CyberPeace Institute

Quarterly Analysis Report
Q3 July to September 2022

Cyber Dimensions
of the Armed Conflict in Ukraine

TABLE OF CONTENTS

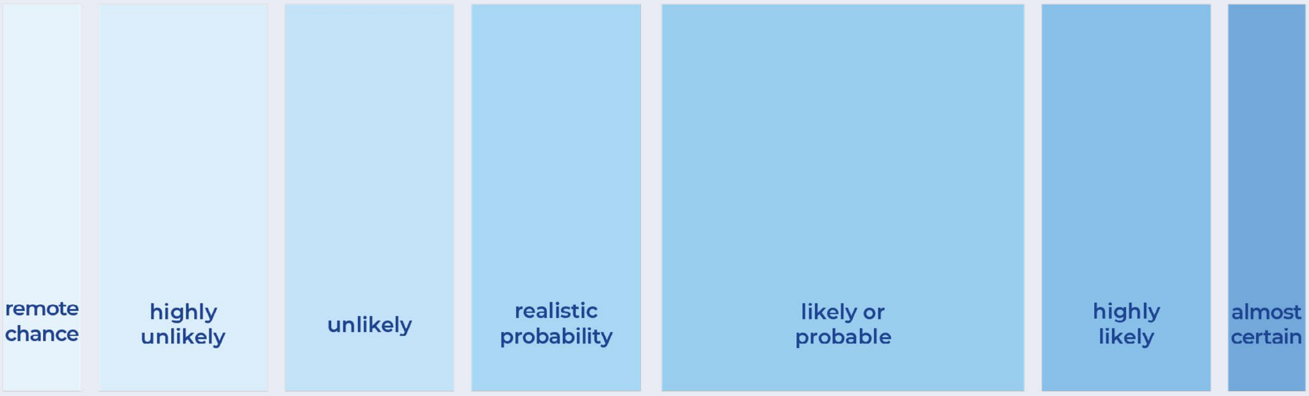
Report Methodology

This 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. As one campaign might target more than one sector, each attack in a campaign against each sector is processed separately.

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'.[4] 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 **178**[5] **cyber incidents against entities in Ukraine between January and September 2022**. With **87 incidents impacting 17 sectors in Q3**, there has been a **248% increase** in incidents compared to the previous quarter. This increase is driven by a significant increase in DDoS attacks targeting organizations in Ukraine.

Public Administration remains the most targeted sector in Q3. Compared to previous quarters, there was a notable increase in attacks against organizations in the Media, ICT, Energy and Transportation sectors.

Trends

DDoS attacks account for 71,3% of all incidents, followed by Malware (8%). Hacktivist collectives account for 80% of all incidents.

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

- Gamaredon, attributed to Russia's Federal Security Services[6] campaigns: GammaLoad.PS1[7] delivery, GammaLoad.PS1_v2[8] delivery and a campaign delivering information-stealing malware[9].
- Turla, attributed to Russia's Federal Security Services[10] campaign[11], using a well-known StopWar Android application, creating a fake "CyberAzov" DDoS application.
- Sandworm, attributed to Russia's foreign military intelligence[12] campaign[13], emulating a Ukrainian telecommunication provider, distributing malware.

Emerging Issues

New malware

Cisco Talos[14] discovered an uncommon piece of malware targeting a large software development company whose software is used in various state organizations within Ukraine. The malware was first observed in March 2022 and is reported to be a slightly modified version of the open-source backdoor named "GoMet".

Notable threat actor activity

CERT-UA discovered two campaigns targeting civilians, attributed to the threat actor identified as UAC-0100:

- a phishing campaign, impersonating[15] the Red Cross;
- Fraudulent Facebook pages distributing a website aiming to steal bank card details[16].

The increase in DDoS activities against Ukrainian entities is likely related to Russian media coverage of Russian hacktivist collectives[17]. Media interviews with the groups' leaders portray them as "defenders of Russia" and "patriots", likely causing increased awareness and participation in the groups' activities. Those collectives rely in part on the participation of the general population.

The moderator(s) of their social media channels announce the start of an attack, providing the victim's details, and subsequently report on whether the DDoS attack was successful.

One such group, the most active threat actor in Ukraine for Q3, is the Russian-affiliated "People's CyberArmy". The collective created its first social media account on March 2, 2022. Their Telegram description includes instructions on how the general population can participate in the group's activities. The hacktivist collective predominantly conducts DDoS attacks and have conducted attacks against organizations in 13 sectors, with a focus on Public Administration and Media.

There is a realistic possibility that "People's CyberArmy"[18] is affiliated with KillNet, as KillNet published a recruitment advertisement for a "Russian Cyber Army" three days after "People's CyberArmy" created their first Telegram channel. Additionally, the founder of KillNet, KillMilk, is referred[19] to as the creator of Russia's CyberArmy. The CyberPeace Institute first documented an incident attributed to the "People's CyberArmy" on July 23; however, it is almost certain that the group was actively targeting entities before that.

Notable incidents in Ukraine

Disinformation & Propaganda

July 21, 2022

The confirmed defacement of a Ukrainian radio channel. The perpetrators played a voice saying that the Ukrainian President is in intensive care, and falsely claiming the Chairman of the Verkhovna Rada will undertake the President's duties.

Data

July 25, 2022

An alleged cyberattack against one of Ukraine's largest internet providers, with an alleged impact of stealing more than 300GB of compressed information, "setting up the stage" for a subsequent event, and defacing more than 100 websites, including governmental ones.

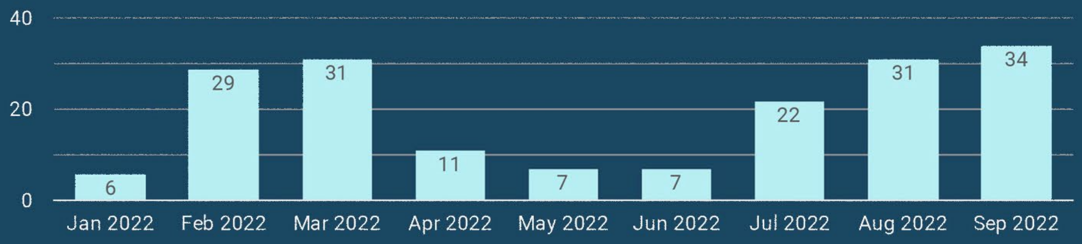
August 19, 2022

An alleged hack and leak operation against a Ukrainian administrative center with a potential impact from the leaked data containing 342,294 lines of information, including names and unique phone numbers of Ukrainian citizens (the leaked file contains 227,220 unique phone numbers).

Facts & Figures

Ukraine

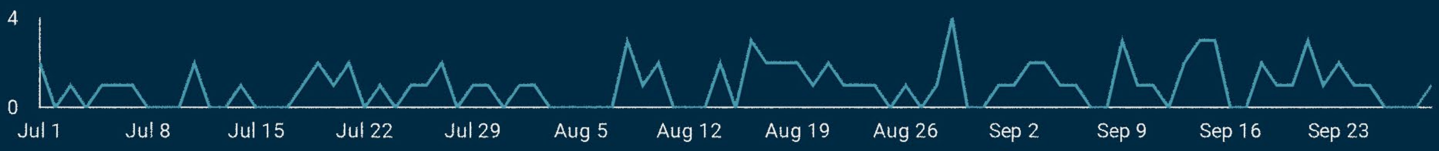
CyberPeace Institute



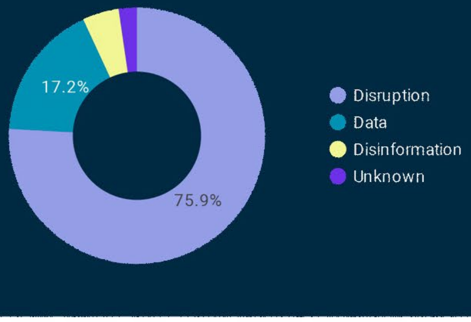
Incidents Jan-Sep 2022
178

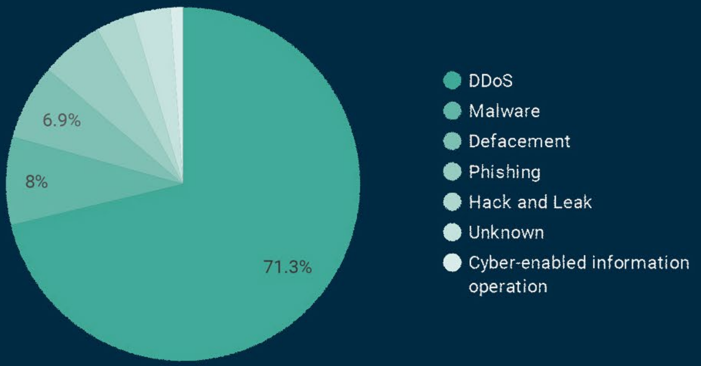
Sectors Jan-Sep 2022
20

Q3 July - September 2022

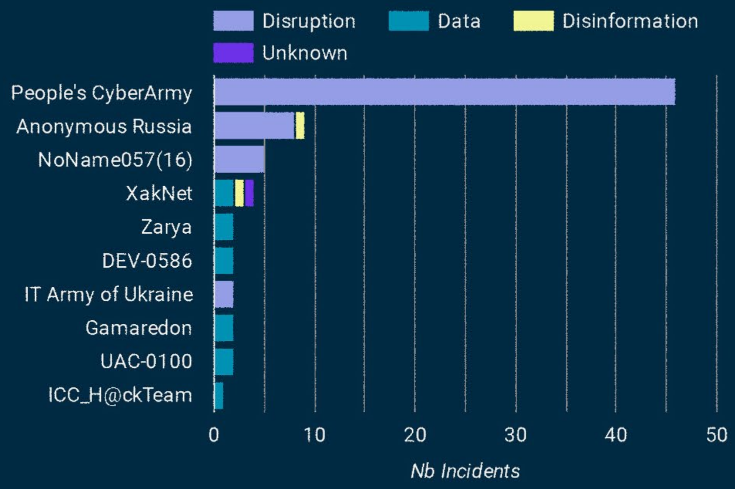


Nb Incidents	Sectors	Threat Actors
87	17	17
⬆ 248.0%	⬆ 142.9%	⬆ 112.5%





	Sector	Nb Incidents	% Δ
1.	Public administration	23	283.3% ⬆
2.	Media	14	250.0% ⬆
3.	ICT	6	100.0% ⬆
4.	Financial	6	-
5.	Civilians	5	0.0%
6.	Manufacturing	5	-
7.	Energy	4	100.0% ⬆
8.	Unknown	4	33.3% ⬆
9.	Transportation	4	100.0% ⬆
10.	Trade	4	-
11.	Other service	3	-
12.	Administrative / Supp...	3	-
13.	Arts	2	-
14.	Nonprofit	1	-
15.	Accommodation	1	-
16.	Education	1	-
17.	Construction	1	-



TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Trends and Emerging Issues

Russian Federation

The CyberPeace Institute documented **152 cyber incidents against entities in the Russian Federation between January and September 2022**. With **48 incidents impacting 12 sectors in Q3**, there has been a **27,3% decrease** in incidents compared to the previous quarter.

Trends

While the Public Administration of Russia was the most targeted sector in the previous quarters, there was a 72.7% decrease in attacks against this sector, which was replaced by attacks against the Media in Q3.

The Financial sector remains the second most attacked Russian sector since the February 2022 invasion, despite a 20% decrease in incidents compared to Q2.

Cyberattacks against Russia's Energy sector have also fallen by 83.3% compared to the previous quarter.

A 93% decrease in activity compared to Q2 of the hacking collective Anonymous and its affiliates.

Hacktivist collectives account for 34% of all incidents against entities in the Russian Federation.

Emerging Issues

Notable threat actor activity

The most active threat actors targeting Russian entities were the IT Army of Ukraine[20] and Haydamaki, with 24 and 9 incidents, respectively.

The IT Army of Ukraine[21] (IT Army henceforth) was officially established on February 26, 2022 following a declaration of Mykhailo Fedorov, Ukraine's Deputy PM and Minister of Digital Transformation. A journalist from a reputable Dutch media interviewed[22] an alleged current member of the IT Army who indicated that the Security Services of Ukraine (SBU) is entirely in charge of the IT Army. For their DDoS activities, the IT Army has two DDoS crowdsourcing projects (see Cumulative harm and impact).

Haydamaki is a Ukrainian hacktivist collective that was quite active during Q3 (9 incidents). They specialized in DDoS - they would release the information of a target and call all volunteers to act. Their activities gradually decreased by the end of Q3, and they have been inactive since October 22, 2022.

Persistently targeted since the February 2022 invasion, disruptive attacks against the Financial sector likely aim to put additional pressure on the sector that is heavily sanctioned on an international level. The decrease in attacks against Russian entities correlates with a decrease in activity of the hacktivist collective Anonymous and its affiliates; no information is currently available to explain this decrease in activity.

Furthermore, the reduced activity of Anonymous is linked to a decrease in hack and leak operations against Russian organizations. While 52% of the incidents in Q2 were hack and leak operations, and 18% were DDoS attacks, in Q3, the former types of incidents account for only 12.5%, while the latter account for 79.2% of all incidents.

Notable incidents in Russian Federation

Disruption

July 11, 2022

An alleged DDoS campaign against online ticket services of 80 cinemas, disrupting operability and preventing citizens from buying tickets for an unknown period.

September 1, 2022

An alleged cyberattack against one of Russia's largest taxi companies caused an alleged massive traffic jam in Moscow.

September 6, 2022

An alleged DDoS attack against a Russian private bank, allegedly disabled the online services of the organization for at least four hours.

Disinformation and Propaganda

August 24, 2022

The IT Army conducted[23] a confirmed cyberattack and defacement operation against a Russian Internet provider in Crimea. The defacement operation left a message[24] on the target organization's website, which congratulated the citizens of Crimea for the Independence Day of Ukraine. According to the victim organization[25], the cyberattack lasted for two hours.

Data

July 4, 2022

The confirmed hack and leak operation against a Russian public transport ticket retailer; impact includes the leak of 2,627,166 lines of data including first and last names, telephone numbers (2.29 million unique numbers) and email addresses (more than 2 million unique addresses).

July 29, 2022

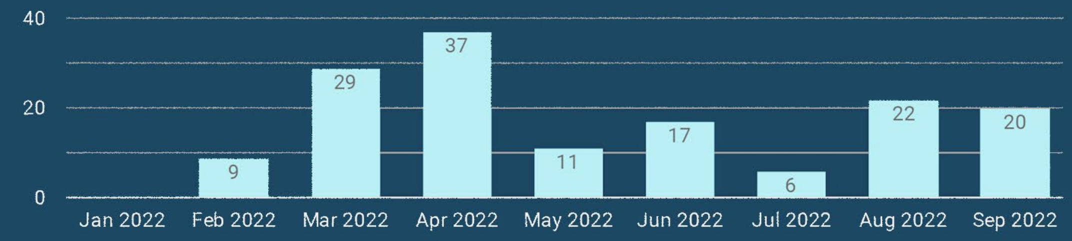
The confirmed hack and leak operation against Russian national postal services; the impact included the leak of over 10 million lines of information, including tracking numbers, full names and postal codes of senders/recipients, recipient's phone numbers, weights/status of shipments, date/time of departures, additionally according to the victim organization an unnamed contractor was compromised as a result of the cyberattack.

August 28, 2022

The confirmed hack and leak operation against a Russian streaming platform; impact includes the leak of 72 GB of data on 44 million customers from 2021, including names, email addresses, hashed passwords, first and last entry to the system, and country of origin (24.6 million from Russia, 2.3 million from Kazakhstan, 2.1 million from China and 1.7 million from Ukraine).

Facts & Figures

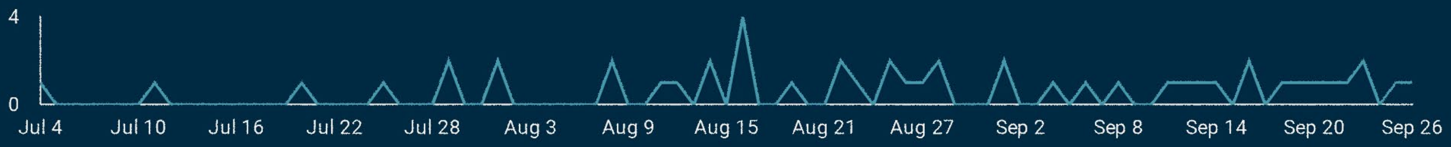
Russian Federation



Incidents Jan-Sep 2022
151

Sectors Jan-Sep 2022
19

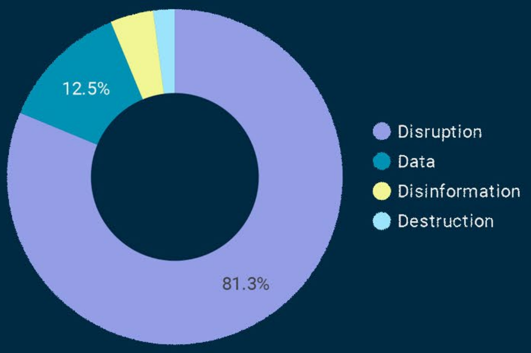
Q3 July - September 2022

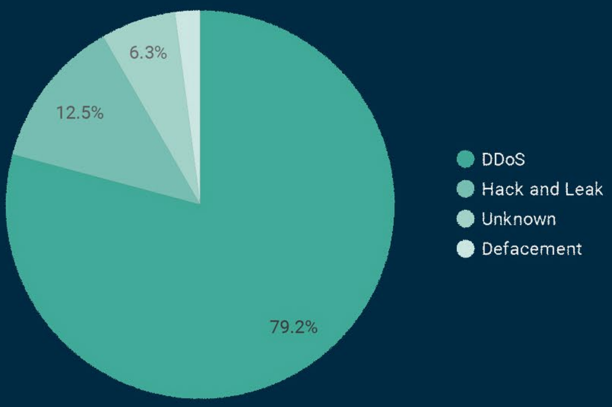


Nb Incidents
48
↓ -26.2%

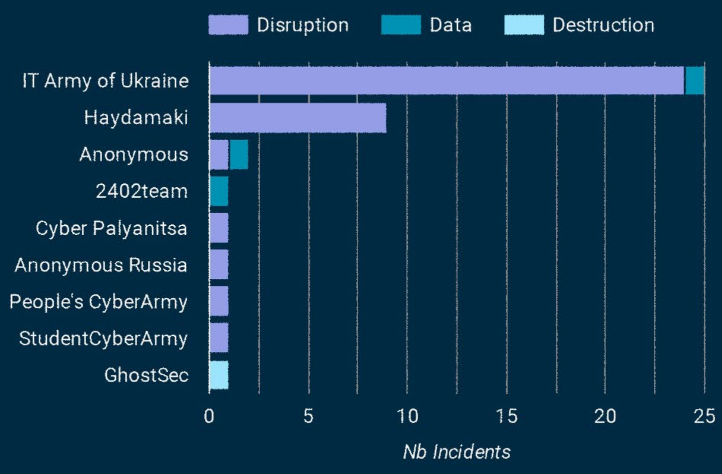
Sectors
12
↓ -20.0%

Threat Actors
10
0.0%





	Sector	Nb Incidents ▾	% Δ
1.	Media	11	450.0% ↑
2.	Financial	8	-20.0% ↓
3.	Administrative / S...	6	500.0% ↑
4.	ICT	5	0.0%
5.	Transportation	4	300.0% ↑
6.	Public administra...	3	-72.7% ↓
7.	Other service	3	200.0% ↑
8.	Trade	3	200.0% ↑
9.	Manufacturing	2	-66.7% ↓
10.	Energy	1	-83.3% ↓
11.	Accommodation	1	-
12.	Civilians	1	-



TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Trends and Emerging Issues

Other Countries

The CyberPeace Institute documented **225 cyber incidents against entities in nation-states that are not the two belligerent states** between January and September 2022. With **141 incidents impacting 19 sectors in Q3**, there has been a **177% increase in attacks** against states outside the two belligerent states compared to the previous quarter.

Trends

DDoS attacks account for 91% of all incidents.

There has been a 220% increase in attacks against the Transportation sector.

There has been a decrease in the activities of the most active threat actors by the end of Q3 (such as KillNet and NoName057(16)).

Hacktivist collectives account for 85% of all incidents.

Anonymous Russia and 13 other hacktivist collectives joined KillNet during Q3.

Emerging Issues

New malware

STIFF#BIZON, a new Konni-based malware.[26] Konni malware is classified as a remote access trojan (RAT), which has been previously attributed to the North Korean APT37. The campaign with the new malware targeted high-value targets in several countries and was attributed to Fancy Bear, attributed to Russia's foreign military intelligence[27]. This quarter saw the release of DDoS-crowdsourcing projects (see Cumulative harm and impact).

Notable threat actor activity

The most active threat actor was the Russian-affiliated collective NoName057(16), accounting for 46% of all attributed incidents, and almost all attacks against the Transportation sector. The group was formed in early March 2022 and specializes in DDoS attacks. In August, the group released its DDoS-crowdsourcing project.[28] Through an invite-only group, the group distributes a software that turns a member's device into a bot, which is used for DDoS attacks. There is a financial incentive for the most active members.

At the beginning of September, Avast published[29] a report connecting the Bobik malware - a Remote Access Trojan that has been around since 2020 - to NoName057(16). Devices infected with Bobik are now part of NoName057(16)'s botnet, servicing their DDoS activities.

While Public Administration was the most targeted sector in Q1 and Q2, the Transportation sector was targeted the most in Q3, with an increase of 220% compared to Q2. Nevertheless, Public Administration remains a high-priority target for threat actors conducting cyberattacks against entities in countries outside the two belligerent states. The Financial sector saw a 380% increase in cyberattacks in Q3 compared to Q2.

Entities in Latvia, Poland, and Lithuania were the most attacked in Q3, which marks a change of targets for Russian-affiliated threat actors compared to Q2, when German and Italian entities were targeted the most after Latvian organizations.

DDoS attacks account for 91% of all incidents, which continues the trend set in Q2 when DDoS attacks accounted for 82% of all incidents. Half of the incidents against the Transportation sector targeted Lithuanian organizations in the period between Lithuania's[30] ban on the transit of some goods through its territory from Russia to its exclave of Kaliningrad on June 18, 2022 and Lithuania's lifting of the said restrictions[31] on July 23, 2022.

Organizations in Estonia also suffered major cyberattacks in Q3. A week after the Prime Minister of Estonia called for a ban[32] on issuing visas to Russian citizens, the country was targeted by what was reported by the Government as the most powerful DDoS campaign since 2007[33].

There was a 32% decrease in the activities of most Russian-affiliated collectives in September, compared to the previous two months. NoName057(16) confirmed that the collective's capacities have grown and are preparing more complex actions.

The decline of activities, and reference to the preparation of more complex attacks, further aligned with the official Ukrainian statement[34] that the Russian Federation is preparing complex cyberattacks on Ukrainian critical infrastructure, and on Ukraine's neighbors, mainly the Baltic states and Poland.

At the end of the quarter, KillNet[35] announced that 14 collectives had joined the KillNet collective, including Anonymous Russia, suggesting a probable intensification of cyber activities.

Notable incidents

July 26, 2022

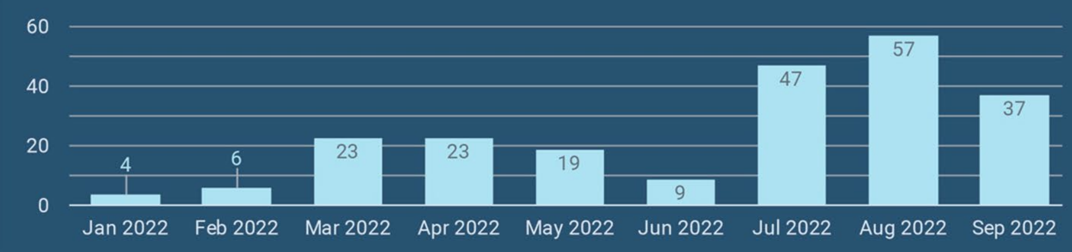
An alleged cyberattack against a Belarusian electrical control system impacted the operability of the hot water supply in several neighborhoods of Minsk. The alleged impact includes the disruption of hot water supplies to 13 kindergartens, 130 residential buildings, three medical and preventive institutions, 25 public and administrative buildings, and eight schools on the street.

August 17, 2022

The most extensive DDoS campaign against Estonia since 2007 was confirmed by Estonia's Government Chief Information Officer[36]; according to them the campaign had little impact and went by unnoticeable to the general public. KillNet claimed responsibility for the campaign, which targeted entities in both the public and private sectors.

Facts & Figures

Other Countries



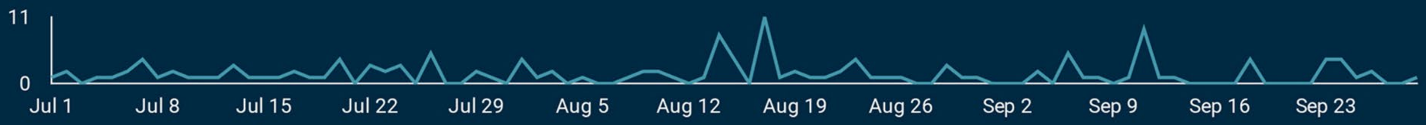
Incidents Jan - Sep 2022

225

Sectors Jan - Sep 2022

21

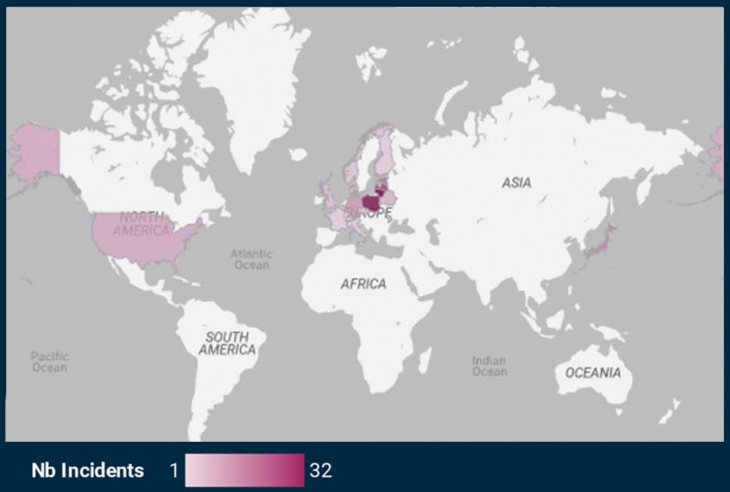
Q3 July - September 2022

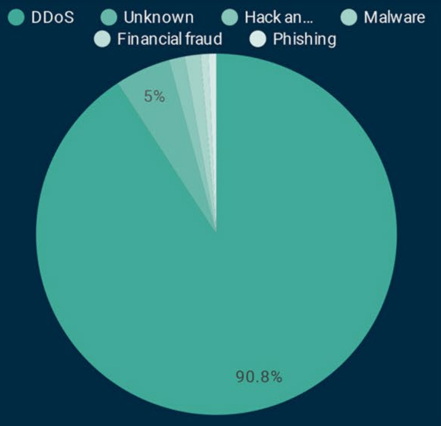


Nb Incidents

141

↑ 176.5%





Sectors

19

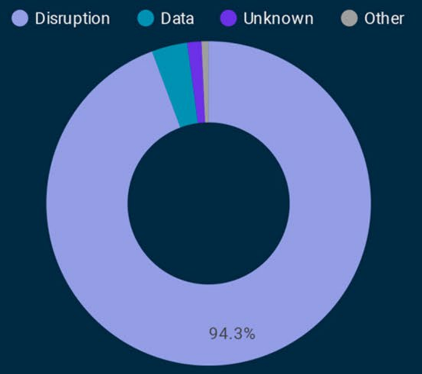
↑ 90.0%

Threat Actors

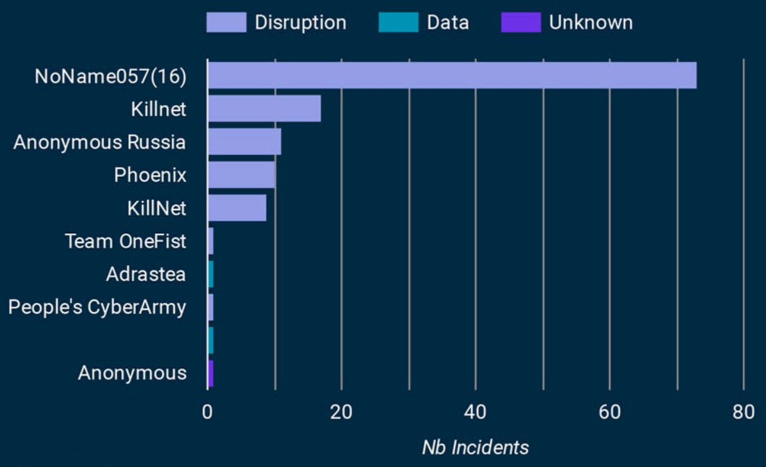
12

↑ 9.1%

	Country	Nb Incidents ▾	% Δ
1.	LT	30	2,900.0% ↑
2.	PL	26	2,500.0% ↑
3.	LV	15	114.3% ↑
4.	EE	13	1,200.0% ↑
5.	JP	12	-



	Sector	Nb Incidents ▾	% Δ
1.	Transportation	32	220.0% ↑
2.	Public administration	28	75.0% ↑
3.	Financial	24	380.0% ↑
4.	ICT	8	300.0% ↑
5.	Administrative / Support	7	-
6.	Media	6	0.0%
7.	Manufacturing	6	500.0% ↑
8.	Other service	6	-
9.	Energy	5	66.7% ↑
10.	Nonprofit	4	33.3% ↑



TLP:WHITE

Disclosure is not limited.

TLP:WHITE information may be distributed freely.

Harm and Impact on Civilians and People

As previously noted, most incidents processed by the CyberPeace Institute for Q3 were DDoS attacks. While DDoS attacks could pose a significant risk to organizations, including financial losses, reputational damage, and operational disruption[37], they often have a limited impact, as long as organizations have taken precautionary measures. The measures include implementing DDoS protection mechanisms or temporarily geo-blocking malicious traffic using IP geolocation software.

The latter consists of the rejection of traffic originating from locations with a history of launching DDoS attacks and was seen by the CyberPeace Institute to be used by several targeted organizations in the Baltic states. Therefore, the most common impact observed to date of DDoS attacks is a temporary connectivity disruption to specific websites. Temporary inaccessibility to the services of certain organizations can impact the everyday life of the general population.

The impact of DDoS attacks also has a psychological dimension. On the one hand, the DDoS activities of hacktivist collectives are often reported by the media, especially in the Russian Federation. The Russian news media often portrays the DDoS activities of such collectives as the duty of Russian patriots protecting the information space against Western aggression.[38] On the other hand, civilians and citizens from targeted countries could have a decreased sense of security and trust in institutions when the media reports DDoS attacks on certain services, such as the Public Administration.

DDoS Crowdsourcing

The CyberPeace Institute also identified a trend of crowdsourcing DDoS attacks. Several threat actors have created software to crowdsource their DDoS activities amongst a broader public, functionally involving the general population in attacks and campaigns. The IT Army has released two software - disBalancer and Liberator[39]. The former is a crowdsourcing DDoS protection software, while the latter is similar software, albeit offensive. The IT Army has also created scripts, such as db1000n (death by 1000 needles).

The script automatically runs on an IT Army member's device, connecting to the Command & Control center of the IT Army. Members do not need to enter target details manually, as the script automates targeting and attacking. Russian-affiliated threat actors, notably NoName057(16)[40] and Anonymous Russia, have also released their DDoS crowdsourcing projects.

Hack and Leak Operations

Hack and leak operations are types of attacks that could pose a significant risk to the general population. The CyberPeace Institute notes a decrease in hack and leak operations in Q3 compared to Q2. Nevertheless, the documented hack and leak operations have usually impacted thousands of people, to whom they pose a multitude of risks. Leaked personal information, including email addresses, phone numbers, and credit card details, could further victimize people by exposing them to subsequent phishing campaigns, financial fraud, and cyberbullying[41].

Wider Contextual Considerations

Other research

A Cloudflare[42] report on their findings for Q3 also discovered an increase in DDoS attacks compared to last year. However, their findings differ to a certain extent from the findings of the CyberPeace Institute. According to Cloudflare, the most targeted sector with DDoS attacks in Ukraine was the Professional, followed by Education and Public Administration sectors. In Russia, the most targeted industry was Financial, Media, and Trade.

The perpetrators of most of the DDoS attacks in Q3 were hacktivist collectives. Two publications provide insight into the changing hacktivist ecosystem in the context of the conflict in Ukraine:

1. De Volkskrant, a Dutch newspaper published an interview[43] with a Dutch veteran, now a member of the IT Army of Ukraine. The interview reveals insights into Ukraine's cyber army's organizational structure, targeting, and modus operandi.
2. Checkpoint[44] published a research paper on the hacktivist ecosystem developments throughout the conflict. The research focuses mainly on Russian-affiliated threat actors, with a case study on KillNet.

Lastly, Meta[45] published a quarterly report on the actors spreading disinformation on their platforms.

Events

Several geopolitical events increased the tensions between the belligerents and between belligerent and non-belligerent states.

In July 2022, the United States emphasized its cybersecurity support for Ukraine. On July 19, the FBI Director met[46] with Ukrainian law enforcement and cybersecurity leaders in New York to discuss the Russian Federation's ongoing cyber operations and campaigns against Ukraine. On July 27, a Memorandum of Cooperation[47] was signed between the US Cybersecurity and Infrastructure Security Agency (CISA) and the Ukrainian State Service of Special Communications and Information Protection of Ukraine (SSSCIP). At the beginning of September, the SSSCIP and the Cyberspace Defense Forces of Poland signed a Memorandum of Understanding[48].

Economic sanctions, military aid, and public statements

The primary rationale of Russian-affiliated state actors for targeting non-belligerent states is that they either provide military aid to Ukraine or are thought to demonstrate hostility towards the Russian Federation through economic sanctions or parliamentary declarations.

The following list of countries that provided military aid to Ukraine and implemented sanctions against the Russian Federation is non-exhaustive. Nevertheless, it gives an overview of the trends in international relations surrounding the conflict and how they may impact stability in cyberspace.

Military aid

Western countries pledged[49] more than US $1.5 billion to boost Ukrainian military capabilities at the beginning of August whilst the European Union, through the European Peace Facility[50], increased military aid to Ukraine to 2.5 billion euros. Several individual states also sent military aid to Ukraine in Q3. Bulgaria allegedly sent[51] 4,200 tons[52] of weapons through Romania and Poland to Ukraine.

Other states that reportedly sent military aid to Ukraine were: Croatia[53], Czech Republic[54], Germany[55], Finland[56], France[57], Lithuania[58], Poland[59], Slovakia[60], Sweden[61], the United States of America[62], and the United Kingdom[63].

The CyberPeace Institute has identified incidents targeting entities in all aforementioned nation-states with the exception of Sweden.

Sanctions and statements

Along with common EU sanctions several member states announced individual sanctions including:

- Lithuania's[64] ban on the rail transport of goods from Russia to Kaliningrad;
- Estonia[65] announced a ban on the purchase of natural gas and liquefied gas;
- Poland[66] imposed sanctions on Gazprom Export.

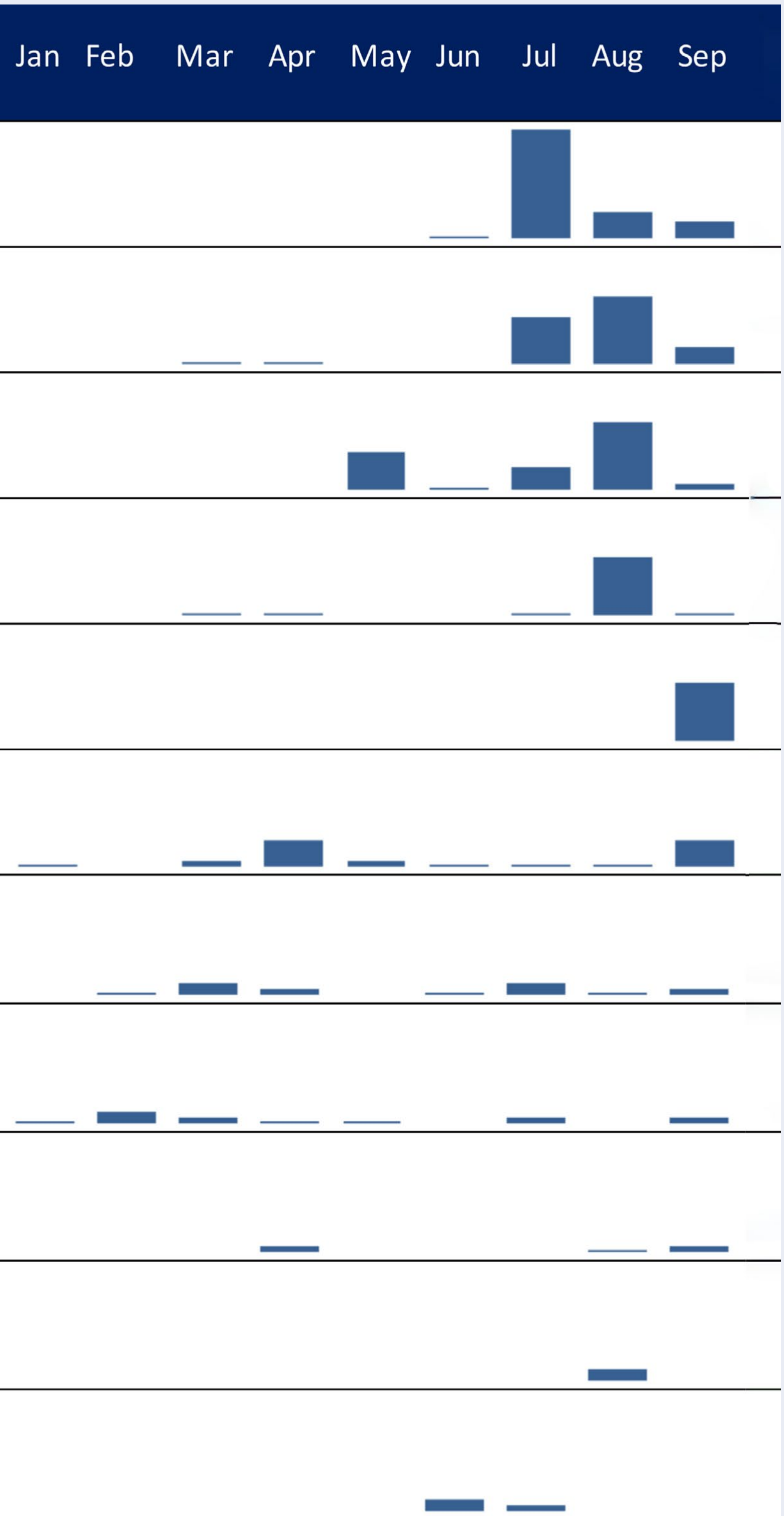
Russian-affiliated threat actors are highly likely to have deemed the imposition of sanctions and other declarations as a threat towards the Russian Federation further fuelling activity in cyberspace against Ukrainian allies. Several statements in Q3 2022 illustrate this:

- Latvia's Saeima, the parliament of the Republic of Latvia, adopted a statement[67] declaring Russia a state sponsor of terrorism;
- The UN Independent International Commission of Inquiry on Ukraine announced[68] that war crimes had been committed in Ukraine;
- Estonia's[69] Prime Minister calls for a ban on issuing visas to citizens of the Russian Federation.

Cyber incidents in other countries combined with dates of recent key events

An illustration of how announcements relating to sanctions, military aid and geopolitical positioning are likely to trigger a response in cyberspace.

Country	Recent notable sanctions, military aid & statements	Nb Incidents Q3
Lithuania	2022-06-18 Sanctions 2022-07-05 Military 2022-07-10 Sanctions 2022-09-07 Military	32
Poland	2022-06-07 Military 2022-07-25 Military 2022-08-22 Military 2022-09-29 Sanctions	28
Latvia	2022-07-28 Military 2022-08-11 Statement	21
Estonia	2022-06-03 Statement 2022-09-29 Sanctions 2022-09-09 Statement	14
Japan	2022.08.04 Military	12
Germany	2022-07-13,15,19 Military 2022-08-02,10,19 Military 2022-09-07 Military	8
United States	2022-07-22 Military 2022-08-01,08,19,24 Military 2022-09-08,15,28 Military	6
Belarus	2022-06-25 Statement 2022-06-27 Military	4
United Kingdom	2022-07-21 Military 2022-08-11,24,27 Military	3
Denmark	2022-07-13,15,19 Military 2022-08-02,10,19 Military 2022-09-07 Military	3
Norway	2022-06-29 Military	2



References

[1] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: - cyberconflicts.cyberpeaceinstitute.org (Accessed: 15 December 2022)

[2] Ibid.

[3] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 15 December 2022).

[4] 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)

[5] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 15 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). 'Kiberataky hrupy UAC-0010 (Armageddon): shkidlyvi prohramy GammaLoad, GammaSteel (CERT-UA#5134)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/1229152 (Accessed: 12 August 2022).

[8] CERT-UA. (2022). 'Kiberataky hrupy UAC-0010 (Armageddon) z vykorystannyam shkidlyvoyi prohramy GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071)'. Computer Emergency Response Team of Ukraine. Available at:https://cert.gov.ua/article/971405 (Accessed: 29 July 2022).

[9] Malhotra, A. and Venere, G. (2022). 'Gamaredon APT targets Ukrainian government agencies in new campaign., Cisco Talos. Available at: https://blog.talosintelligence.com/gamaredon-apt-targets-ukrainian-agencies/ (Accessed: 19 September 2022).

[10] EFIS. (2018) 'International Security and Estonia'. Estonia Foreign Intelligence Service. Available at: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf (Accessed: 21 April 2021)

[11] Leonard, B. (2022) 'Continued cyber activity in Eastern Europe observed by TAG'. Google's Threat Analysis Group. Available at: https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/ (Accessed: 2 August 2022).

[12] 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).

[13] Insikt Group (2022) 'Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine'. RecordedFuture. Available at: https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine (Accessed: 22 September 2022).

[14] Shultz, J. (2022) 'Attackers target Ukraine using GoMet backdoor'. Cisco Talos. Available at: https://blog.talosintelligence.com/attackers-target-ukraine-using-gomet/ (Accessed: 2 August 2022).

[15] CERT-UA. (2022). 'Onlajn-shaxrajstvo z vykorystannyam tematyky "dopomohy vid Chervonoho Xresta" (CERT-UA#5063)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/987552 (Accessed: 29 July 2022).

[16] CERT-UA. (2022. ‘Onlajn-shaxrajstvo z vykorystannyam tematyky "hroshovoyi kompensaciyi" (CERT-UA#4964)’. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/761668 (Accessed: 29 July 2022).

[17] Kil’djushkin, R. (2022) ‘V Rossii ja stanu geroem, a za rubezhom – prestupnikom». Interv'ju s osnovatelem gruppirovki Killnet’, Gazeta, 7 August. Available at: https://www.gazeta.ru/tech/2022/08/07/15229652.shtml?updated (Accessed: 12 August 2022). Kommersant (2022) ‘Haker iz gruppirovki RaHDit rasskazal o peredache «kuda nuzhno» dannyh sotrudnichajushhih s razvedkoj Ukrainy rossijan’, Kommersant, 18 July. Available at: https://www.kommersant.ru/doc/5469098 (Accessed: 27 July 2022). Riafan (2022) ‘Killnet: kak rossijskie hakery ob"javili vojnu Zapadu’, Riafan, 2 July. Available at: https://riafan.ru/23516587-killnet_kak_rossiiskie_hakeri_ob_yavili_voinu_zapadu (Accessed: 20 July 2022).

[18] KillNet_Reservs (2022) [Telegram] 5 March. Available at: https://t.me/killnet_reservs/81 (Accessed:11 August 2022).

[19] KillNet_Reservs (2022) [Telegram] 27 July. Available at: https://t.me/killnet_reservs/2206 (Accessed: 27 July 2022).

[20] Soesanto, S. (2022) ‘The IT Army of Ukraine Structure, Tasking, and Ecosystem’. Center for Security Studies (CSS), ETH Zürich. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf (Accessed: 28 July 2022).

[21] Ibid.

[22] Modderkolk, H. (2022) ‘Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol’. deVolkskrant. Available at: https://www.volkskrant.nl/kijkverder/v/2022/een-internationaal-cyberleger-tegen-rusland-met-een-nederlander-in-de-hoofdrol~v580287/?referrer=https%3A%2F%2Fwww.google.com%2F (Accessed: 24 September 2022)

[23] Kunder, N. (2022) ‘IT Army of Ukraine claims to have destroyed Russian Miranda-media!’. TheTechOutlook. Available at: https://www.thetechoutlook.com/news/technology/security/it-army-of-ukraine-claims-to-have-destroyed-russian-miranda-media/ (Accessed: 1 September 2022).

[24] Timoshhenko, A. (2022) ‘Hakery vzlomali sajt internet-provajdera i pozdravili krymchan s Dnem nezavisimosti Ukrainy’, Komsomol'skaja pravda, 25 August. Available at: https://www.crimea.kp.ru/daily/27436/4637757/?ysclid=l7g1j39ooh68975679 (Accessed: 1 September 2022).

[25] Miranda-Media (2022) ‘Na sajt «Miranda-media» sovershena hakerskaja ataka’. Available at: https://www.miranda-media.ru/about/news/na_sait_miranda_media_sovershena_hakerskaya_ataka_?ysclid=l7g1hbm0x8930683714 (Accessed: 1 September 2022).

[26] Iuzvyk, D., Peck, T., and Kolesnikov, O. (2022). ‘Securonix Threat Labs Initial Coverage Advisory: STIFF#BIZON Detection Using Securonix - New Attack Campaign Observed Possibly Linked to Konni/APT3, Securonix Threat Labs. Available at: https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/ (Accessed: 22 July 2022).

[27] Crowdstrike. (2019). ‘Who is FANCY BEAR (APT28)?’, Crowdstrike Research &Threat Intel. Available at: https://www.crowdstrike.com/blog/who-is-fancy-bear/ (Accessed: 2 December 2022).

[28] Radware. (2022). 'Project DDOSIA Russia's answer to disBalancer', Radware. Available at: https://www.radware.com/security/threat-advisories-and-attack-reports/project-ddosia-russias-answer-to-disbalancer/ (Accessed: 17 October 2022).

[29] Chlumecky. (2022). 'Pro-Russian Group Targeting Ukraine Supporters with DDoS Attacks', Avast Threat Intelligence Team. Available at: https://decoded.avast.io/martinchlumecky/bobik/ (Accessed: 17 October 2022).

[30] Euronews. (2022). 'Anger as Lithuania bans transit of goods to Russia exclave Kaliningrad', Euronews, 20 June. Available at: https://www.euronews.com/2022/06/20/anger-as-lithuania-bans-transit-of-goods-to-russia-exclave-kaliningrad (Accessed: 1 December 2022).

[31] BBC. (2022). 'Kaliningrad row: Lithuania lifts rail restrictions for Russian exclave', BBC, 23 July. Available at: https://www.bbc.com/news/world-europe-62274474 (Accessed 1 December 2022).

[32] Kallas, K. (2022) [Twitter] 9 August. Available at: https://twitter.com/kajakallas/status/1556903576726896642 (Accessed: 30 November 2022).

[33] Ilves, L. (2022) [LinkedIn] 9 August. Available at: https://twitter.com/kajakallas/status/1556903576726896642 (Accessed 10 August 2022).

[34] Vicens, A. (2022). 'Ukraine warns of 'massive cyberattacks' coming from Russia on critical infrastructure sites, Cyberscoop, 26 September. Available at: https://www.cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/ (Accessed 26 September 2022).

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

[36] Ilves, L. (2022) [LinkedIn] 9 August. Available at: https://twitter.com/kajakallas/status/1556903576726896642 (Accessed 10 August 2022).

[37] CISA (2022) 'Understanding and Responding to Distributed Denial-of-Service Attacks', Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf (Accessed 29 November 2022).

[38] Galeev, B.A. (2022) '«Ne nado bylo ugrozhat' moej strane» Hakery Killnet zashhishhajut Rossiju, srazhajas' s Anonymous i NATO. Kto za nimi stoit?', 15 April. Available at: https://lenta.ru/articles/2022/04/15/killnet/ (Accessed: 15 December 2022).

[39] Soesanto, S. (2022) 'The IT Army of Ukraine Structure, Tasking, and Ecosystem'. Center for Security Studies (CSS), ETH Zürich.. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf (Accessed: 28 July 2022).

[40] Radware. (2022). 'Project DDOSIA Russia's answer to disBalancer', Radware. Available at: https://www.radware.com/security/threat-advisories-and-attack-reports/project-ddosia-russias-answer-to-disbalancer/ (Accessed: 17 October 2022).

[41] For example, a website, developed by the Polish-affiliated Squad303 hacktivist collective, which allows its users to send messages/emails and call random citizens of the Russian Federation.

[42] Cloudflare. (2022). 'DDoS Attack Trends for 2022 Q3', Cloudflare. Available at: https://radar.cloudflare.com/reports/ddos-2022-q3 (Accessed 28 November 2022).

[43] Modderkolk, H. (2022) 'Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol'. deVolkskrant. Available at: https://www.volkskrant.nl/kijkverder/v/2022/een-internationaal-cyberleger-tegen-rusland-met-een-nederlander-in-de-hoofdrol~v580287 (Accessed: 24 September 2022).

[44] Checkpoint. (2022). 'The New Era of Hacktivism State-Mobilized Hacktivism Proliferates to the West and Beyond', CheckPoint Research. Available at: https://research.checkpoint.com/2022/the-new-era-of-hacktivism/ (Accessed 1 December 2022).

[45] Nimmo, B., Agranovich, D., Franklin, M., Dvilyanski, M., and Gleicher, N. (2022). 'Quarterly Adversarial Threat Report', Meta. Available at: https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf (Accessed 30 November 2022).

[46] FBI (2022) [Twitter] 19 July. Available at: https://twitter.com/FBI/status/1549499103201136643 (Accessed: 5 December 2022).

[47] CISA (2022) 'United States and Ukraine expand cooperation on cybersecurity', Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity (Accessed: 5 December 2022).

[48] SSSCIP. (2022). 'SSSCIP: Ukraine expands cooperation in cybersecurity with Poland', State Service of Special Communications and Information Protection, 1 September.
Available at: https://www.kmu.gov.ua/en/news/ukraina-pohlybliuie-spivpratsiu-z-polshcheiu-u-sferi-kiberbezpeky (Accessed: 5 December 2022).

[49] Gronholt-Pedersen, J. (2022). 'Western countries pledge $1.55 bln in military aid to Ukraine', Reuters, 11 August. Available at: https://www.reuters.com/world/europe/denmark-will-contribute-additional-110-mln-euros-ukraine-pm-2022-08-11/ (Accessed: 6 December 2022).

[50] Council of the EU. (2022). 'European Peace Facility: EU support to Ukraine increased to €2.5 billion', Council of the European Union, 22 July. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/07/22/european-peace-facility-eu-support-to-ukraine-increased-to-2-5-billion/ (Accessed: 6 December 2022).

[51] Marchenko, N. (2022). 'Sofia secretly selling old weapons meant for Ukraine via Romania and Poland', Bivol, 19 July. Available at: https://bivol.bg/en/sofia-secretly-selling-old-weapons-meant-for-ukraine-via-romania-and-poland.html (Accessed 6 December 2022).

[52] European Pravda. (2022). 'Bulgaria Sent 4,200 Tons of Weapons to Ukraine - Secretly via Poland', European Pravda, 5 August. Available at: https://www.eurointegration.com.ua/eng/news/2022/08/5/7144530/ (Accessed 6 December 2022).

[53] Shephard. (2022). 'Croatia donates M-46 field guns to Ukraine', ShephardMedia, 15 August. Available at: https://www.shephardmedia.com/news/landwarfareintl/croatia-donates-m-46-field-guns-to-ukraine/ (Accessed: 6 December 2022).

[54] Shephard. (2022). 'Bohemian Brotherhood: List of Czech Weapons Deliveries To Ukraine', Shephard Media, 10 July. Available at: https://www.oryxspioenkop.com/2022/07/bohemian-brotherhood-list-of-czech.html (Accessed: 6 December 2022).

[55] Oryx. (2022). 'Fact Sheet on German Military Aid to Ukraine', Oryx, 1 September. Available at: https://www.oryxspioenkop.com/2022/09/fact-sheet-on-german-military-aid-to.html (Accessed: 6 December 2022).

[56] Oryx. (2022). 'Joining NATO, Joining the Cause: Finnish Aid to Ukraine', Oryx, 5 September. Available at: https://www.oryxspioenkop.com/2022/09/joining-nato-joining-cause-finnish-aid.html (Accessed: 6 December 2022).

[57] Oryx. (2022). 'Arms for Ukraine: French Weapons Deliveries to Kyiv', Oryx, 13 July. Available at: https://www.oryxspioenkop.com/2022/07/arms-for-ukraine-french-weapon.html(Accessed: 6 December 2022).

[58] Oryx. (2022). 'You've Got A Friend In Me - Lithuanian Weapons Deliveries To Ukraine', Oryx, 17 June. Available at: https://www.oryxspioenkop.com/2022/06/youve-got-friend-in-me-lithuanian.html (Accessed: 6 December 2022).

[59] Oryx. (2022). 'A European Powerhouse: Polish Military Aid To Ukraine', Oryx, 18 August. Available at: https://www.oryxspioenkop.com/2022/08/a-european-powerhouse-polish-military.html (Accessed: 6 December 2022).

[60] Oops Top Team. (2022). 'Slovakia will give Ukraine 30 BMP-1 in exchange for German weapons', Oops Top, 23 August. Available at: https://oopstop.com/slovakia-will-give-ukraine-30-bmp-1-in-exchange-for-german-weapons/ (Accessed: 6 December 2022).

[61] Preussen, W. (2022). 'Sweden to boost military aid to Ukraine', Politico, 29 August. Available at: https://www.politico.eu/article/sweden-boost-military-aid-ukraine-magdalena-andersson-dmytro-kuleba-kyiv/ (Accessed: 6 December 2022).

[62] U.S. Department of Defense. (2022). '$270 Million in Additional Security Assistance for Ukraine', U.S. Department of Defense, 22 July, Available at: https://www.defense.gov/News/Releases/Release/Article/3102984/270-million-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022). Haboush, J. (2022). 'More ammo for HIMARS in new $550 mln weapons package for Ukraine: Pentagon', AlarabiyaNews, 1 August. Available at: https://english.alarabiya.net/amp/News/world/2022/08/01/More-ammo-for-HIMARS-in-new-550-mln-weapons-package-for-Ukraine-Pentagon (Accessed: 6 December 2022); U.S. Department of Defense. (2022). '$1 Billion in Additional Security Assistance for Ukraine', U.S. Department of Defense, 8 August, Available at: https://www.defense.gov/News/Releases/Release/Article/3120059/1-billion-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022). U.S. Department of Defense. (2022). '$775 Million in Additional Security Assistance for Ukraine', U.S. Department of Defense, 19 August, Available at: https://www.defense.gov/News/Releases/Release/Article/3134457/775-million-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022). U.S. Department of Defense. (2022). '$675 Million in Additional Security Assistance for Ukraine', U.S. Department of Defense, 8 September, Available at: https://www.defense.gov/News/Releases/Release/Article/3152071/675-million-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022) U.S. Department of Defense. (2022). '$600 Million in Additional Security Assistance for Ukraine', U.S. Department of Defense, 15 September, Available at: https://www.defense.gov/News/Releases/Release/Article/3160503/600-million-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022) U.S. Department of Defense. (2022). '$1.1 Billion in Additional Security Assistance for Ukraine', U.S. Department of Defense, 28 September, Available at: https://www.defense.gov/News/Releases/Release/Article/3173378/11-billion-in-additional-security-assistance-for-ukraine/ (Accessed: 6 December 2022) Euractiv. (2022). 'US to give $3 billion in military aid as Ukraine marks 6 months of war', Euractiv, 24 August. Available at: https://www.euractiv.com/section/global-europe/news/us-to-give-3-billion-in-military-aid-as-ukraine-marks-6-months-of-war/ (Accessed: 6 December 2022)[59] Oryx. (2022). 'A European Powerhouse: Polish Military Aid To Ukraine', Oryx, 18 August. Available at: https://www.oryxspioenkop.com/2022/08/a-european-powerhouse-polish-military.html (Accessed: 6 December 2022).

[63] Somerville, E., Parekh, M., & Zagon, C. (2022). 'Kremlin set to 'run out of steam' giving Kyiv chance to strike, says MI6 chief', The Telegraph, 21 July. Available at: https://www.telegraph.co.uk/world-news/2022/07/21/russia-ukraine-vladimir-putin-war-latest-news-weapons-nukes/ (Accessed: 6 December 2022)
Shephard. (2022). 'UK to double M270 MLRS deliveries to Ukraine', ShephardMedia, 11 August. Available at: https://www.shephardmedia.com/news/landwarfareintl/uk-to-double-m270-mlrs-deliveries-to-ukraine/ (Accessed: 6 December 2022)
Government of the UK. (2022). 'Prime Minister tells Ukraine "they will win" as he marks Independence Day: 24 August 2022', Government of the United Kingdom, 24 August. Available at: https://www.gov.uk/government/news/prime-minister-tells-ukraine-they-will-win-as-he-marks-independence-day-24-august-2022 (Accessed: 6 December 2022)
Government of the UK. (2022). 'UK donating undersea minehunter drones to help Ukraine clear coastline', Government of the United Kingdom, 27 August. Available at: https://www.gov.uk/government/news/uk-donating-undersea-minehunter-drones-to-help-ukraine-clear-coastline (Accessed: 6 December 2022).

[64] ReilFreight. (2022). 'Lithuania imposes more traffic restrictions on Kaliningrad despite second thoughts', RailFreight, 11 July. Available at: https://www.railfreight.com/policy/2022/07/11/lithuania-imposes-more-traffic-restrictions-on-kaliningrad-despite-second-thoughts/?gdpr=accept (Accessed: 1 August 2022).

[65] Vabariigi Valitsus. (2022). 'Vabariigi Valitsuse sanktsiooni kehtestamine maagaasi ja veeldatud maagaasi ostu keeluks seoses Venemaa Föderatsiooni agressiooniga Ukrainas, mida toetab Valgevene Vabariik' Vabariigi Valitsus, 29 September. Available at: https://www.riigiteataja.ee/akt/101102022007 (Accessed: 3 October 2022).

[66] Reuters. (2022). 'Poland imposes sanctions on Russia's Gazprom Export, interior ministry says', Reuters, 29 September. Available at: https://www.reuters.com/business/energy/poland-imposes-sanctions-russias-gazprom-export-interior-ministry-says-2022-09-29/ (Accessed: 3 October 2022).

[67] Saeima. (2022). 'Saeima adopts statement declaring Russia a state sponsor of terrorism', the Saeima of the Republic of Latvia, 11 August. Available at: https://www.saeima.lv/en/news/saeima-news/31309-saeima-adopts-statement-declaring-russia-a-state-sponsor-of-terrorism?phrase=russia (Accessed: 5 December 2022).

[68] UN. (2022). 'War crimes have been committed in Ukraine conflict, top UN human rights inquiry reveals', The United Nations, 23 September. Available at: https://news.un.org/en/story/2022/09/1127691 (Accessed: 5 December 2022).

[69] Kallas, K. (2022) [Twitter] 9 August. Available at: https://twitter.com/kajakallas/status/1556903576726896642 (Accessed: 30 November 2022).