed: 9 January 2023).

[124] Ministry of Foreign Affairs of Japan (2022) 'Emergency Grant Aid for winterization assistance in Ukraine'. Ministry of Foreign Affairs of Japan. Available at: https://www.mofa.go.jp/press/release/press4e_003183.html (Accessed: 18 January 2023).

[125] Militarniy (2022) 'The Czech Republic announces further military support for Ukraine'. Militarniy. Available at: https://mil.in.ua/en/news/the-czech-republic-announces-further-military-support-for-ukraine/ (Accessed: 18 January 2023).