CyberPeace Institute

Quarterly Analysis Report
Q2 April to June 2023

Cyber Dimensions
of the Armed Conflict in Ukraine

TABLE OF CONTENTS

Background

January 2022 - June 2023

Since the start of the armed invasion of Ukraine in February 2022, the CyberPeace Institute has been documenting cyberattacks against critical infrastructure and civilian objects in Ukraine and the Russian Federation and cyberattacks against targets beyond the two belligerent countries. Between January 2022 and June 2023, the CyberPeace Institute has documented a total of 2189 cyber incidents conducted by 108 different threat actors. The data is available through the Cyber Attacks in Times of Conflict Platform[1] #Ukraine.

474 incidents against entities in **Ukraine**

The hacktivist collectives *People's CyberArmy* (168) and *NoName057*(16) (52) were the most active threat actors targeting Ukrainian entities, while *Sandworm* (19) and *APT28* (7) were attributed with the highest number of attacks among Russia's state-sponsored actors.

Top 5 targeted sectors:

- Public administration (113)
- Financial (53)
- Media (46)
- ICT (44)
- Transportation (27)

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

The most active threat actors conducting attacks against Russian entities were the *IT Army of Ukraine* (72), *Anonymous Italia* (59), and *Anonymous* (50).

Top 5 targeted sectors:

- Public administration (47)
- Financial (43)
- Media (30)
- ICT (29)
- Energy (23)

1425 incidents against entities in **other countries**

The most active threat actors were the hacktivist collectives *NoName057(16)* (780), *Anonymous Russia* (102), and *KillNet* (65).

Top 3 targeted sectors:

- Public administration (440)
- Transportation (259)
- Financial (132)

Top 3 targeted countries:

- Poland (238)
- Germany (113)
- Lithuania (111)

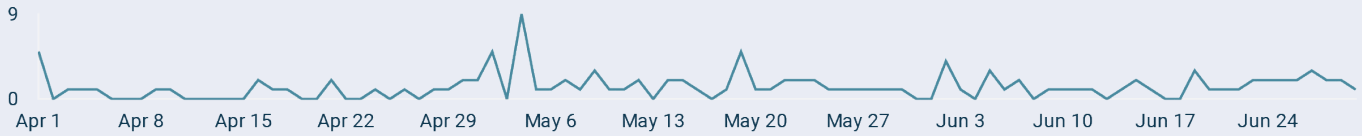
The remainder of this report focuses on the incidents documented by the CyberPeace Institute in the second quarter of 2023; April 1 until June 30, 2023. Notably during this period, the CyberPeace Institute identified the 100th threat actor operating within the conflict's context, based on our research since January 2022.

Trends and Emerging Issues Q2 2023

Ukraine

Incidents	Sectors	Threat Actors
116	17	16
↑ 9.4%	∞	↓ -15.8%

Daily evolution of cyber incidents impacting entities in Ukraine [April - June 2023]



Trends

- DDoS attacks account for 88.8% of all incidents. The most targeted sectors were the public administration (31), media (11), ICT (11), financial (11), and transportation (10).
- Four Ukrainian nonprofit organizations were targeted by DDoS attacks.

Top 10 sectors impacted in Ukraine [April- June 2023]

	Sector	Incidents	%Δ
1.	Public administration	31	55% ↑
2.	Media	11	120% ↑
3.	ICT	11	10% ↑
4.	Financial	11	-42.1% ↓
5.	Transportation	10	900% ↑
6.	Administrative / Sup.	8	300% ↑
7.	Energy	7	40% ↑
8.	Trade	4	-42.9% ↓
9.	Education	4	300% ↑
10.	Nonprofit	4	-20% ↓

Two cyberespionage campaigns, targeting Ukrainian public administration, have been attributed to *APT28*[2], a Russian state-sponsored actor:

- CERT-UA[3] has reported on a phishing campaign targeting Ukrainian government entities. The phishing emails contained the subject line "windows update" and instructions to run a PowerShell script. If executed, it could enable the threat actor to steal information from the targeted machine.
- CERT-UA[4] and Insikt Group[5] have identified a cyberespionage campaign against Ukrainian public administration entities. Targets were sent phishing emails with news about the conflict as a lure. The phishing emails exploited vulnerable Roundcube servers, immediately compromising the target's device if opened. More than 40 Ukrainian organizations were targeted. The campaign has been attributed to the threat actor *APT28*.

Emerging Issues

- Ukrainian civilians were targeted by a phishing campaign, reported by CERT-UA[6], with the goal of stealing Telegram credentials.

Notable threat actor activity

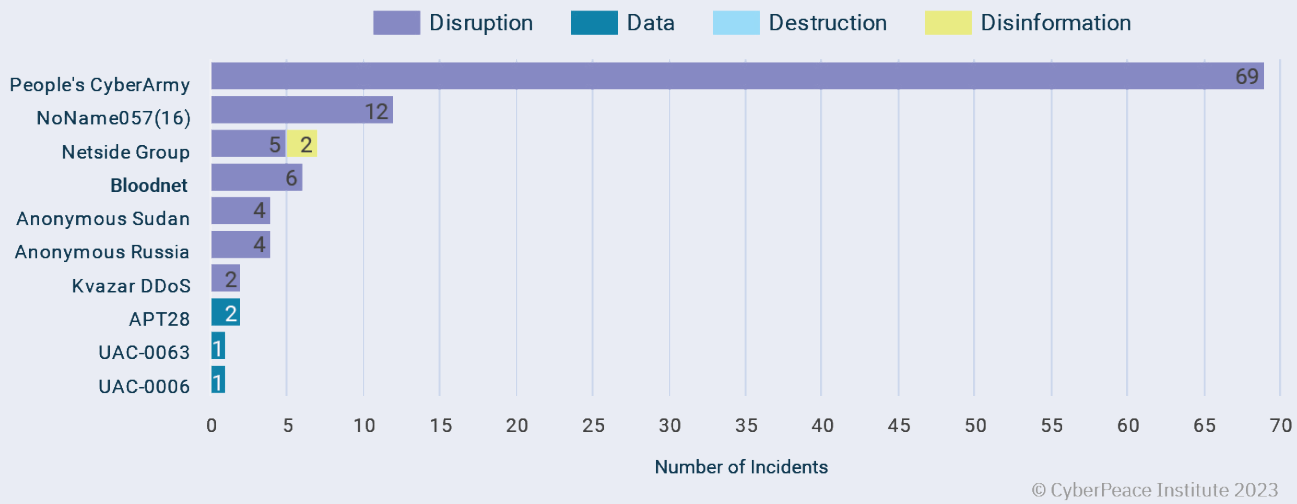
- *Solntsepek*, a newly tracked pro-Russian hactivist collective detected on Telegram. Their Telegram channel was created on April 25, 2022 but remained inactive until June 10, 2022. The group primarily focuses on information collection and the dissemination of data concerning members of the Ukrainian armed forces. *Solntsepek* started conducting cyberattacks in Q2 of 2023. The group mainly targets public administration and media entities in Ukraine. The CyberPeace Institute has recorded two confirmed cyberattacks conducted by *Solntsepek*.

  The name, *Solntsepek*, translates to "blazing sun" and is also a type of military equipment.

Latest malware

- BlackBerry Threat Research and Intelligence Team[7] has reported on a cyberespionage campaign against Ukrainian government officials, attributed to the threat actor *RomCom*. The pro-Russian threat actor created phishing websites, distributing malicious payloads on the target devices, allowing the threat actor to exfiltrate data.
- CERT-UA[8] has reported on a phishing email campaign targeting entities in Ukraine. The emails were sent by compromised accounts and contained a malicious file, which when executed would launch SmokeLoader malware. CERT-UA has attributed this campaign to the financially-motivated threat actor *UAC-0006*.
- CERT-UA[9] has reported a cyberespionage campaign targeting a Ukrainian government agency. The agency was sent phishing emails allegedly from the Embassy of Tajikistan in Ukraine on April 18 and April 20, 2023. The emails contained a malicious file that would compromise the target's device. Malware programs such as LOGPIE keylogger, CHERRYSPY backdoor and STILLARCH malware were used to steal data. CERT-UA uses the identifier *UAC-0063* to track the threat actor behind the campaign.

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



In May 2023, during the month commemorating the Soviet victory over Nazi Germany in World War II, pro-Russian threat actors accounted for 46% of all the incidents recorded during the second quarter of 2023. Furthermore, the pro-Russian hacktivist collective known as *People's CyberArmy* claimed responsibility for nearly 60% of all recorded incidents targeting Ukrainian entities in Q2 of 2023.

As previously noted in Q3 of 2022, it is probable that *People's CyberArmy* is affiliated with the broader *KillNet* collective.[10] However, a recent report published by Microsoft's Threat Analysis Group[11] indicates that *People's CyberArmy* is an online persona created by *Sandworm* to disseminate stolen data as part of *Sandworm*'s operations.

During the second quarter of 2023, the CyberPeace Institute documented four possible Distributed Denial of Service (DDoS) attacks against websites belonging to Ukrainian nonprofit organizations. Among the targeted entities were the websites of an anti-corruption project and a charitable foundation. Additionally, the pro-Russian *People's CyberArmy* directed DDoS attacks towards the websites of an association and an online resource providing assistance to refugees.

Apart from the observed disruption in website connectivity, no further information is currently available regarding any wider impacts of these incidents.

Cyberattacks on Ukrainian entities [Q2 2023 vs Q1 2023]

+9.4 %
cyberattacks

+120 %
cyberattacks on the media sector

+55 %
cyberattacks on the financial sector

Other notable incidents in Ukraine

Destruction

April 29, 2023

CERT-UA[12] has reported on a cyberattack against a Ukrainian state organization. According to CERT-UA, the threat actor was able to disable computers running Windows OS with RoarBat and computers running Linux with a BASH script. This attack is similar to a previous one reported by the Telegram channel *CyberArmyofRussia_Reborn* on January 17, 2023. CERT-UA attributes the described activity to *Sandworm* with a moderate level of confidence, but the corresponding identifier *UAC-0165* has been created for its tracking.

Disruption

June 14, 2023

Confirmed cyberattack against a Ukrainian public television and radio company leading to the disruption of services. The pro-Russian threat actor, *Solntsepek*[13], claimed responsibility for the attack.

Data

April 18, 2023

CERT-UA[14] has reported a cyberespionage campaign targeting a Ukrainian government agency. The agency was sent phishing emails allegedly from the Embassy of Tajikistan in Ukraine on April 18 and April 20, 2023. The emails contained a malicious file that would compromise the target's device. Malware programs such as LogPie keylogger, CherryPy backdoor and Stillarch malware were used to steal data. CERT-UA uses the identifier *UAC-0063* to track the threat actor behind the campaign.

June 19, 2023

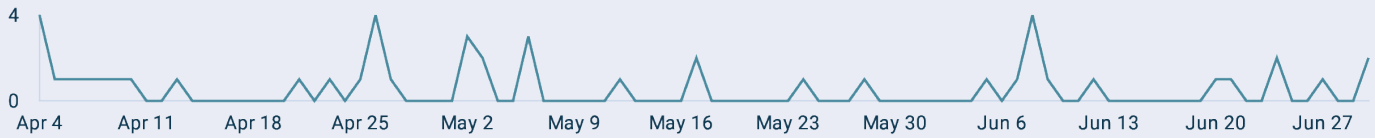
CERT-UA[15] has identified a phishing campaign against users of a Ukrainian email service. Targets were sent phishing emails posing as the Ukrainian email service. These emails contained a PDF file with a malicious link leading to a fraudulent site masquerading as the official Ukrainian email service. The threat actor was then able to obtain the targets' login and passwords. This campaign was attributed to the threat actor *UAC-0102*.

Trends and Emerging Issues Q2 2023

Russian Federation

Incidents	Sectors	Threat Actors
47	16	5
↓ -30.9%	↓ -11.1%	↓ -16.7%

Daily evolution of cyber incidents impacting entities in the Russian Federation [April - June 2023]



Trends

- DDoS attacks account for 72.3% of all incidents, followed by Defacement operations (8.5%).

Top 10 sectors impacted in the Russian Federation [April- June 2023]

	Sector	Incidents ▼	%Δ
1.	Public administration	7	600% ↑
2.	Manufacturing	7	133.3% ↑
3.	ICT	7	40% ↑
4.	Transportation	4	-66.7% ↑
5.	Media	4	-33.3% ↑
6.	Civilians	3	50% ↑
7.	Administrative / Sup.	3	-40% ↑
8.	Arts	2	∞
9.	Other service	2	
10.	Professional/ Scientific	2	100% ↑

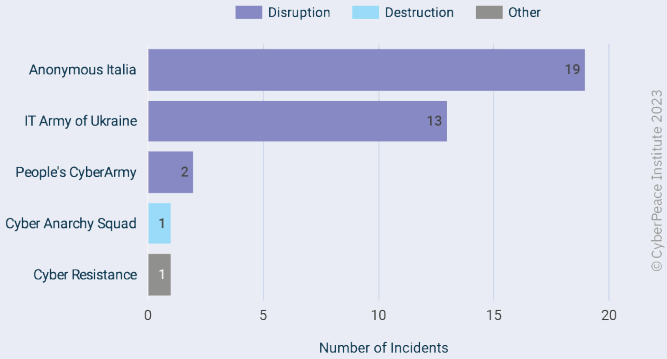
- Reduction in incidents likely caused by a decrease of substantiated claims of attacks by the *IT Army of Ukraine* and *Anonymous Italia*.
- Continuation of cyber-enabled information operation exploiting radio and television stations:
  - June 5[16], 2023 - A radio station broadcasting in different Russian regions was targeted by an unknown, highly likely pro-Ukrainian threat actor in a cyber-enabled information operation. The radio station allegedly played a fake message from President Putin announcing an invasion of the Russian Federation.
  - June 7[18], and 12[19] [20] 2023 - Cyber-enabled information operations conducted against radio stations in various regions of the Russian Federation. Unknown threat actor(s) targeted radio stations in different Russian regions leading to the broadcast of allegedly pro-Ukrainian messages.

Notable threat actor activity

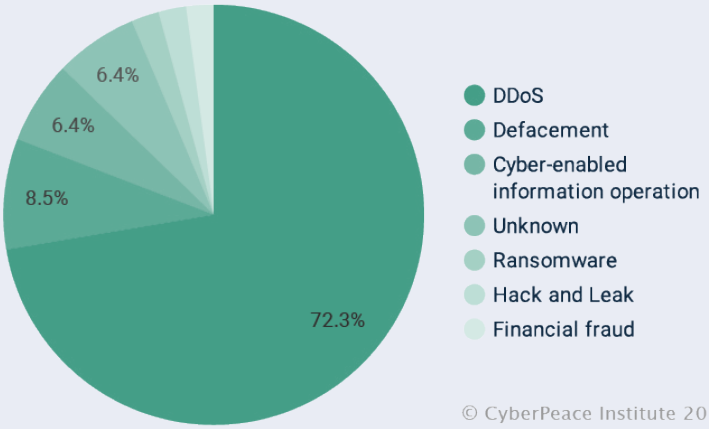
- Two incidents, purportedly attributed to, albeit unconfirmed officially , Wagner PMC:
  - An unknown threat actor has allegedly[21] conducted an unknown type of cyberattack against a Russian satellite telecommunications company. The attack led to a disruption of service. Initial reports indicated that the threat actor involved was Wagner PMC. However, there was no confirmation from the Wagner group.

- Cyble[22] has reported on a so-called "Wagner Ransomware" used to recruit new members to the paramilitary group. The ransomware encrypts files on the target's device. The ransom note also encourages a call to war against the Russian ministry of defense. Wagner PMC has not officially claimed responsibility for the ransomware.

Threat actors targeting entities in the Russian Federation [April - June 2023]



Types of cyber incidents targeting entities in the Russian Federation



In the second quarter of 2023, the CyberPeace Institute documented a decrease of 30.9% in malicious activities and a 16.7% decrease in active threat actors targeting Russian entities compared to Q1 of 2023. Additionally, the two most active pro-Ukrainian threat actors, namely *Anonymous Italia* and *IT Army of Ukraine*, have also seen a decline in incidents attributed to them by 49% and 24%, respectively.

The decrease noted by the CyberPeace Institute can likely be attributed to the Institutes's inclusion criteria[23] for data collection and processing. The CyberPeace Institute focuses on substantiated claims of attacks and other reports of malicious cyber activities. Consequently, claims of successful attacks by threat actors lacking additional proof are excluded from the platform. Nevertheless, the CyberPeace Institute continues to monitor the social media channels of threat actors that fail to provide supplementary evidence for their claims.

An illustrative example of potentially unrecorded activities is that of *Team OneFist*, a pro-Ukrainian hacktivist collective, one of whose members was interviewed by the BBC[24]. Despite ongoing monitoring of *Team OneFist*'s official communication channels for a year, only one self-attributed incident by this threat actor has been processed and published on the platform. Therefore, it's important to note that a decrease in processed incidents does not necessarily indicate a reduction in the activities of pro-Ukrainian threat actors against Russian entities.

Lastly, the CyberPeace Institute has documented three instances of cyber-enabled information operations that directly impacted the citizens of the Russian Federation. Continuing the trend observed in Q1 of 2023, unidentified pro-Ukrainian threat actors targeted Russian radio stations on three separate occasions in June 2023[25][26][27]. Two of the cyber-enabled information operations conveyed pro-Ukrainian messages, while the third operation broadcasted an alleged message attributed to Russia's President, stating that a full-scale invasion of Russia is currently underway.

Notable incidents in the Russian Federation

Other

April 4, 2023

Cyber Resistance, a pro-Ukrainian threat actor, has breached the account of and committed financial fraud against a Russian blogger, spending $25 000, originally raised for the Russian military, on adult toys.[28]

Disruption

April 10, 2023

A confirmed cyberattack carried out by an unidentified pro-Ukrainian threat actor targeted a Russian federal agency. Although certain IT services have been reinstated, several others remained offline, leading to the necessity of employing conventional paperwork at certain checkpoints.[29]

Data

May 28, 2023

A Russian high-technology project confirmed they had been targeted by a hack and leak operation conducted by a pro-Ukrainian threat actor. The threat actor gained partial access to a number of information systems and network resources, specifically the file exchange, located at the physical facilities of the organization. The target's public information resources, such as the website and online services, were also temporarily inaccessible.[30]

Destruction

June 8, 2023

Cyber Anarchy Squad, a pro-Ukrainian threat actor, has conducted an unknown type of cyberattack against a Russian Internet services provider. The threat actor was able to breach the target's IT systems, damaging a part of the network equipment and taking down the ISP services for 33 hours. Various clients of the ISP were reportedly cut off from the Internet as a result.[31]

Trends and Emerging Issues Q2 2023

Other Countries

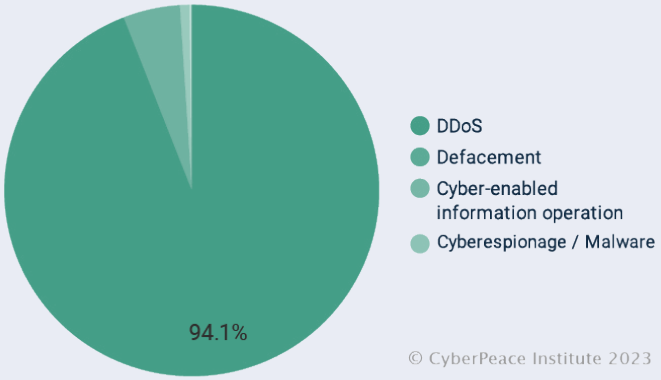
Incidents	Countries	Sectors	Threat Actors
489	38	22	18
↑2.9%	↓ -15,6%	↑ 4.8%	↓ -21.7%

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

Trends

- DDoS attacks account for 94.1% of all incidents recorded in countries which are not belligerents in this conflict.

Types of cyber incidents targeting entities outside the two belligerent states [April-June 2023]



- Most targeted sectors were the public administration (156), transportation (98), and financial (39).
- Sharp increase in attacks against Italian, French, Canadian, and Swiss entities with 100%, 428.6%, 866.7%, and 2500% respectively.

Countries, outside the two belligerent states, with more than 10 cyber incidents relating to the conflict [April - June 2023]

	Country	Incidents ▾	%Δ
1.	POLAND	65	-11%
2.	GERMANY	36	4.5%
3.	**FRANCE**	37	428.6%
4.	**CANADA**	29	866.7%
5.	LITHUANIA	29	-12.1%
6.	**ITALY**	28	100%
7.	**SWITZERLAND**	26	2500%
8.	SWEDEN	26	23.8%
9.	GREAT BRITAIN	23	-8%
10.	ESTONIA	22	∞
11.	SPAIN	20	42.9%
12.	DENMARK	16	23.1%
13.	LATVIA	16	-46.7
14.	CZECHIA	16	-48.4%
15.	NETHERLANDS	14	55.6%

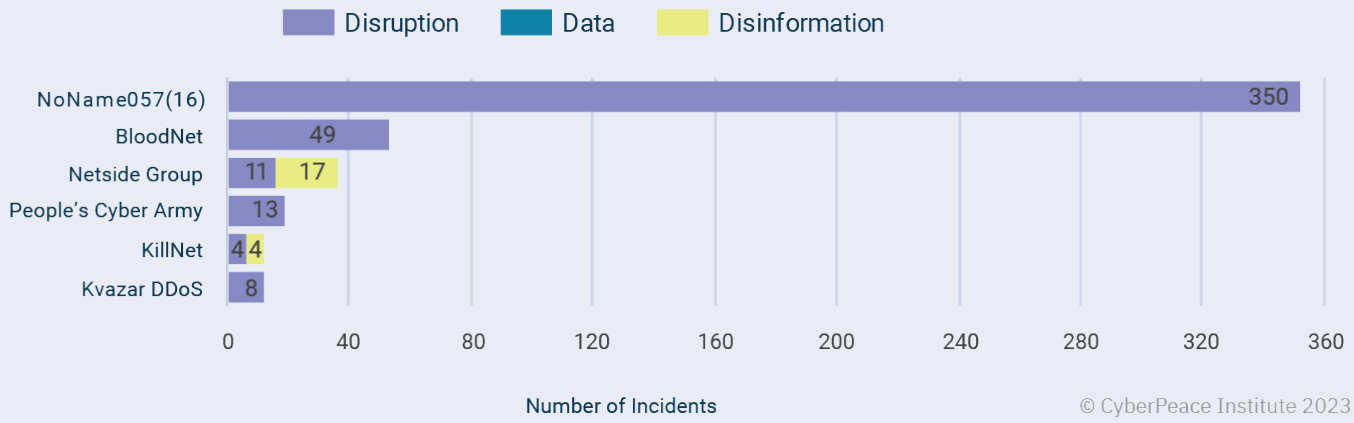
Notable threat actor (in)activity

For the second consecutive quarter, the notorious hacktivist collective *KillNet*, purportedly composed of 50 groups totaling 1250 individuals[32], including *Anonymous Russia*, has had a reduction in their malicious cyber activities. This decline can be attributed to an internal dispute within the larger collective resulting in the doxing[33] of the leader of *Anonymous Russia*. Subsequently, the leader was apprehended[34] in Belarus, prompting a significant restructuring of the group's framework with the intent of commercializing the hacktivist collective's endeavors. For further details on this topic, please refer to the Harm and Impact section later within this report.

Bloodnet

> A pro-Russian threat actor tracked through its Telegram channel, which was created on January 24, 2023. The group was originally affiliated with *Phoenix* until June 11, 2023.[35] The group likely has affiliations with other pro-Russian groups like *Killnet*, given their reposting of *Killnet*'s messages. The Institute started tracking this threat actor in April 2023. *Bloodnet* conducts DDoS attacks against non-belligerent countries such as Germany (11), Hungary (11), Poland (8), and Ukraine (6).

Top 6 threat actors targeting entities outside the two belligerent states [April - June 2023]



The CyberPeace Institute documented a 2.9% increase in malicious activities targeting entities in countries which are not belligerents in this conflict, demonstrating a second consecutive quarter of increased attack occurrences when compared to the preceding quarter. Additionally, *NoName057(16)* continues to be the most active pro-Russian hacktivist collective for the fourth consecutive quarter, increasing their malicious activities by 40% compared to Q1, 2023. It is almost certain that the main rationale behind *NoName057(16)*'s attacks is geopolitical (see Harm and Impact for more details). The second most active pro-Russian threat actor is the newly documented hacktivist collective *Bloodnet*.

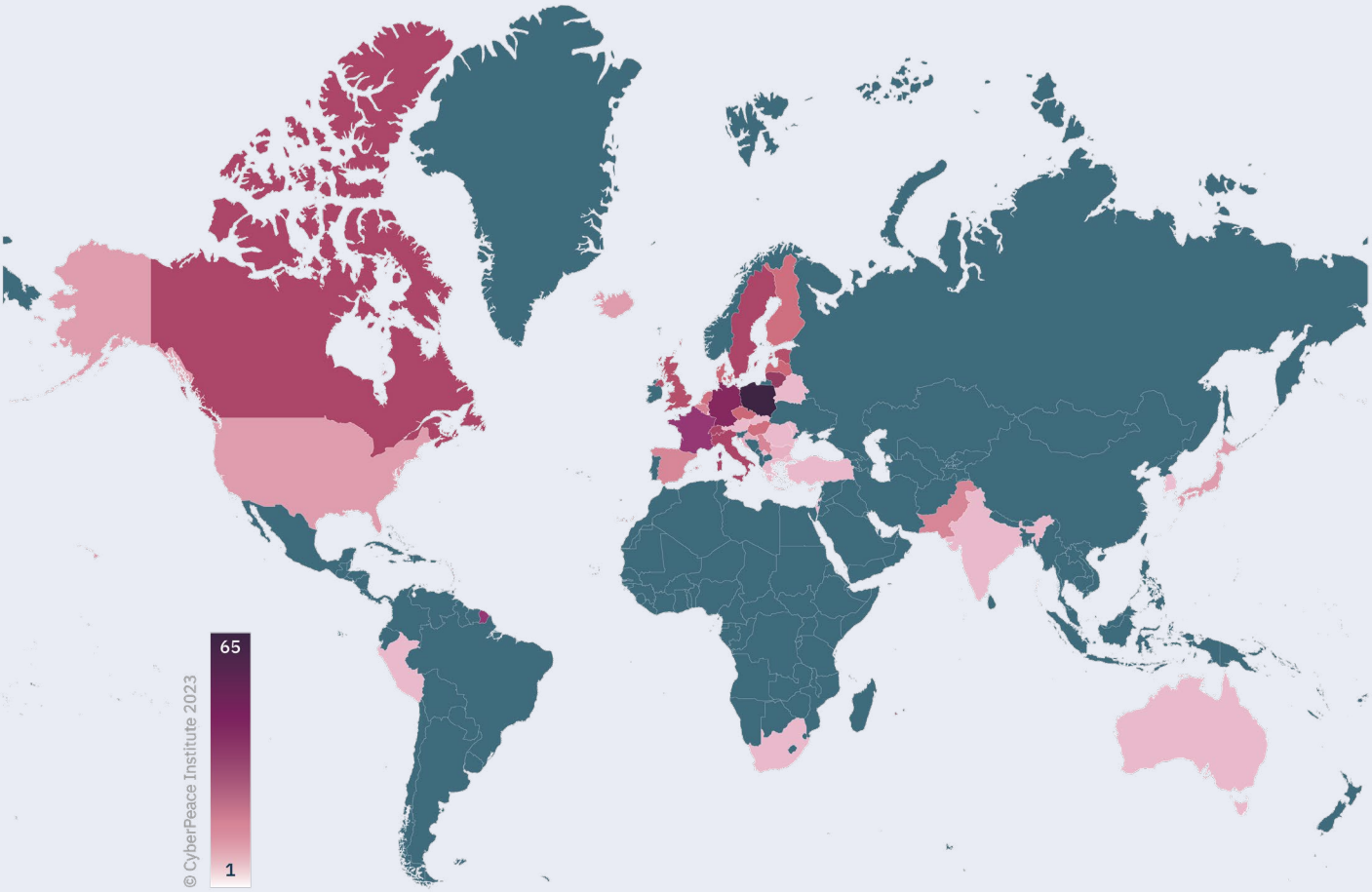
Poland and Germany – Continuing Targeted Actions

For the second consecutive quarter, pro-Russian threat actors have focused their efforts on entities located in Poland and Germany. The CyberPeace Institute has recorded 65 incidents against entities in Poland and 46 incidents against entities in Germany. Notably, a significant portion of these incidents, approximately 70%, can be attributed to attacks by *NoName057(16)*, particularly impacting the public administration (14), transportation (13), and financial (9) sectors in Poland. Similarly, attacks attributed to *NoName057(16)* account for 54% of all documented incidents targeting German entities. Within Germany, the public administration (17), manufacturing (6), and other services (5) sectors have been the primary targets of these attacks.

Switzerland

Throughout the second quarter of 2023, the CyberPeace Institute documented a significant increase in cyberattacks targeting Swiss entities, with attacks escalating by 2,500% compared to the previous quarter. This surge is highly likely linked to Switzerland's Council of State's decision in early June to permit arms re-exports to Ukraine.[36] In the subsequent weeks, the CyberPeace Institute recorded 69% of all cyberattacks conducted against Swiss entities in Q2, 2023.

Number of cyber incidents targeting organizations in countries other than the the two belligerent states [April- June 2023]



Notable incidents

Disruption

April 4, 2023

NoName057(16) claimed responsibility for a confirmed DDoS attack against the website of the Finnish parliament.[37] [38]

May 5, 2023

NoName057(16) claimed responsibility for two confirmed DDoS attacks against the website of the French senate.[30] [40] [41] [42]

June 12, 2023

NoName057(16) claimed responsibility for a confirmed DDoS campaign against Swiss entities, targeting the websites of two federal departments, two federal offices and the parliament. [43] [44] [45] [46] [47] [48]

June 19, 2023

KillNet and *Anonymous Sudan* have conducted DDoS attacks against two websites of a European financial institution. [49] [50]

Disinformation

June 13, 2023

French authorities have reported on an ongoing cyber-enabled information operation against French government websites and French news media. Doppelganger websites have been discovered promoting disinformation in regards to the ongoing armed conflict in Ukraine. This campaign has been attributed to Russian state actors by French authorities.[51]

Harm and Impact

In the second quarter of 2023, the CyberPeace Institute discovered the 100th threat actor[52], conducting malicious cyber activities in the context of the conflict in Ukraine. Currently, the CyberPeace Institute monitors, on a daily basis, the activities of more than 100 threat actors.

The CyberPeace Institute generally delineates the threat actors in three groups: state-sponsored actors, cybercriminals, and hacktivist collectives, of which the latter group accounts for 52% of all tracked threat actors. The modus operandi of the vast majority of hacktivist collectives, both pro-Russian and pro-Ukrainian, is conducting DDoS attacks, which account for 83% of all incidents documented by the CyberPeace Institute, since the start of the monitoring in 2022.

Impact and harm of DDoS attacks

Denial-of-service (DoS) attacks occur when malicious threat actors disrupt the availability of online resources. Distributed denial-of-service (DDoS) attacks, on the other hand, are more powerful and involve a coordinated effort to target the availability of internet services and resources. These attacks use similar techniques as regular DoS attacks, but on a larger scale. They involve multiple sources or locations simultaneously.[53] In practice, DDoS attacks cause an online resource, such as a website with crucial information or an online service portal, to become inaccessible or unavailable to visitors for a period of time during or following an attack.

One of the primary methods used to execute successful DDoS attacks is through the use of botnets. A botnet is a network of internet-connected devices that have been infected with malware and are controlled by a single entity known as a "bot-herder." The bot-herder manages the bots within the network and can orchestrate DDoS attacks by leveraging the resources of all the infected devices simultaneously. *NoName057(16)* is a known threat actor utilizing a botnet, operating a network established by the Bobik malware, with a significant number of bots located in Brazil, India, and Southeast Asia.[54]

However, malware infection is not the sole method for constructing a botnet. Some threat actors, like the pro-Russian *Anonymous Sudan* collective, opt to pay for servers through which they carry out DDoS attacks.[55] Others choose to crowdsource their DDoS activities by distributing downloadable software that adds volunteers' devices into a botnet. Both *NoName057(16)* and *IT Army of Ukraine* have used this approach, the former using an offensive crowdsourcing DDoS tool called DDOSIA Project, while the latter is employing both offensive and defensive crowdsourcing DDoS projects, such as disBalancer and Liberator.[56]

The impact of DDoS attacks can be direct and indirect. For targeted organizations, immediate consequences include disruptions to resource availability, leading to potential financial and reputational losses.[57] Often, due to concerns about reputation, many businesses choose not to disclose DDoS incidents. As Arora, Kumar, and Sachdeva note, the challenge for researchers is obtaining details about these attacks, as disclosure is often limited.[58]

DDoS attacks also have repercussions for the general population. The unavailability of online

resources can disrupt daily lives, leading to widespread issues such as anxiety or loss of confidence in governmental authorities. Research suggests that people are more likely to react to the effects of a cyberattack than the attack itself.[59]

In the context of a conflict, DDoS attacks can directly impact civilians by disrupting the availability of critical online resources. For example, non-governmental organizations play a pivotal role in providing humanitarian aid during conflicts. However, if their online resources are inaccessible, civilians may not be able to access essential services. The CyberPeace Institute has documented DDoS attacks against ten humanitarian funds operating in Ukraine.

The financial sector has been a primary target, with DDoS attacks affecting institutions in Ukraine, other countries, and Russia. Reports have also highlighted an increase in DDoS activities targeting financial institutions.[60] Such attacks may result in monetary losses and reputational damage for financial organizations.

DDoS attacks can hinder healthcare provision by disrupting access to online resources and interrupting business continuity. Healthcare professionals' work can be impacted due to disrupted access to critical assets like health records, medical equipment, or communication channels. Moreover, disruptions in the availability of online resources can affect the prescription of drugs, potentially endangering patients' well-being. Healthcare encompasses various organizations critical to the general population, such as suicide-prevention hotlines. Attacks against these services could have severe consequences. Lastly, an additional impact is caused when devices become corrupted or misconfigured following a crash, placing a significant additional burden on technical and medical staff due to diversion of resources.

Public administration has been a primary target in Ukraine, Russia, and countries which are not belligerents in this conflict. Such attacks not only impact government activities but can also directly and indirectly affect citizens. A DDoS attack that allegedly targeted Russia's only product authentication system, Chestny Znak, serves as an example of the direct impact such attacks can have.[61] As each product in Russia requires its unique identifier and company barcode to be scanned, from production to sale, the DDoS attack on Chestny Znak's servers purportedly led to the inability to authenticate products within the country for several days. Thus, making economic consequences highly likely.

DDoS attacks carry significant implications, impacting organizations, populations, and even influencing narratives amidst a conflict.

Monetization of hacktivism

In the second quarter of 2023, two prominent pro-Russian hacktivist collectives, *NoName057(16)* and *KillNet*, continued to be responsible for a significant portion of Distributed Denial of Service (DDoS) attacks targeting both Ukrainian and non-belligerent entities in the conflict. Notably, *NoName057(16)* maintained its malicious activities, while *KillNet* underwent significant changes in its structure and ideology.

Originally established by an individual using the pseudonym *KillMilk* as a DDoS-as-a-service in late 2021, *KillNet* began its participation in response to the global hacktivist collective *Anonymous* declaring a "cyber war against the Russian Federation".[62] Over time, *KillNet* expanded and evolved into one of the most prominent politically motivated pro-Russian hacktivist groups. However, beginning in 2023, a gradual decline in *KillNet*'s activities was observed by the CyberPeace Institute. *KillMilk* announced a restructuring of *KillNet* into the "Private Military Hackers Organization Black Skills," (*Black Skills*) citing a dispute within the Russian cyber community as a contributing factor.[63] This reorganization signaled a shift towards monetization of the hacktivist collective's activities, potentially posing threats to Ukrainian civilians and populations in other countries.

Shortly after the announcement of Black Skills, *KillNet*'s Telegram channel promoted the potential sale of the source code of a well-known spyware.[64] Subsequently, *KillNet* introduced Dark School, an educational initiative aimed at teaching individuals various malicious cyber techniques. This "school" offered nine courses in four languages – Russian, English, Spanish, and Hindu.[65] Later, another dispute led to the exposure of *Anonymous Russia*'s founder, a member of *KillNet* since September 2022.[66][67][68] Following this, an individual using the pseudonym *Radis* was appointed as the new leader of *Anonymous Russia*.[69] *Radis* quickly declared a shift in *Anonymous Russia*'s approach by offering paid services, thereby also embracing monetization.[70][71] Throughout Q2 of 2023, *Anonymous Russia* introduced a rental service for the TITAN Stealer malware.[72]

The TITAN Stealer is a type of information-stealing Trojan, written in Golang, designed to surreptitiously extract sensitive data from infected systems.[73] It primarily targets financial institutions and organizations, stealing login credentials, passwords, credit card details, and other personal or financial information. Distribution typically occurs through malicious email attachments, compromised websites, or social engineering tactics. Once installed, TITAN Stealer collects data from the target's computer and sends it to a remote server controlled by the attackers. This stolen information can be exploited for identity theft, financial fraud, or other illicit activities.[74]

On April 26, 2023, *KillMilk* officially announced the establishment of the "Russian private military hacker company *KillNet*," signaling the end of *KillNet*'s "altruistic activities". A week later, *KillNet* introduced an official crypto-exchange market.[76] On May 15, 2023, Radis similarly announced the cessation of "altruism" and transitioned to commercial activities, potentially establishing an online dark market for trading malware and malicious services.[77]

On May 24, 2023, *KillMilk* confirmed the disbandment of *KillNet*'s core, attributing it to the collective's perceived shift away from hacktivism.[78] *Radis* announced his departure a week later, citing a lack of progress on the dark web and a desire to avoid resentment.[79]

The CyberPeace Institute is unaware of the chronological progression of events that led to the disbandment of the *KillNet* group and the subsequent alterations within its structure.

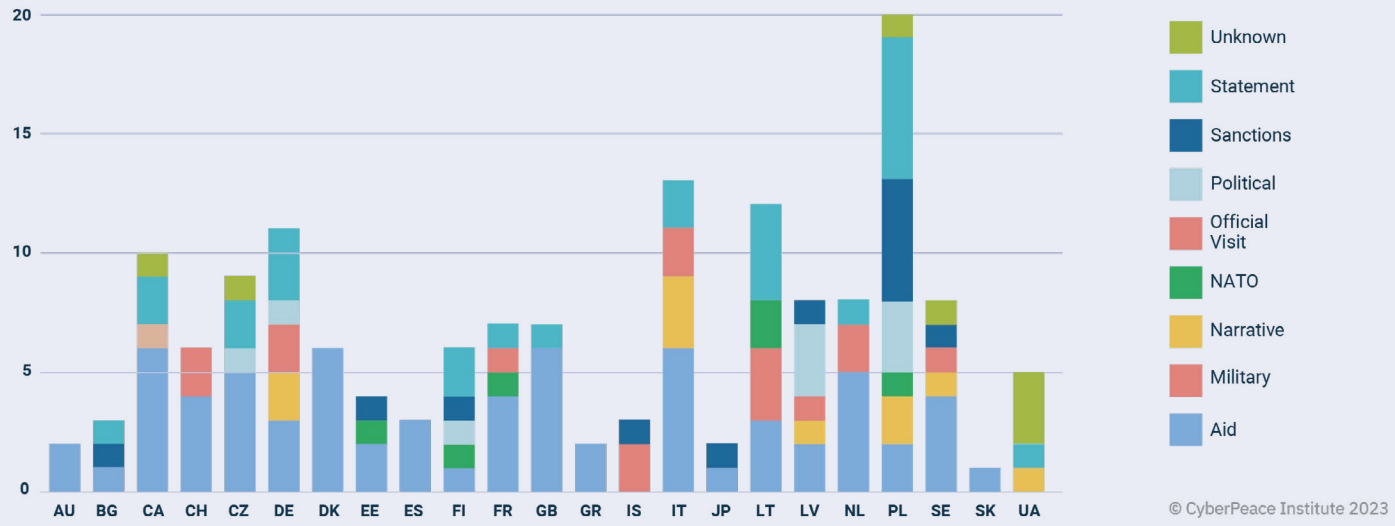
KillNet reportedly reemerged with a new core on June 12, although no incidents have been conclusively attributed to them for the remainder of the quarter due to a lack of substantiating evidence for their attack claims.

While internal conflicts have disrupted the *KillNet* collective, *NoName057(16)* has shown a continued escalation in its malicious activities, primarily targeting entities situated in countries which are not belligerents in this conflict. Radware[80] positions *NoName057(16)* as the most prolific threat actor, aligning with the findings of the CyberPeace Institute based on the incidents cataloged on the Cyber Attacks in Times of Conflict Platform #Ukraine.[81] Notably, the Institute's data collection has unveiled a discernible pattern in *NoName057(16)*'s actions – the threat actor predominantly employs Distributed denial-of-service (DDoS) attacks as a responsive measure to geopolitical events. Examples of these events include official visits by Ukraine's President Zelenskyy or media reports concerning new military and economic assistance for Ukraine.

Displayed below is a graphical representation wherein the CyberPeace Institute has categorized the rationales presented by *NoName057(16)* behind executing DDoS attacks on entities across several countries. These rationales have been compartmentalized into eight distinct classes. The term "Aid" pertains to financial and/or civilian support extended to Ukraine by countries which are not belligerents in the conflict, while "Military" signifies any form of military assistance. "Narrative" denotes motivations for attacks aimed at advancing specific narratives related to the conflict, usually coined by official governmental bodies within the Russian Federation. "NATO" encompasses rationales tied to official announcements or training activities by NATO.

The "Official Visits" category encompasses motives for attacks arising from visits of Ukrainian officials to other countries. "Political" refers to motivations related to official political shifts categorized as Russophobic by *NoName057(16)*. "Sanctions" encompasses motives for attacks triggered

Reason for DDoS attacks self-attributed by NoName057(16).



by the imposition of global and/or national sanctions targeting the Russian Federation. "Statements" covers rationales stemming from statements made and/or endorsed by official entities in the targeted countries. Lastly, "Unknown" encompasses any motivations that do not fit within the scope of the other seven categories.

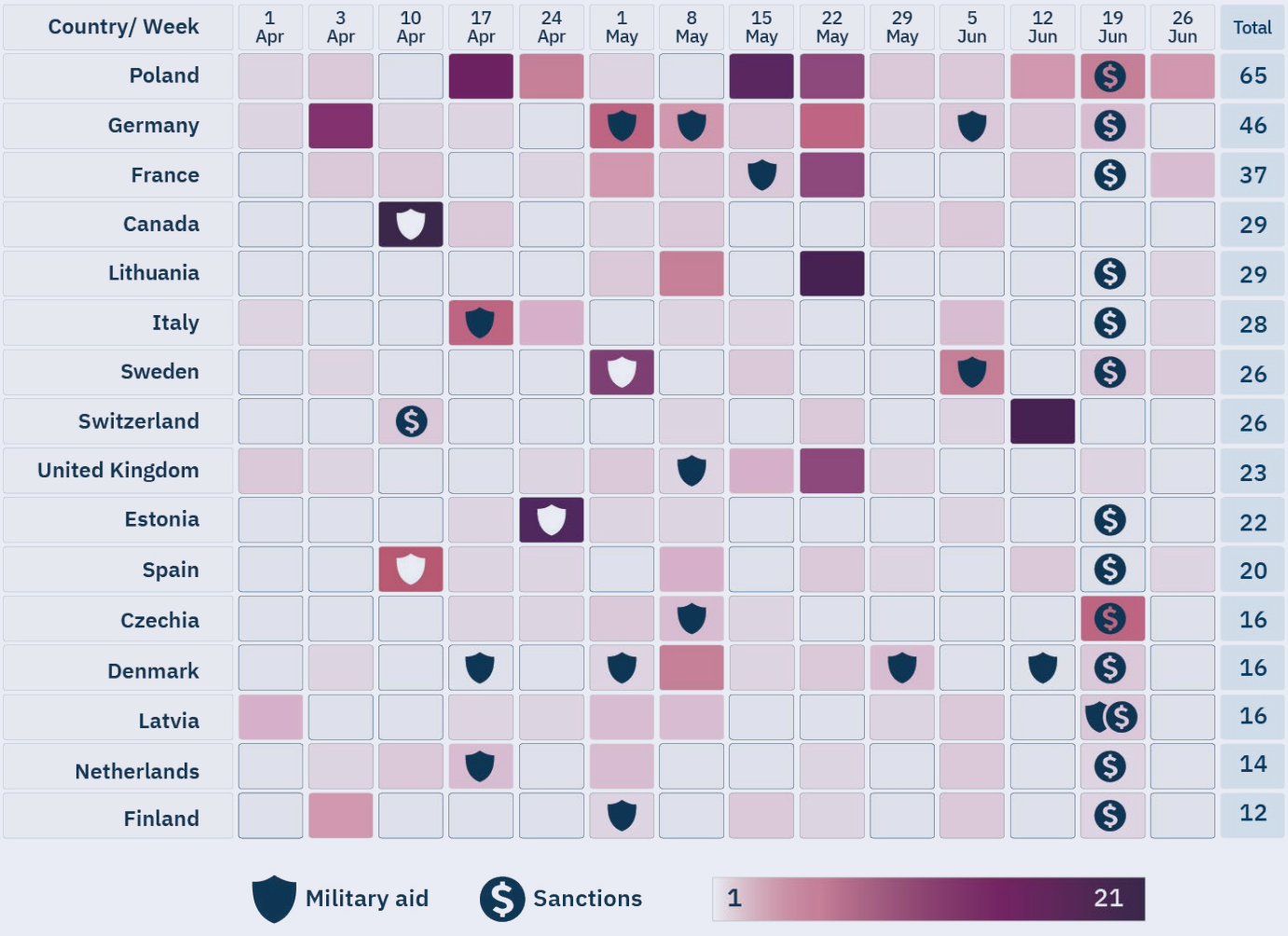
Wider Contextual Considerations

Events

During the second quarter of 2022, the most notable kinetic development affecting one of the belligerent nations in the conflict was Wagner's advance toward Moscow.[82] The CyberPeace Institute did not observe any escalation in malicious cyber activities targeting Russian entities during Wagner's PMC march to Moscow. The incident was widely seen as a challenge to the legitimacy of the Russian Federation's official government from Yevgeny Prigozhin.

In the heatmap depicted below, the CyberPeace Institute has documented instances of cyberattacks associated with geopolitical occurrences, specifically focusing on non-belligerent countries' responses concerning sanctions, military assistance, and public statements related to the conflict.

Heat matrix indicating the number of incidents per week for all countries with more than 10 incidents in Q2 2023 overlaid with documented



At the beginning of April, Ukraine's military initiated the deployment of the first MiG-29 fighters aircrafts received from Poland. It is highly likely this action led pro-Russian threat actors to intensify attacks against Polish entities, with Poland becoming the most targeted country beyond the 2 belligerent countries, during Q2 of 2023. During March, Slovakia had also announced their decision to deliver 13 MG-29 aircraft to Ukaine.[83]

The delivery of tanks has also continued, with Germany, Canada, and the United Kingdom successfully completing the transfer of Leopard 2 and Challenger tanks[84], which highly likely caused an increase of attacks against entities in Germany and Canada by 4.5% and 867%, respectively. In a continuation of support from European Union members, Spain dispatched six Leopard 2A4s. It's highly likely that this action contributed to a 43% surge in attacks against Spanish entities in Q2.[85] Throughout April, additional commitments were made for tank transfers, including Denmark and the Netherlands pledging to send 14 more Leopard 2 tanks, likely leading to a 23%, and 56% increase in attacks against entities in the two countries respectively.[86] Denmark later announced, in early May, the intention to transfer an additional 80 Leopard 1 tanks to Ukraine, in conjunction with Germany.

Over the course of the second quarter, countries including the United Kingdom, Latvia, Estonia, Canada, Italy, Denmark, the Netherlands, Sweden, and Poland continued, or made promises, to provide training for Ukrainian soldiers to effectively operate the weaponry supplied by Ukraine's allies.[87 88 89 90 91 92 93 94 95]

The landscape of sanctions and official statements also saw notable developments. In the second quarter of 2023, several countries imposed fresh sanctions against the Russian Federation. Latvia enhanced regulations governing the presence of Russian citizens within its territory, while Bulgaria closed off access to all ports for Russian vessels.[96 97] The general secretary of Japan's government declared new sanctions against Russia.[98] However, the CyberPeace Institute did not document any pronounced surge in cyberattacks targeting entities within these mentioned countries. By the conclusion of the quarter, the European Union collectively agreed on the 11th sanctions package, specifically targeting the Druzhba oil pipeline.[99 100]

Other Research

In recent months, several significant developments have emerged in the realm of cyber operations and threat activities, particularly within the context of the ongoing Russia-Ukraine conflict. These events shed light on evolving tactics, potential risks, and the intricate interplay between cyber warfare and kinetic actions.

Stiftung Wissenschaft und Politik (SWP) published an insightful analysis on the role of cyber operations in the Ukraine conflict.[101] The report delves into Russia's cyber strategies, emphasizing intelligence gathering, data destruction, and Denial-of-Service (DoS) attacks on critical infrastructure. While acknowledging Ukraine's proactive cyber defense measures and societal resilience, the analysis questions the strategic effectiveness of Russia's cyber warfare in terms of substantial gains. The importance of cyber resilience is underscored, along with key takeaways from Ukraine's wartime cyber efforts.

ESET released a comprehensive report summarizing observations and analyses of advanced persistent threat (APT) groups from Q4 2022 to Q1 2023.[102] The report highlights APT activities across various countries, including China, India, Iran, North Korea, and Russia. In this period, ESET researchers provided a critical assessment of APT group operations, shedding light on their evolving tactics and potential implications for cybersecurity.

Microsoft Threat Intelligence presented an updated evaluation of a threat actor, now identified as *Cadet Blizzard*, previously known as *DEV-0586*.[103] This actor is associated with the Russian General Staff Main Intelligence Directorate (GRU). Microsoft highlighted *Cadet Blizzard*'s resurgence in early 2023, engaging in heightened operations across Ukraine and Europe. The report emphasizes the importance of protective measures against *Cadet Blizzard*'s activities, accompanied by discussions on detection and prevention strategies.

Sekoia's blog post delves into the DDoSia project, a Distributed Denial of Service (DDoS) attack toolkit attributed to the pro-Russian hacktivist group *NoName057(16)*.[104] The analysis uncovers the project's mechanics, communication channels, registration processes, and execution of attacks. Notably, the report highlights the project's primary targets: Ukraine, NATO countries, and select Western nations supporting Ukraine. Various sectors, including education, finance, government, and transport, are among the specific targets.

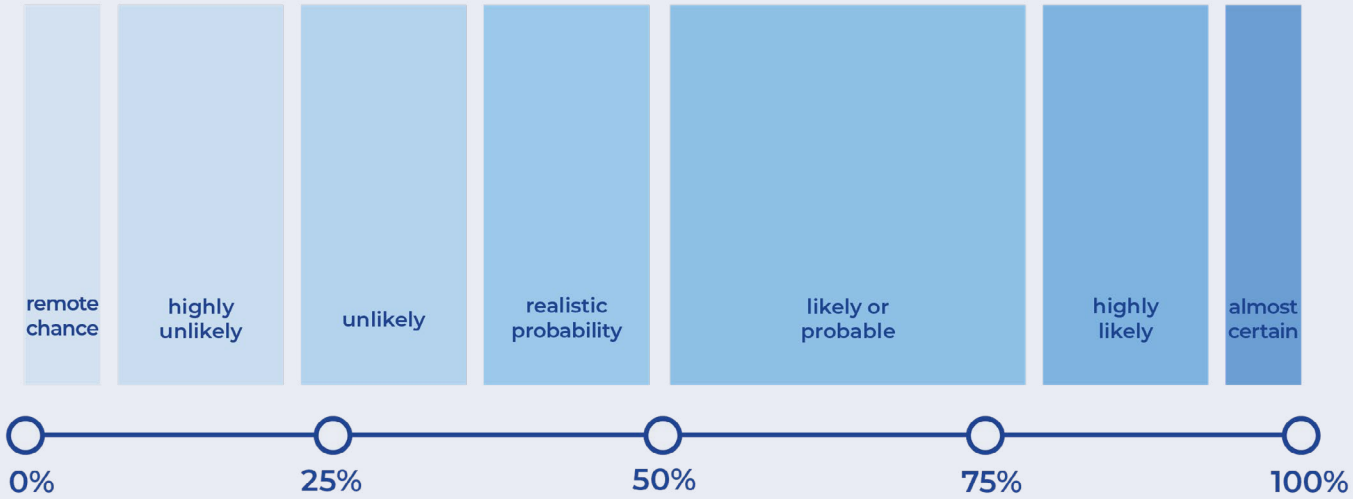
Mandiant's M-Trends 2023 Special Report offers insights from consulting investigations spanning January 1, 2022, to December 31, 2022.[105] The report covers diverse topics, such as cyber operations within the Ukraine conflict, notable threat groups, vulnerabilities, and North Korean cybercrime. An intriguing highlight is the potential overlap between cyber operations and kinetic warfare, as evidenced by Russian actions impacting industrial control systems and critical infrastructure.

These reports provide a comprehensive view of recent cyber operations, threat activities, and their implications. The evolving nature of cyber warfare underscores the necessity for enhanced cyber resilience and adaptive strategies in conflicts.

Report Methodology

This report focuses on the incidents documented by the CyberPeace Institute in the second quarter of 2023. Therefore, analysis only covers attacks and campaigns between April 1 and June 30, 2023. For trends-based analysis, the CyberPeace Institute may refer to numbers during a wider date range, in this case the dates are referenced accordingly in the report. Information within the report is generated from data collected by the CyberPeace Institute and made accessible through the Cyber Attacks in Times of Conflict Platform[106]#Ukraine. Specific details and sources of information regarding any individual cyber incidents referenced in this report can be found in the Attack Details[107] 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[108]. Additionally, the CyberPeace Institute distinguishes between singular incidents and campaigns.[109] When conducting analysis it is instrumental to accurately communicate probability in the assessment of our findings and inferences. The CyberPeace Institute uses the UK's Defence Intelligence standard for conveying probability; the 'Professional Head of Intelligence Assessment (PHIA) probability yardstick'.[110] This scale demonstrates broad ranges of certainty or uncertainty that can be translated into consistent language; this language is used throughout this report.



PHIA Probability Yardstick

Source: United Kingdom College of Policing

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

References

[1] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 7 April 2023)

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

[3] CERT-UA. (2023). 'Kiberataka hrupy APT28: rozpovsyudzhennya elektronnyx lystiv z "instrukciyamy" shhodo "onovlennya operacijnoyi systemy" (CERT-UA#6562)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4492467 (Accessed: 29 April 2023).

[4] CERT-UA. (2023). 'Hrupoyu APT28 zastosovano try eksplojty dlya Roundcube (CVE-2020-35730, CVE-2021-44026, CVE-2020-12641) pid chas cherhovoyi shpyhuns"koyi kampaniyi (CERT-UA#6805)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4905829 (Accessed: 21 June 2023).

[5] Recorded Future. (2023). 'BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities'. Insikt Group. Available at: https://www.recordedfuture.com/bluedelta-exploits-ukrainian-government-roundcube-mail-servers (Accessed: 21 June 2023).

[6] CERT-UA. (2023). 'Rozsylannya SMS-povidomlen" z temoyu sudovyx povistok z vykorystannyam shaxrajs"koho al"fa-imeni "SUDpovistka" (CERT-UA#6804)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4789582 (Accessed: 3 June 2023).

[7] BlackBerry. (2023). 'RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine'. The BlackBerry Research & Intelligence Team. Available at: https://blogs.blackberry.com/en/2023/06/romcom-resurfaces-targeting-ukraine (Accessed 8 June 2023).

[8] CERT-UA. (2023). 'Povernennya UAC-0006: masove rozpovsyudzhennya SmokeLoader z vykorystannyam tematyky "raxunkiv" (CERT-UA#6613)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4555802 (Accessed 6 May 2023).

[9] CERT-UA. (2023). 'Shpyhuns"ka aktyvnist" UAC-0063 u vidnoshenni Ukrayiny, Kazaxstanu, Kyrhyzstanu, Monholiyi, Izrayilyu, Indiyi (CERT-UA#6549)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4697016 (Accessed: May 23 2023).

[10] CyberPeace Institute. (2022). 'Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q3 July to September'. CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q3%20Report.pdf (Accessed: 7 August 2023).

[11] Google. (2023). 'Ukraine remains Russia's biggest cyber focus in 2023'. Threat Analysis Group. Available at: https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/ (Accessed: 20 April 2023).

[12] CERT-UA. (2023). 'WinRAR yak "kiberzbroya". Destruktyvna kiberataka UAC-0165 (jmovirno, Sandworm) na derzhsektor Ukrayiny iz zastosuvannyam RoarBat (CERT-UA#6550)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4501891 (Accessed: 30 April 2023).

[13] Solntsepek (2023) [Telegram] 14 June. Available at: https://t.me/solntsepekZ/846 (Accessed: 15 June).

[14] CERT-UA. (2023). 'Shpyhuns"ka aktyvnist" UAC-0063 u vidnoshenni Ukrayiny, Kazaxstanu, Kyrhyzstanu, Monholiyi, Izrayilyu, Indiyi (CERT-UA#6549)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4697016 (Accessed: 23 May 2023).

[15] CERT-UA. (2023). 'Cil"ovi kiberataky UAC-0102 u vidnoshenni korystuvachiv servisu UKR.NET (CERT-UA#6858)'. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/4928679 (Accessed: 20 June 2023).

[16] Radio MIR (2023) [VKontakte]. Available at: https://vk.com/wall-35310608_118918 (Accessed: 13 June).

[17] Privet-Rostov. (2023). 'Fejkovoe obrashhenie Putina o voennom polozhenii i vseobshhej mobilizacii v Rostovskoj oblasti zapustili hakery'. Privet-Rostov. Available at: https://privet-rostov.ru/gorod/91202-fejkovoe-obraschenie-putina-o-voennom-polozhenii-i-vseobschej-mobilizacii-v-rostovskoj-oblasti-zapustili-hakery.html (Accessed: 7 June 2023).

[18] Operatyvnyj shtab - Krasnodarskyj kraj (2023) [Telegram]. Available at: https://t.me/opershtab23/7041 (Accessed: 13 June).

[19] Operatyvnyj shtab - Krasnodarskyj kraj (2023) [Telegram]. Available at: https://t.me/opershtab23/7054 (Accessed: 13 June).

[20] News Media Source

[21] Antoniuk, D. (2023). 'Hackers claim to take down Russian satellite communications provider'. Recorded Future. Available at: https://therecord.media/hackers-take-down-russian-satellite-provider (Accessed: 30 June 2023).

[22] Cyble. (2023) 'Unveiling Wagner Group's Cyber-Recruitment'. Cyble. Available at: https://cyble.com/blog/unveiling-wagner-groups-cyber-recruitment/ (Accessed: 30 June 2023).

[23] CyberPeace Institute (2022). 'FAQ Data & Methodology'. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 1 August 2023).

[24] Tidy, J. (2023). 'Meet the hacker armies on Ukraine's cyber front line'. British Broadcasting Company. Available at: https://www.bbc.com/news/technology-65250356 (Accessed: 16 April 2023).

[25] Radio MIR (2023) [VKontakte]. Available at: https://vk.com/wall-35310608_118918 (Accessed: 13 June).

[26] Operatyvnyj shtab - Krasnodarskyj kraj (2023) [Telegram]. Available at: https://t.me/opershtab23/7041 (Accessed: 13 June).

[27] Operatyvnyj shtab - Krasnodarskyj kraj (2023) [Telegram]. Available at: https://t.me/opershtab23/7054 (Accessed: 13 June).

[28] Atlas News. (2023). 'Ukrainian Hackers Spend $25,000 of Russian Funds on Sex Toys'. Atlas News. Avaiable at: https://theatlasnews.co/conflict/2023/04/04/ukrainian-hackers-spend-25000-of-russian-funds-on-sex-toys/ (Accessed: 5 April 2023).

[29] Port News. (2023). 'FCS' IT resources under a cyberattack'. Port News. Available at: https://portnews.ru/news/345714/ (Accessed: 19 April 2023).

[30] Skolkovo Live (2023) [Telegram]. Available at: https://t.me/skolkovolive/4497 (Accessed: 30 May 2023).

[31] SecurityLab. (2023). 'Proukrainskie hakery utverzhdajut, chto otkljuchili sistemy operatora bankovskoj sistemy Rossii'. SecurityLab. Available at: https://www.securitylab.ru/news/538863.php (Accessed: 20 June 2023).

[32] KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/836 (Accessed: 25 May 2023).

[33] KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/724 (Accessed: 20 April 2023).

[34] Keffer, L. (2023). 'V Belorussii arestovan osnovatel' Telegram-kanala, vhodjashhego v set' hakerov Killnet'. Kommersant. Available at: https://www.kommersant.ru/doc/5939125 (Accessed: 20 April 2023)

[35] Phoenixinform (2023) [Telegram]. Available at: https://t.me/phoenixinform/2118 (Accessed: 12 June 2023).

[36] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/2656 (Accessed: 5 April 2023).

[37] https://www.eduskunta.fi/EN/tiedotteet/Pages/ddos_webservice_parliament_20230404.aspx

[38] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3110 (Accessed: 6 May 2023).

[39] Senat (2023) [Twitter]. Available at: https://twitter.com/Senat/status/1654408818934120448?cxt=HHwWgIC83cWD0vUtAAAA (Accessed: 6 May 2023).

[40] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3262 (Accessed: 16 May 2023).

[41] Senat (2023) [Twitter]. Available at: https://twitter.com/Senat/status/1658029548670205953?cxt=HHwWgoC2ueDFwIIuAAAA (Accessed: 16 May 2023).

[42] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3660 (Accessed: 13 June 2023).

[43] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3659 (Accessed: 13 June 2023).

[44] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3658 (Accessed: 13 June 2023).

[45] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3657 (Accessed: 13 June 2023).

[46] NoName057(16) (2023) [Telegram]. Available at: https://t.me/noname05716/3655 (Accessed: 13 June 2023).

[47] Le Temps. (2023). 'Derrière la cyberattaque contre l'administration suisse, l'ombre grandissante de la Russie'. (Accessed: 13 June 2023).

[48] KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6977 (Accessed: 20 June 2023).

[49] European Investment Bank (2023) [Twitter]. Available at: https://twitter.com/EIB/status/1670783791600656384 (Accessed: 20 June 2023).

[50] Ministères de L'Europe et des affairs etrangères. (2023). Déclaration de Catherine Colonna - Ingérences numériques étrangères – Détection par la France d'une campagne de manipulation de l'information (13 juin 2023). Available at: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2023/article/declaration-de-catherine-colonna-ingerences-numeriques-etrangeres-detection-par (Accessed: 15 June 2023).

[51] CyberPeace Institute. (2023). 'From 0 to 100: a story of the escalation of Threat Actors'. Available at: https://cyberpeaceinstitute.org/news/story-of-the-escalation-of-threat-actors/ (Accessed: 10 August 2023).

[52] Cloudflare.(n.d.). 'What is a DDoS attack?'. Cloudflare. Available at: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/ (Accessed: 2 August 2023).

[53] Chlumecky, M. (2022). 'Pro-Russian Group Targeting Ukraine Supporters with DDoS Attacks'. Avast. Available at: https://decoded.avast.io/martinchlumecky/bobik/ (Accessed: 2 August 2023).

[54] Wahlen M. (2023) Anonymous Sudan. Threat Intelligence Report. Truesec. Available at: https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf (Accessed 12 April 2023).

[55] https://disbalancer.com

[56] 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).

[57] Arora, K., Kumar, K. & Sachdeva, M. (2011). 'Impact Analysis of Recent DDoS Attacks'. International Journal on Computer Science and Engineering 3(2). Available at: https://www.researchgate.net/publication/50247519_Impact_Analysis_of_Recent_DDoS_Attacks (Accessed: 7 August 2023).

[58] Bada, M. & Nurse, J.R.C. (2019). 'The Social and Psychological Impact of Cyber-Attacks'. Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press. Available at: https://www.semanticscholar.org/paper/The-Social-and-Psychological-Impact-of-Bada-Nurse/1a9c74586a7ecf5c3e32b75e5b73919182cb0746 (Accessed: 7 August 2023).

[59] Picus. (2022). 'UK Finance sector reports increase in DDoS-related cyber incidents'. Picus. Available at: https://www.picussecurity.com/resource/fca-data-reveals-increase-in-ddos-incidents (Accessed: 7 August 2023).

[60] Tidy, J. (2023). 'Meet the hacker armies on Ukraine's cyber front line'. British Broadcasting Company. Available at: https://www.bbc.com/news/technology-65250356 (Accessed: 16 April 2023).

[61] 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: 7 August 2023).

[62] CyberPeace Institute. (2022). 'Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q4 October to December 2022'. CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf (Accessed: 7 August 2023).

[63] Milmo, D. (2022). 'Anonymous: the hacker collective that has declared cyberwar on Russia'. The Guardian. Available at: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia (Accessed: 20 June 2023).

[64] KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5681 (Accessed: 13 March 2023).

[65] KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5740 (Accessed: 19 March 2023).

[66] KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/5967 (Accessed: 5 April 2023).

[67] KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/724 (Accessed: 18 April 2023).

[68] Keffer, L. (2023). 'V Belorussii arestovan osnovatel' Telegram-kanala, vhodjashhego v set' hakerov Killnet'. Kommersant. Available at: https://www.kommersant.ru/doc/5939125 (Accessed: 18 April 2023).

[69] Bracken, B. (2023). 'Killnet Boss Exposes Rival Leader in Kremlin Hacktivist Beef'. Dark Reading. Available at: https://www.darkreading.com/threat-intelligence/killnet-boss-rival-leader-kremlin-hacktivist-beef (Accessed: 20 April 2023).

[70] Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/3 (Accessed: 17 April 2023).

[71] Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/6 (Accessed: 17 April 2023).

[72] Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/94 (Accessed: 23 April 2023).

[73] Anonymous Russia (2023) [Telegram]. Available at: https://t.me/anon_russ/217 (Accessed: 4 May 2023).

[74] Cyble. (2023). 'Titan Stealer: The Growing Use of GoLang Among Threat Actors'. Cyble. Available at: https://cyble.com/blog/titan-stealer-the-growing-use-of-golang-among-threat-actors/ (Accessed: 2 August 2023).

[75] Kathiresan, K. (2023). 'The Titan Stealer: Infamous Telegram Malware Campaign'. Uptycs. Available at: https://www.uptycs.com/blog/titan-stealer-telegram-malware-campaign (Accessed: 2 August 2023).

[76] KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/794 (Accessed: 27 April 2023).

[77] KillNet (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6595 (Accessed: 10 May 2023).

[78] Radis (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6668 (Accessed: 16 May 2023).

[79] KillMilk (2023) [Telegram]. Available at: https://t.me/killmilk_rus/836 (Accessed: 26 May 2023).

[80] Radis (2023) [Telegram]. Available at: https://t.me/killnet_reservs/6830 (Accessed: 6 June 2023).

[81] Radware. (2023). 'Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists'. Radware. Available at: https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/ (Accessed: 2 May 2023).

[82] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 7 April 2023)

[83] Schulze, M. and Kerttunen, M. (2023). 'Cyber Operations in Russia's War against Ukraine'. Stiftung Wissenschaft und Politik. Available at: https://www.swp-berlin.org/publikation/cyber-operations-in-russias-war-against-ukraine (Accessed: 7 August 2023).

[84] Boutin,J.M. (2023). 'ESET APT Activity Report Q4 2022–Q1 2023'. ESET. Available at: https://www.welivesecurity.com/2023/05/09/eset-apt-activity-report-q42022-q12023/ (Accessed: 7 August 2023).

[85] Microsoft Threat Intelligence. (2023). 'Cadet Blizzard emerges as a novel and distinct Russian threat actor'. Microsoft. Available at: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/ (Accessed: 7 August 2023)

[86] Amaury G., Charles M. and Threat & Detection Research Team. (2023). 'Following NoName057(16) DDoSia Project's Targets'. Sekoia. Available at: https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/ (Accessed: 7 August 2023).

[87] Mandiant. (2023). 'M-Trends 2023'. Mendiant. Available at: https://www.mandiant.com/m-trends (Accessed: 7 August 2023).

[88] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 7 April 2023)

[89] Ibid

[90] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 2 May 2023).

[91] Ibid

[92] 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)

[93] Reuters. (2023). 'Netherlands wants to give Ukrainian pilots F-16 training as soon as possible'. Reuters. Available at: https://www.reuters.com/world/europe/netherlands-wants-give-ukrainian-pilots-f-16-training-soon-possible-2023-05-24/ (Accessed: 30 June 2023).

[94] Försvarsmakten. (2023). 'Ukrainian soldiers ready for the front'. Försvarsmakten. Available at: https://www.forsvarsmakten.se/en/news/2023/06/ready-for-the-front/ (Accessed: 10 June 2023).

[95] Joint-Forces. (2023). 'Ukrainian Soldiers In Poland Train On Leopard Tanks'. Joint-Forces. Available at: https://www.joint-forces.com/world-news/defence-news/63480-ukrainian-soldiers-in-poland-train-on-leopard-tanks (Accessed: 20 April 2023).

[96] Ministry of Foreign Affairs. (2023). 'Entry into Latvia by citizens of the Russian Federation and Frequently Asked Questions'. Available at: https://www.mfa.gov.lv/en/entry-latvia-citizens-russian-federation-and-frequently-asked-questions?utm_source=https%3A%2F%2Fwww.google.com%2F (Accessed: 20 June 2023).

[97] TVP. (2023). 'Bulgaria closes sea and river ports to Russian ships'. TVP World. Available at: https://tvpworld.com/69017706/bulgaria-closes-sea-and-river-ports-to-russian-ships (Accessed: 10 April 2023).

[98] Suetomi, J. (2023). 'Japan introduces further sanctions against Russia'. Baker McKenzie. Available at: https://sanctionsnews.bakermckenzie.com/japan-introduces-further-sanctions-against-russia-8/ (Accessed: 1 June 2023).

[99] European Commission. (2023). 'EU adopts 11th package of sanctions against Russia for its continued illegal war against Ukraine'. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3429 (Accessed: 26 June 2023).

[100] Perkins, R. & Bowles, A. (2023). 'EU adopts new sanctions package to clamp down on illicit Russian oil exports'. S&P Global. Available at: https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/062323-eu-adopts-new-sanctions-package-to-clamp-down-on-illicit-russian-oil-exports (Accessed: 23 August 2023).

[101] Schulze, M. and Kerttunen, M. (2023). 'Cyber Operations in Russia's War against Ukraine'. Stiftung Wissenschaft und Politik. Available at: https://www.swp-berlin.org/publikation/cyber-operations-in-russias-war-against-ukraine (Accessed: 7 August 2023).

[102] Boutin,J.M. (2023). 'ESET APT Activity Report Q4 2022–Q1 2023'. ESET. Available at: https://www.welivesecurity.com/2023/05/09/eset-apt-activity-report-q42022-q12023/ (Accessed: 7 August 2023).

[103] Microsoft Threat Intelligence. (2023). 'Cadet Blizzard emerges as a novel and distinct Russian threat actor'. Microsoft. Available at: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/ (Accessed: 7 August 2023)

[104] Amaury G., Charles M. and Threat & Detection Research Team. (2023). 'Following NoName057(16) DDoSia Project's Targets'. Sekoia. Available at: https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/ (Accessed: 7 August 2023).

[105] Mandiant. (2023). 'M-Trends 2023'. Mendiant. Available at: https://www.mandiant.com/m-trends (Accessed: 7 August 2023).

[106] CyberPeace Institute. (2022) Cyber Attacks in Times of Conflict Platform #Ukraine. Available at: cyberconflicts.cyberpeaceinstitute.org (Accessed: 7 April 2023)

[107] Ibid

[108] CyberPeace Institute. (2022) FAQ Data & Methodology. Available at: https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (Accessed: 2 May 2023).

[109] Ibid

[110] 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)