CyberPeace Institute

Quarterly Analysis Report
Q1 January to March 2023

Cyber Dimensions
of the Armed Conflict in Ukraine

TABLE OF CONTENTS

Background

January 2022 - March 2023

Since the February 2022 Russian military invasion of Ukraine, the CyberPeace Institute has been documenting cyber incidents in the context of the Russian-Ukrainian war including incidents in Ukraine, the Russian Federation and other countries notably those targeting and/or impacting civilians, civilian objects (including private companies) and infrastructure ensuring the delivery of essential services to civilians.Between January 2022 and March 2023, the CyberPeace Institute has documented a total of 1,537 cyber incidents conducted by 91 different threat actors. The data is available through the Cyber Attacks in Times of Conflict Platform[1] #Ukraine.

360
incidents against entities in
Ukraine

The threat actors that were the most active in targeting Ukrainian entities were the hacktivist collectives *People's CyberArmy* (99), *NoName057(16)* (40) and *Anonymous Russia* (26). *Sandworm* (19) and *DEV-0586* (12) have had the most attacks attributed to them among Russia's state-sponsored threat actors.

Top 5 targeted sectors:

- Public administration (81)
- Financial (43)
- Media (34)
- ICT (33)
- Transportation (18)
  & Energy (18)

241
incidents against entities in the
Russian Federation

The most active threat actors conducting attacks against Russian entities were the *IT Army of Ukraine* (59), the global hacktivist collective *Anonymous* (49) and *Anonymous Italia* (37).

Top 5 targeted sectors:

- Financial (42)
- Public administration (39)
- Media (25)
- ICT (21)
- Energy (18)

936
incidents against entities in
other countries

The most active threat actors conducting attacks were the hacktivist collectives *NoName057(16)* (431), *Anonymous Russia* (100) and *KillNet* (88).

Top 3 targeted sectors:

- Public administration (284)
- Transportation (161)
- Financial (93)

Top 3 targeted countries:

- Poland (173)
- Latvia (92)
- United States of America (83)

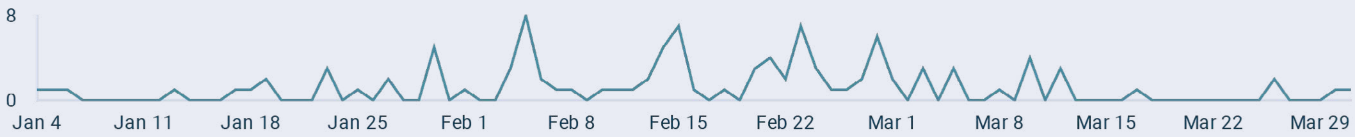
The remainder of this report focuses on the incidents documented by the CyberPeace Institute in the first quarter of 2023; January 1 to March 31, 2023. Of note during this period, is that February 24, 2023 marked the one-year anniversary of Russia's recent military invasion of Ukraine.

Trends and Emerging Issues Q1 2023

Ukraine

Incidents	Sectors	Threat Actors
104	17	17
↑ 36.8%	↑ 6.3%	↑ 13.3%

Daily evolution of cyber incidents impacting entities in Ukraine [Jan - Mar 2023]



© CyberPeace Institute 2023

Trends

- DDoS attacks account for 87.5% of all incidents. The most targeted sectors were the financial (19), public administration (19) and the ICT (10).
- 12 Ukrainian nonprofit organizations were targeted in 5 DDoS attacks or campaigns in February 2023.

Top 10 sectors impacted in Ukraine [Jan - Mar 2023]

	Sector	Incidents ▾	% Δ
1.	Financial	19	46.2% ↑
2.	Public administration	19	58.3% ↑
3.	ICT	10	66.7% ↑
4.	Manufacturing	10	400.0% ↑
5.	Trade	7	40.0% ↑
6.	Unknown	7	40.0% ↑
7.	Energy	5	66.7% ↑
8.	Media	5	25.0% ↑
9.	Nonprofit	5	∞
10.	Other service	5	400.0% ↑

© CyberPeace Institute 2023

- Five incidents have been attributed to Russian state-sponsored threat actors including three campaigns attributed to Sandworm (attributed[3] to Russia's foreign military intelligence - GRU):
  - CaddyWiper wiper malware used against Ukrainian public administration[4],
  - SwiftSlicer malware used against Ukrainian private organizations[5],
  - CaddyWiper and ZeroWipe wiper malware used against a Ukrainian national news agency[6].
- And two cyberattacks attributed to DEV-0586[7]:
  - Graphiron information stealing malware deployed against Ukrainian targets[8],
  - CERT-UA discovered a malware, installed through a web shell, which allowed for the modification of content on the webpage, gaining remote access and gathering data from the servers of an unknown Ukrainian public administration.[9]

Emerging Issues

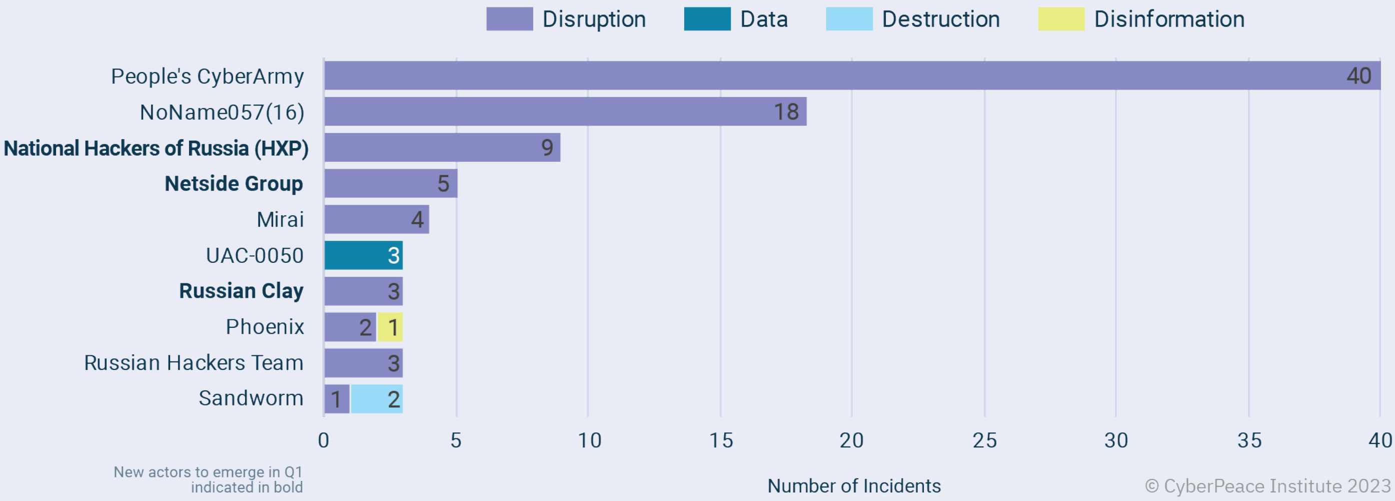
Latest malware

- Researchers from the cybersecurity company ESET[10] discovered the use of a new wiper malware dubbed "SwiftSlicer", attributed to Russia's state-sponsored threat actor *Sandworm*[11]. The wiper malware, found on the networks of an unknown Ukrainian organization on January 25, was written in GO language and took control of the victim's Active Directory environment.
- Symantec's Threat Hunter Team[12] discovered the use of a new information-stealing malware dubbed "Graphiron" against the networks of unknown Ukrainian organizations. The cybersecurity company attributed the new malware to the Russian state-sponsored threat actor *DEV-0586*[13]. The malware was written in GO language and is designed to harvest information from a targeted device, including system information, credentials, screenshots and files.
- The Computer Emergency Response Team of Ukraine[14] discovered the reappearance of a destructive wiper malware dubbed "CaddyWiper". The CyberPeace Institute has been monitoring the deployment of the wiper malware, attributed to Russia's state-sponsored threat actor *Sandworm*, since March 2022.[15] The wiper targets Windows-based devices. The latest deployment of the wiper malware took place at the end of January against Ukraine's National Information Agency "Ukrinform".

Notable threat actor activity

- There was a 207.6% increase in incidents attributed to the hacking collective *People's CyberArmy*.
- The CyberPeace Institute identified three new hacktivist collectives targeting Ukrainian entities:
  - *National Hackers of Russia* who committed 9 DDoS attacks against entities across 5 sectors including nonprofit (3), public administration (2) and financial (2).
  - *Netside Group* who committed 5 DDoS attacks against entities across 3 sectors (public administration - 3; financial - 1; ICT - 1).
  - *Russian Clay* who committed 3 DDoS attacks against entities across the financial, manufacturing and other sectors.

Top 10 threat actors targeting entities in Ukraine [Jan - Mar 2023]



National Hackers of Russia

> A pro-Russian threat actor tracked through Telegram. The group had two Telegram channels where they reported on their alleged DDoS attacks against targets in Ukraine and other countries supporting Ukraine. The group first appeared in late January 2023 (channel created January 20, 2023) and was active until early March, when both Telegram channels were permanently deleted. According to Radware[16] (a cybersecurity company), *National Hackers of Russia* belonged to the *KillNet* hacktivist collective and have responded to calls to act alongside *Killnet*.[17] As both Telegram channels have since been closed, the CyberPeace Institute is still investigating whether or not the group continues to operate. However, while active, the group mostly targeted organizations in Ukraine and Lithuania.

Netside Group

> A pro-Russian threat actor tracked through Telegram. The *Netside Group* channel was created on November 23, 2022, but has been active since January 23, 2023. *Netside Group* is a pro-Russian hacktivist collective that finances its own DDoS attacks against organizations in Ukraine and other countries supporting Ukraine.[18] *Netside Group* is likely linked to the *KillNet* hacktivist collective, as they repost messages from the *KillNet* Telegram channel and have also participated in DDoS attacks alongside *KillNet*.[19] Since the CyberPeace Institute started tracking the threat actor, the group has primarily targeted organizations in Ukraine, the United States of America and Germany.

Russian Clay

> A pro-Russian threat actor tracked through Telegram. The group moves from channel to channel with the first channel tracked by the CyberPeace Institute created on February 7, 2023. The second channel was created on March 30, 2023. They recently created a third channel on April 7, 2023. Like other pro-Russian hacktivist collectives, *Russian Clay* primarily uses DDoS attacks against targets in Ukraine and other countries supporting Ukraine. Although the group is in contact with the *KillNet* hacktivist collective[20], they are likely not officially part of it. However, *Russian Clay* has joined forces with another group, *Russian Hackers Community*.[21] *Russian Clay* has also published a propaganda video on Youtube addressing Russian citizens and Ukrainians.[22] Since the CyberPeace Institute started tracking *Russian Clay*'s activities, this group has targeted Ukraine the most, followed by the United States of America.

In February 2023, the month that marked the one-year anniversary of the Russian Federation's recent military invasion of Ukraine, pro-Russian threat actors conducted 62% of all recorded incidents for the first quarter of 2023. This one-year anniversary is the likely reason for the increase in the activities of pro-Russian threat actors, such as the hacktivist collective *People's CyberArmy* activities and the appearance of several other new hacktivist collectives, such as *National Hackers of Russia*, *Netside Group* and *Russian Clay*. At this stage there is little publicly available information to indicate any significant disruption resulting from the recorded incidents which were predominantly DDoS attacks.

The CyberPeace Institute documented five possible incidents against Ukrainian nonprofit organizations in February 2023. The pro-Russian hacktivist collective *National Hackers of Russia* claimed responsibility for three DDoS campaigns, targeting ten Ukrainian humanitarian funds. Whilst *People's CyberArmy* claimed responsibility for the two other attacks; one DDoS attack against a Ukrainian nonprofit union focusing on education development and another DDoS attack against a Ukrainian NGO providing services to the Ukrainian military. All of the processed incidents against Ukrainian nonprofit organizations in Q1, 2023, targeted their websites. Besides the disrupted connectivity to the websites, there is currently no other information available on the additional impacts of these incidents.

Cyberattacks on Ukrainian entities [Q1 2023 vs Q4 2022]

+36.8%
cyberattacks

+13.3 %
unique threat actors

+46.2 %
cyberattacks on the financial sector

Other notable incidents in Ukraine

Disruption

March 17, 2023

A confirmed DDoS campaign against several online resources of Ukraine's public administrations leading to the inaccessibility of these resources.[23]

Data

March 12, 2023

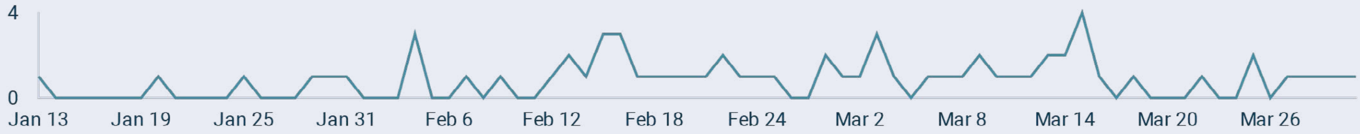
A confirmed hack and leak operation against a Ukrainian video game developer. The pro-Russian threat actor, *Vestnik TSS*, claimed responsibility for the attack and threatened to use the stolen data for blackmail and intimidation.[24] The hack and leak operation was allegedly conducted in response to a perceived hostility towards "Russian and Belarusian players" from the Ukrainian video game developer.

Trends and Emerging Issues Q1 2023

Russian Federation

Incidents	Sectors	Threat Actors
65	18	6
↑ 150%	↑ 63.6%	↓ -25%

Daily evolution of cyber incidents impacting entities in the Russian Federation [Jan - Mar 2023]



© CyberPeace Institute 2023

Trends

- The most targeted sectors in Q1 of 2023 were the financial (15), transportation (9) and media (6).

Top 5 sectors impacted in the Russian Federation [Jan - Mar 2023]

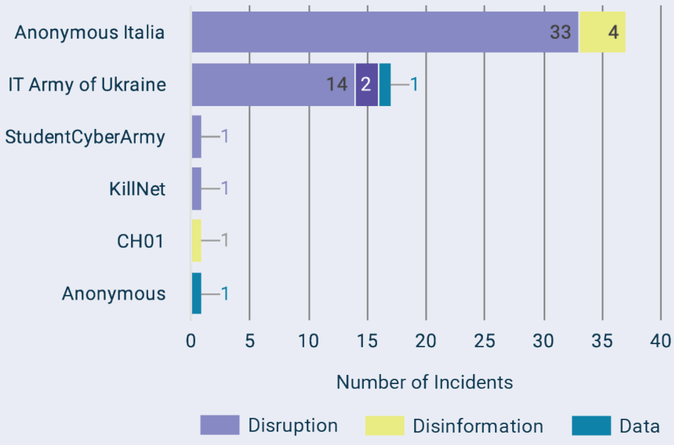
	Sector	Incidents ▾	% Δ
1.	Financial	15	275.0% ↑
2.	Transportation	9	800.0% ↑
3.	Media	6	500.0% ↑
4.	Administrative / Support	5	∞ -
5.	ICT	5	-16.7% ↓

- Several cyber-enabled information operations, conducted by unknown threat actor(s), took place against Russian TV channels and radio stations, likely seeking to influence Russia's information space. The operations consisted of infiltrating the servers of Russian targets and releasing false information on air alerts and aerial bombardment against Russian targets.
- This quarter saw a decrease in the number of threat actors conducting cyberattacks against organizations in the Russian Federation.

Notable threat actor activity

- The CyberPeace Institute has been monitoring a new threat actor, *Anonymous Italia*, since the start of 2023. *Anonymous Italia* has increased its activities against entities in the Russian Federation since the start of 2023; between July and December 2022 they claimed to have conducted 36 cyberattacks against Russian entities compared to 37 cyberattacks in Q1 2023 (33 DDoS and 4 defacements attacks).

Threat actors targeting entities in the Russian Federation [Jan - Mar 2023]



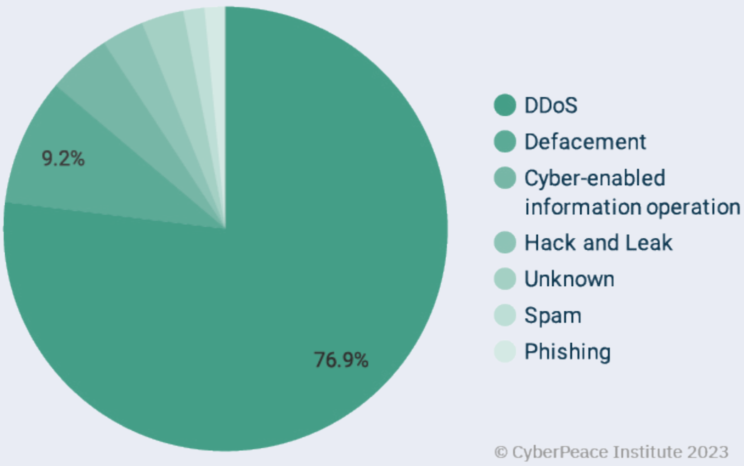
© CyberPeace Institute 2023

Anonymous Italia

> The CyberPeace Institute has begun to track a group allegedly representing an Italian faction of the hacktivist collective *Anonymous*.The group *Anonymous Italia* carries out mainly DDoS attacks and defacement operations against various targets in different regions of the world. The group, which created its Telegram channel in July 2022, is also present on Twitter and has its own website,[25] carries out mainly DDoS attacks and defacement operations against various targets in different regions of the world. In the context of the Russian invasion of Ukraine, the group has come out supporting Ukraine and thus targets Russian organizations. Many of the alleged attacks during this quarter are against Russian companies that have alleged ties to a specific Russian Oligarch. [26]

The CyberPeace Institute noted a 150% increase of cyberattacks against entities in the Russian Federation despite a 25% decrease in the number of unique threat actors targeting Russian organizations. This increase in malicious cyber activities correlates with a slight increase in the activities of the *IT Army of Ukraine*, and the discovery of a new threat actor – *Anonymous Italia*. Furthermore, the increased targeting of Russian organizations correlates with a 284.6% increase in DDoS activities.

Types of cyber incidents targeting entities in the Russian Federation



The CyberPeace Institute also discovered a trend consisting of several cyber-enabled information operations directly impacting the citizens of the Russian Federation. Unknown pro-Ukrainian threat actor(s) conducted cyberattacks against Russian TV channels and radio stations and released false air alerts of missile strikes on the territory of the Russian Federation. The threat actor(s) is highly likely to be aiming to influence the Russian information space by increasing perceptions of proximity of Russian civilians to the conflict, and thus aiming to weaken support for the government amongst the general population.

Notable incidents in the Russian Federation

Disruption

March 1, 2023

KillNet claimed responsibility for a confirmed DDoS attack against a Russian news media website. The hacktivist collective deemed the target as a "foreign agent" after the news media website had published false information about the group.[27] [28]

March 14, 2023

A confirmed DDoS attack against the website and mobile application of a Russian bank. According to the target, the attack affected the bank's mobile and Internet banking, as well as logging into the website.[29]

Disinformation and Propaganda

January 25, 2023

A confirmed defacement operation against all Russian federal TV channels broadcasting in the Belgorod Oblast. The operation replaced the content of the TV channels with a legitimate appeal made by Ukraine's President.[30]

February 22, 2023

A confirmed cyber-enabled information operation using the servers of a number of commercial radio stations in different regions of the Russian Federation to air information about a false air alert and the threat of a missile strike. [31]

February 28, 2023

A confirmed cyber-enabled information operation using the servers of Russian radio stations and television channels to air information about a false air alert.[32]

March 6, 2023

A confirmed disinformation campaign consisting of messages warning of a false air raid sent to Russian citizens residing in border regions.[33]

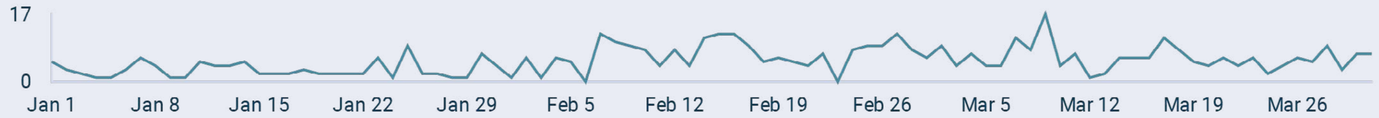
March 9, 2023

A confirmed cyber-enabled information operation using the servers of Russian regional radio stations and television channels to air information about a false air alert.[34]

Trends and Emerging Issues Q1 2023
Other Countries

Incidents	Countries	Sectors	Threat Actors
475	36	21	13
↑ 98.7%	↑ 5.9%	↑ 31.3%	↑ 8.3%

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

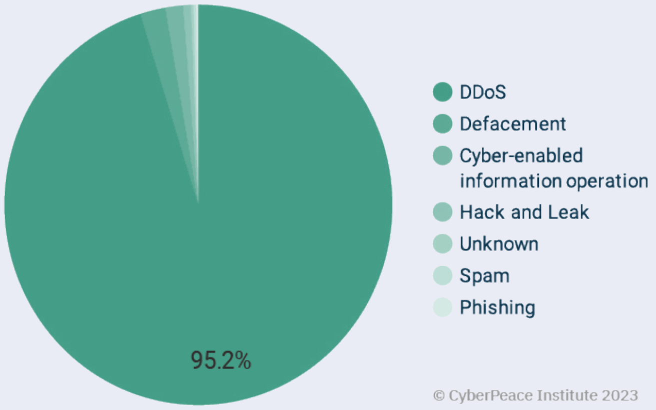


© CyberPeace Institute 2023

Trends

- The CyberPeace Institute has documented 475 incidents in Q1 of 2023, compared to 461 incidents documented throughout the whole of 2022. The majority of incidents recorded are DDoS attacks (95.2%).

Types of cyber incidents targeting entities outside the two belligerent states [Jan - Mar 2023]



© CyberPeace Institute 2023

- The most targeted sectors were the public administration (139), transportation (74) and manufacturing (51).
- Entities in Poland (73), the United States of America (47) and Germany (44) were targeted the most in Q1 of 2023. There was a significant increase in attacks against Germany, Sweden, Slovakia, Japan, Spain, Italy, Denmark and Norway.

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

	Countries	Incidents	% Δ
1.	POLAND	73	4.3% ↑
2.	UNITED STATES	47	114 % ↑
3.	**GERMANY**	44	**1,367%** ↑
4.	LITHUANIA	33	100% ↑
5.	CZECHIA	31	107% ↑
6.	LATVIA	30	-6 % ↓
7.	UNITED KINGDOM	25	108 % ↑
8.	ESTONIA	22	100 % ↑
9.	**SWEDEN**	21	**950%** ↑
10.	**SLOVAKIA**	20	**1,900%** ↑
11.	**JAPAN**	14	**∞**
12.	**SPAIN**	14	**1,300%** ↑
13.	**ITALY**	14	**∞**
14.	**DENMARK**	13	**∞**
15.	ROMANIA	11	267% ↑
16.	**NORWAY**	10	**900%** ↑

© CyberPeace Institute 2023

Notable threat actor activity

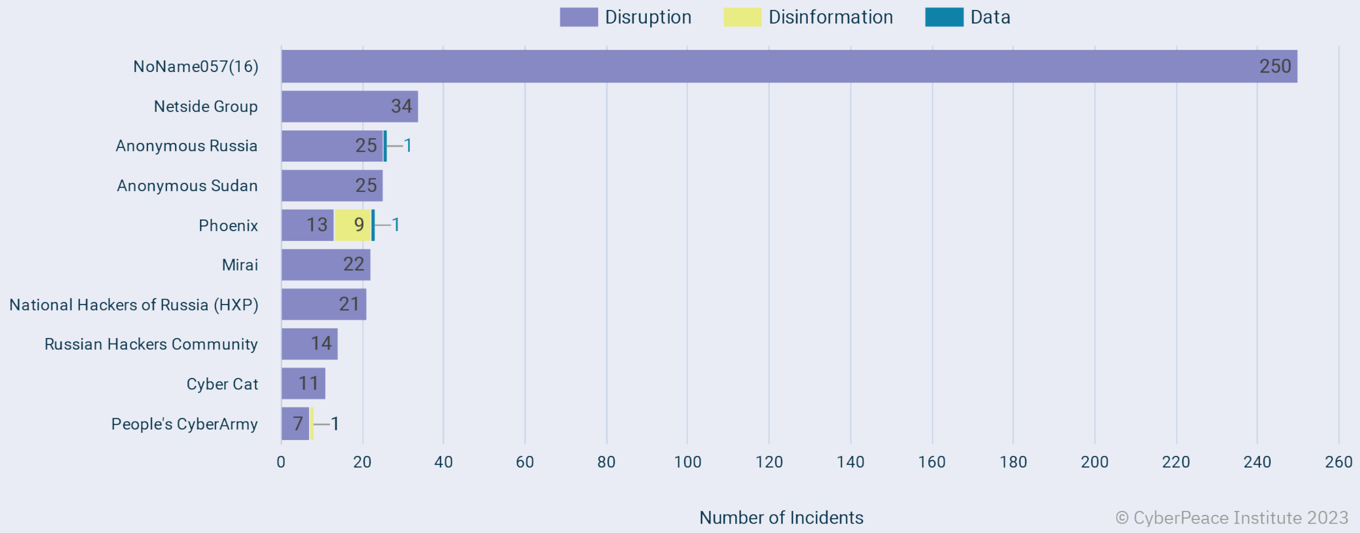
- *Anonymous Sudan* claimed responsibility for 25 DDoS attacks against 5 countries and 8 sectors in Q1 2023. In the context of the ongoing armed conflict, the threat actor has primarily targeted the United States of America (14), the Netherlands (5) and Germany (4). The threat actor targets the health (8), public administration (4), ICT (4), transportation (3) and financial (3) sectors the most.

Anonymous Sudan

> A pro-Russian threat actor tracked by the CyberPeace Institute through its Telegram channel, created on January 18, 2023. The group has been conducting DDoS attacks since January 23, 2023, on Western countries that support Ukraine and against Western countries deemed Islamophobic by the threat actor group. The group claims to be Sudanese, not Russian.[35] However, in February 2023, the group stated they were now officially a part of the *KillNet* collective.[36] According to Truesec (a cybersecurity company)[37], this group is not an official *Anonymous* collective but was created as a Russian information operation to harm Sweden's NATO integration. Moreover, Truesec states that the threat actor uses paid infrastructure for its DDoS attacks suggesting that they are not simple hacktivists but are being financed.[38]

During this quarter the most active pro-Russian threat actor has been *NoName057*(16), with a noted increase of 133.6% in its activities compared to the previous quarter. The second most active pro-Russian threat actor is a newly documented hacktivist collective *NetSide Group*. The CyberPeace Institute noted a 60.3% decrease in the activities of *Anonymous Russia* compared to the previous quarter.

Top 10 threat actors targeting entities outside the two belligerent states [Jan - Mar 2023]

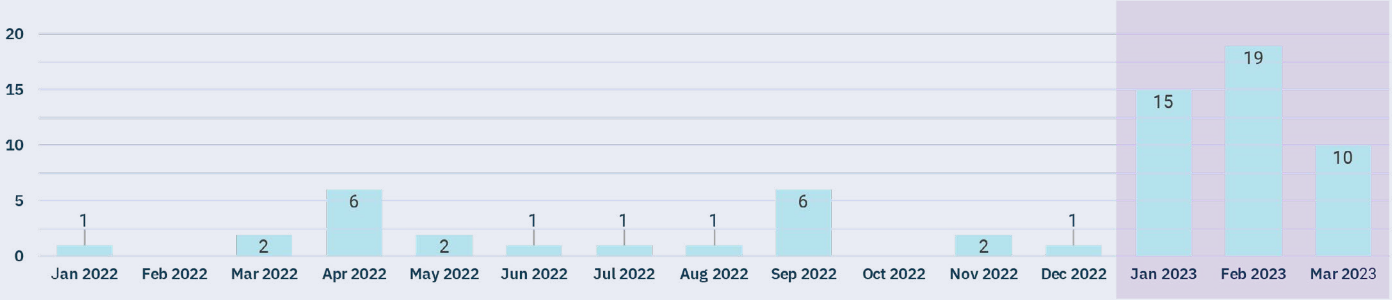


The increase in malicious activities in Q1 2023 is highly likely to be associated with the increased support for Ukraine, including the announcements[39] of several countries of increased military support in the form of heavy weaponry. The primary targeting of entities in Poland, the United States of America and Germany by pro-Russian threat actors is highly likely to be associated with the targeted countries' military support for Ukraine.[40] The significant increase in attacks against Spain, Sweden and Norway is likely associated with the countries' military support for Ukraine (see 'Military aid' section).

Germany – a significant target

For the first time since the hostilities launched by Russia in 2022, the CyberPeace Institute noted a sharp increase in malicious cyber activities against German organizations. Germany's manufacturing (11), health (7) and public administration (7) sectors were targeted the most this quarter, mainly by *NoName057(16)* (9) and *Phoenix* (9). It is highly likely that Germany's announcement that it would send Leopard 2 tanks to Ukraine[41] led to a sharp increase in targeting by pro-Russian threat actors, particularly against the manufacturer of the tanks.

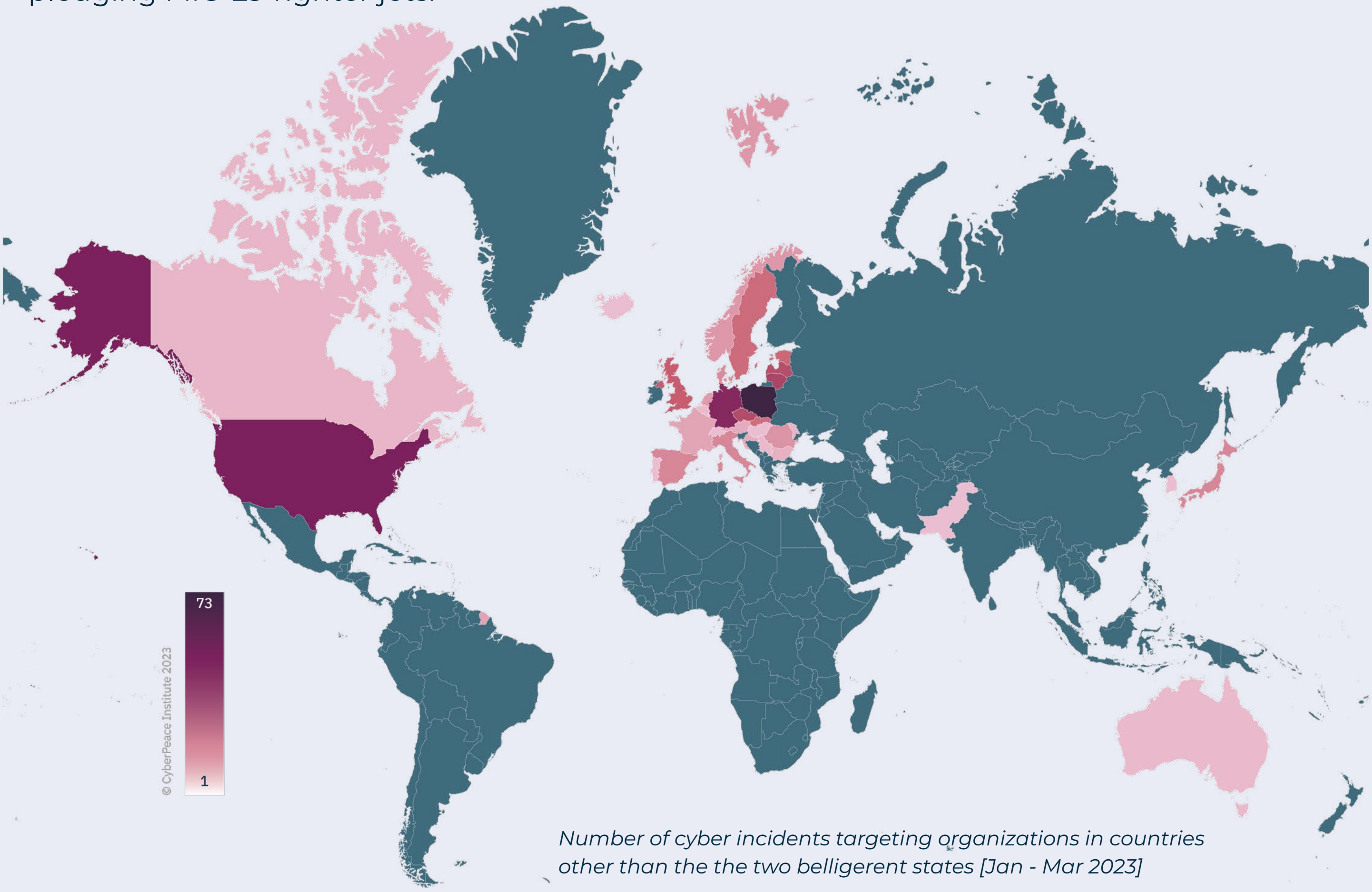
Cyber incidents targeting entities in Germany illustrating the increase in attacks in Q1 2023 [Jan 2022 - Mar 2023]



© CyberPeace Institute 2023

Poland – pro-Russian hacktivists' main target

For a second consecutive quarter, Poland remains the non-belligerent country most attacked by pro-Russian threat actors. Poland's public administration (28), transportation (10) and manufacturing (9) sectors were targeted the most, mainly by *NoName057(16)* (38) and *Anonymous Russia* (10). The targeting of Polish entities is highly likely associated with the country's position as one of Ukraine's leading supporters,[42] providing Ukraine with tanks [43] and pledging MiG-29 fighter jets.[44]



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

Notable incidents

Data

March 1, 2023

In an attempt to target EU countries aiding Ukraine, *APT29*, a Russian state-sponsored threat actor,[45] sent spear phishing emails with information concerning the Polish Ambassador's visit to the United States.

Another lure used in this campaign was the mirroring of real information exchange systems used by EU nations. The emails contained malware allowing the threat actor to drop files on the victim's machine and move through the victim's network.[46]

Disruption

January 28, 2023

Anonymous Sudan claimed responsibility[47] [48] [49] for a confirmed DDoS campaign against 19 Dutch hospitals. According to sources,[50] the threat actor successfully disrupted the functioning of the hospitals' websites.[51]

March 27, 2023

NoName057(16) claimed responsibility[52] [53] for confirmed DDoS attacks against the websites of the French Senate and the National Assembly. The threat actor successfully disrupted the functioning of the targets' websites.[54]

Harm and Impact

The Russian Federation has been conducting information operations and campaigns targeting the populations in Ukraine and other countries supporting Ukraine. This forms part of its 'information-technological warfare' or 'information confrontation' approach. By disseminating false or misleading information, it is likely the Russian Federation is aiming to decrease popular support for governments backing Ukraine.

Many Ukrainian allied countries, especially those in Western Europe, have begun to experience what is called war fatigue.[55]

Fighting Western war fatigue has even become a central challenge for Ukraine, according to Ukrainian Deputy Foreign Minister Andrij Melnyk.[56] This feeling may be due to the rising cost of living, inflation and overall economic hardship, which could be a consequence of the ongoing armed conflict or other factors such as the COVID-19 pandemic. Thus, to sway the opinion of different populations in its interest, the Russian Federation aims to exacerbate these feelings of war fatigue. Russian information operations target populations living in a broad range of countries to influence them to pressure their governments to either stop supporting - financially and/or militarily - Ukraine, or to persuade Ukraine to negotiate with the Russian Federation to put an end to the war.[57]

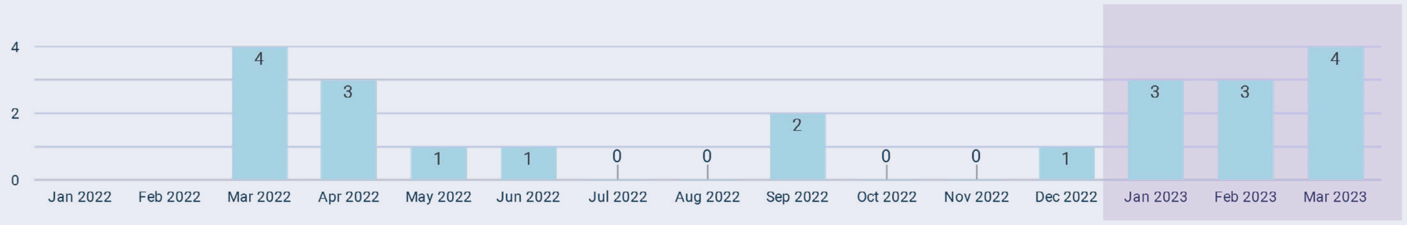
Threat actors taking advantage of the apparent war fatigue is likely to be the reason for the increase in cyber incidents by pro-Russian threat actors against countries which are supporting Ukraine, as they have conducted more attacks in Q1 of 2023 than throughout 2022. While DDoS attacks are malicious activities with usually short-term impact on the targets, they can successfully be used to have an impact on the general population.[58] The societal impact of DDoS attacks derives from the disruption of people's daily lives. People may rely on specific online resources for their day to day lives and livelihood; therefore, their unavailability may directly impact the population financially and psychologically. Furthermore, members of the public are more likely to react to the effects of a cyberattack rather than the cyberattack itself. [59]

As RecordedFuture argues "Hacktivism has become symbolic in the public's perception of the "cyberwar" raging parallel to Russia's war against Ukraine".[60] Coupled with all other problems in the daily lives of the countries' populations supporting Ukraine, the increase of malicious cyber activities by pro-Russian threat actors is likely to increase the perception of proximity to the conflict, exacerbating the feelings of "war fatigue".

However, not only are pro-Russian threat actors conducting information operations. The series of cyber-enabled information operations, conducted by unknown pro-Ukrainian threat actor(s), consisting of false air alerts about incoming aerial bombardments, also highly likely aiming to increase the perception of proximity of the conflict to the Russian Federation's civilian population.

These operations could potentially have an immediate psychological impact on the civilian population, leading to feelings of fear and anxiety.

Disinformation and propaganda incidents targeting entities in the Russian Federation illustrating the increase in attacks in Q1 2023 [Jan 2022 - Mar 2023]



© CyberPeace Institute 2023

Continued involvment of civilians

A persistent concern in relation to the cyber dimensions of the armed conflict in Ukraine is the involvement of private persons or groups in carrying out malicious activities. Such an involvement could be determined as a direct participation in the hostilities for which actors could lose their protections from attack (as civilians), and could be held accountable for any violations of international law. On the one hand, a Newsweek article,[61] on a pending Ukrainian draft cyber law, raised several questions on the future status of the *IT Army of Ukraine*. Claiming to have received a written response from Nataliya Tkachuk, Secretary of Ukraine's National Coordination Center for Cybersecurity, the new Ukrainian draft law on the creation and functioning of cyber forces reportedly could pave the way for volunteers such as those in the IT Army of Ukraine to be absorbed into Ukraine's reserve forces. This would go some way to clarifying the legal status, in particular under which legal framework they are operating and the obligations that they must respect.

This would still leave questions with regard to the conduct of other private persons or groups operating from other countries who are conducting malicious cyber activities in relation to the conflict in the name of an "IT Army", who could potentially be determined to be participating in the hostilities and subject to legal proceedings.

Furthermore, the CyberPeace Institute notes a probable continued involvement of Russian-speaking citizens in malicious cyber activities. *KillNet*'s forum, one of the most prominent pro-Russian hacktivist collectives, became more popular throughout Q1. The forum provides its registered users access to a multitude of educational materials for conducting malicious cyber activities, including DDoS attacks and social engineering. The forum's accessibility and provision of such content make it a significant threat. While currently the creation, use and distribution of malware are illegal in the Russian Federation, there are reportedly plans for an amendment to the legislature, releasing threat actors acting in the interest of the Russian Federation from liability, as put forward by Alexander Khinshtein, member of the State Duma and head of the Committee on Information Policy.[62]

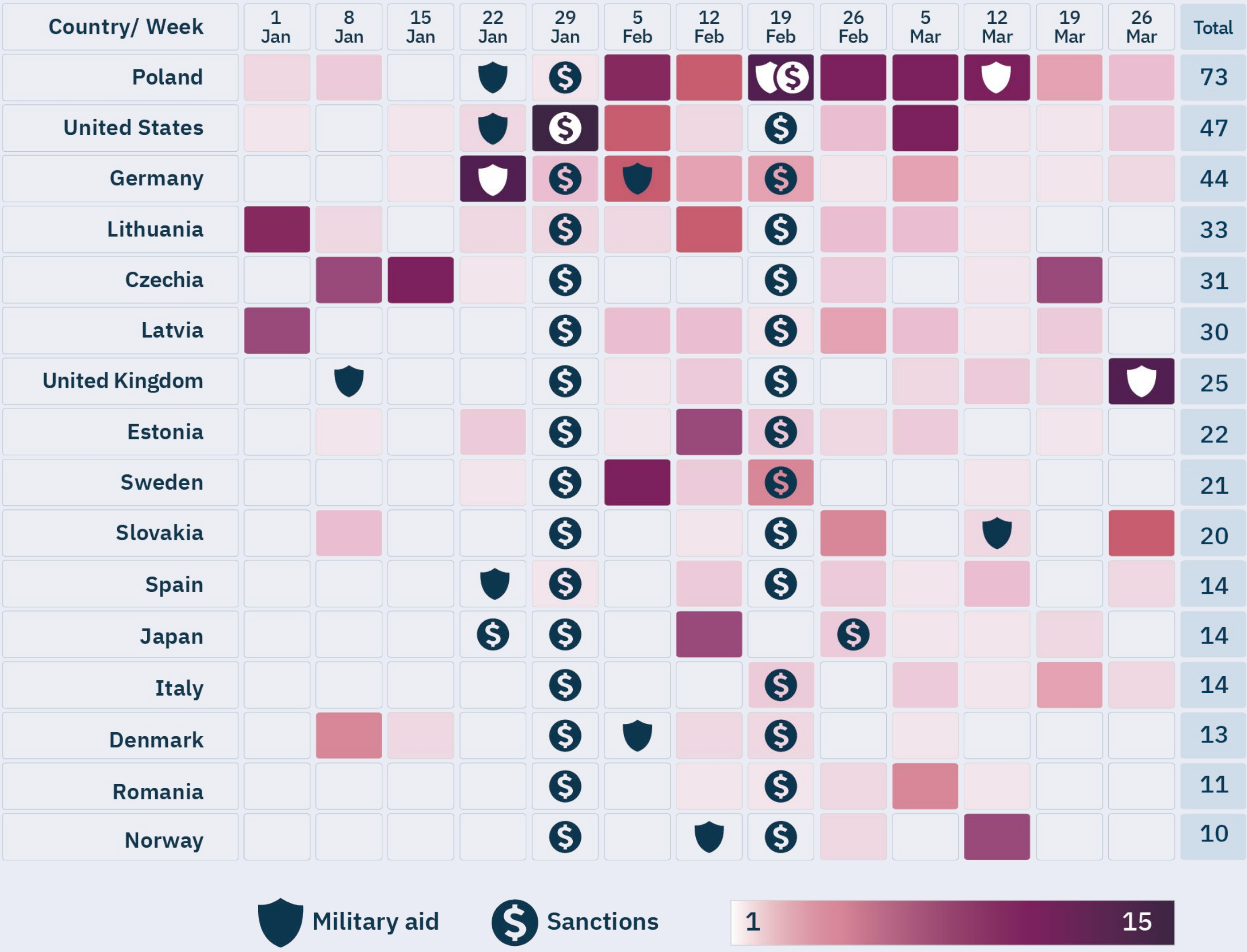
Wider Contextual Considerations

Events

During the first quarter of 2023 there were at least four notable events that took place at an international level. Shortly before the one year anniversary of the Russian Federation's recent military invasion of Ukraine,[63] on February 20, 2023, the President of the United States of America, Joseph Biden, visited Kyiv,[64] the capital of Ukraine. Then on March 17, 2023, two key events took place. Firstly, Türkiye's President, Recep Erdoğan, announced that Türkiye will ratify Finland's request to join NATO.[65] Secondly, the International Criminal Court issued an arrest warrant for the Russian Federation's President, Vladimir Putin and Children's Rights Commissioner for the President of the Russian Federation Maria Lvova-Belova.[66] On the next day, on March 18, Vladimir Putin visited the Russian-occupied territories of Crimea[67] and Mariupol.[68]

The CyberPeace Institute, however, has not documented any occurrence of cyber incidents that could potentially be related to those four key events.

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



© CyberPeace Institute 2023

Sanctions and Statements

For the first quarter of 2023, many countries have shifted focus on tightening previously imposed sanctions. For example, on February 1, 2023, the United States of America imposed new sanctions against entities related to a "sanctions evasion network supporting the Russian military-industrial complex".[69] On February 4, 2023, the European Council, the Price Cap Coalition of the G7 and Australia set price caps for Russian petroleum products to go along with the previous oil price cap on Russian crude oil implemented in December 2022.[70] On the one year anniversary of the war, the United States of America announced new sanctions targeting the metals and mining sector of the Russian Federation,[71] along with the United Kingdom of Great Britain and Northern Ireland which announced sanctions on "every item Russia is using on the battlefield".[72] On February 25, 2023, one year after the beginning of the Russian Federation's 2022 full-scale invasion of Ukraine, the European Union adopted its tenth package of sanctions against the Russian Federation with the goal of amending and broadening the scope of previously implemented sanctions.[73] However, in order for sanctions to be fully effective, there must be full "alignment and enforcement".[74] Japan also imposed new sanctions against the Russian Federation on two separate occasions this quarter, specifically on January 27 [75] and February 28.[76]

Military Aid

Since the start of 2023, at least 13 countries pledged to provide tanks as military aid to Ukraine. The United Kingdom of Great Britain and Northern Ireland was one of the first countries to agree to transfer tanks to Ukraine, with an announced transfer of 14 Challenger tanks communicated on January 14.[77] Thereafter, until the end of January, more countries announced decisions to donate tanks to Ukraine. The United States of America pledged to deliver 31 M1A1 Abrams tanks.[78] Germany followed the international call and announced that it would donate Leopard 2 tanks.[79] Canada and Spain also announced they would support Ukraine with German-made Leopard 2 tanks at the end of January.[80] [81] Promises for tanks continued throughout February with Portugal pledging Leopard tanks to Ukraine on February 4, 2023.[82] On February 7, the Dutch Ministry of Defense communicated that the Netherlands, along with Denmark and Germany, would purchase 100 Leopard 1A5 main battle tanks for Ukraine.[83] On February 14, Norway communicated their newest tanks-package for Ukraine, pledging to donate 8 tanks.[84] Those tanks were delivered by March 20, 2023.[85] By the end of February, Finland and Sweden also announced they would provide Ukraine with Leopard tanks.[86] [87]

Poland, being one of Ukraine's strongest allies and having supported Ukraine with battle tanks since April 2022,[88] announced it would continue sending more tanks to Ukraine,[89] with the first Leopard tanks having been delivered by Poland on the one-year anniversary of the recent military invasion of Ukraine.[90] On March 16, Poland was also the first NATO member state to announce it would send MiG-29 fighter jets – to Ukraine.[91] A day later, on March 17, Slovakia also declared it would assist Ukraine by sending MiG-29 fighter jets.[92]

Based on the timing of the military announcements and cyberattacks, the CyberPeace Institute considers it unlikely that the cyberattacks against the Netherlands, Canada, Denmark, and Portugal were related to those announcements. On the other hand, cyberattacks against the other countries who've made public announcements to provide military aid in support of

Ukraine are highly likely to have triggered retaliatory cyberattacks. For example, the increase in attacks against Norwegian entities is highly likely associated with the weapons' delivery, as all documented incidents occurred in March. Polish entities were highly likely targeted the most because of the country's strong support for Ukraine, with the majority of attacks occurring the day after Poland announced that the first Leopard tanks had been delivered.

Since the start of 2023, the United States of America has been the second most targeted non-belligerent country, highly likely associated with the promises for A1M1 Abrams tanks. Germany is the third most targeted country, with the German manufacturing sector being attacked the most after Germany declared it would support Ukraine with Leopard tanks. The United Kingdom of Great Britain and Northern Ireland was also targeted by pro-Russian threat actors, with a steady increase of the attacks occurring throughout March, peaking at the end of the month. The increase in attacks coincided with the United Kingdom's Ministry of Defense announcing the completion of a training program for a group of Ukrainian soldiers. The soldiers reportedly traveled to the United Kingdom in January and received instructions on operating and fighting with Challenger 2 tanks.[93] [94] Lastly, after Slovakia became the second country to promise to donate fighter jets MiG-29, pro-Russian threat actors increased the targeting of Slovak entities. The CyberPeace Institute notes that some increases in cyberattacks against entities in particular countries have not been associated with any notable economic or geopolitical activities whilst others appear to be connected with geopolitical statements made by government officials about the ongoing armed conflict itself rather than specific announcements relating to economic sanctions or military aid.

Other Research

During the first quarter of 2023 SentinelOne published research into the activities of one of the most active pro-Russian threat actors *NoName057*(16).[95]

Most of the published research into the cyber dimensions of the conflict during this first quarter of 2023 focused on analyzing the malicious cyber activities for the one-year anniversary of the 2022 military invasion. Some of the organizations, which published a summary and impact of the malicious cyber activities, throughout 2022 were:

- State Service of Special Communications and Information Protection of Ukraine[96] - On March 8, 2023, the SSSCIP of Ukraine published a report on Russian cyberattacks on Ukraine from 2022. The report, which compares Russian threat actor activity from the second half of 2022 to the first half, analyzes different Russian groups, discussing their motivation, methods and tools.
- RecordedFuture[97] - Recorded Future's report discussed the impact of the conflict in Ukraine on the cybercriminal ecosystem. According to the researchers, the cybercriminal ecosystem in the Commonwealth of Independent States (CIS) has been damaged due to divergent views on the conflict in Ukraine. Additionally, the researchers note that the hacktivist collectives are vital for certain information operations.
- Computer Emergency Response Team of the European Union - CERT-EU[98] analyzed 806

cyberattacks associated with the conflict in Ukraine, outlining the timeline of cyber operations in three phases: preparation (until February 24, 2022), fast and furious (from February 24, 2022 until March 2022), and sustained phase with ups and downs (until February 24, 2023). According to CERT-EU, the most targeted EU countries were Poland, Latvia, Estonia, and Lithuania, while the most targeted sectors were the public administration, defense, ICT, civilian, and energy. CERT-EU has recorded incidents by at least 33 pro-Ukrainian and 18 pro-Russian hacktivist groups.

- The Atlantic Council[98] - The Atlantic Council analyzes the role of the private sector in providing assistance to Ukraine, demonstrating Ukraine's resilience against the Russian Federation's physical assaults, cyberattacks and disinformation campaigns.
- Microsoft Threat Intelligence [100]- According to the Microsoft Threat Intelligence team, the analysis of the Russian Federation's cyber activities since the start of the conflict could fit into three periods of the war: Phase one (January until March 2022), Phase two (March until September 2022), and Phase three (September 2022 until today). Microsoft concludes that the cyber and influence operations running in parallel to the Russian Federation's physical assault have largely failed. Three trends, likely to shape Russian cyber operations going forward, were noted by Microsoft: the use of ransomware as a deniable destructive weapon (e.g., Prestige ransomware used against Ukrainian and Polish transportation sector), gaining initial access through diverse means and the integration of real and pseudo hacktivists for power projection.
- Thales [101]- Thales' threat intelligence team discusses various aspects of the Russian Federation's invasion of Ukraine in regard to cyberspace, including the geopolitical and cyber context, cyber capabilities of the belligerent countries, new malware that have been used in the context of the conflict and the rise of hacktivism in regards to the conflict. Thales specifically highlights the different risks due to the conflict, such as non-belligerent European countries being at a high risk of either attacks against Ukraine that spread to European countries or being targeted directly, or other actors may take advantage of the conflict to conduct their own cyberattacks. Finally, the report also gives various recommendations to organizations, so that they may protect themselves.

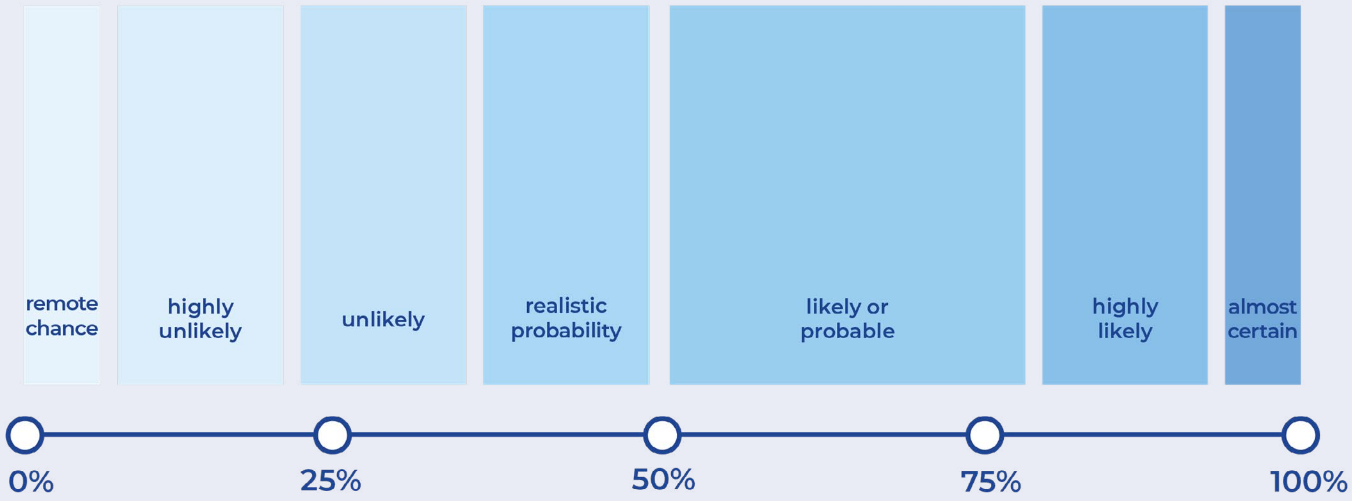
Report Methodology

This report focuses on the incidents documented by the CyberPeace Institute in the first quarter of 2023. Therefore, analysis only covers attacks and campaigns between January 1 and March 31, 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[102]#Ukraine. Specific details and sources of information regarding any individual cyber incidents referenced in this report can be found in the Attack Details[103] 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[104]. Additionally, the CyberPeace Institute distinguishes between singular incidents and campaigns.[105] 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'.[106] 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



References

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

[2] Alternative identifiers used by other organizations related to the activities of this threat actor: BlackEnergy, Iridium, UAC-0082, Voodoo Bear, Sandworm Team, CTG-7263, Quedagh, TEMP.Noble, ATK 14, BE2.

[3] 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).

[4] CERT-UA. (2023) ‘Kiberataka na informacijno-komunikacijnu sistemu Ukrinform (CERT-UA#5850)’. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/3639362 (Accessed: 3 April 2023).

[5] ESET. (2023) ‘SwiftSlicer: New destructive wiper malware strikes Ukraine’. ESET. Available at: https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/ (Accessed: 3 April 2023).

[6] CERT-UA. (2023) 'Kiberataka na informacijno-komunikacijnu sistemu Ukrinform (CERT-UA#5850)’. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/3718487 (Accessed: 3 April 2023).

[7] Alternative identifiers used by other organizations related to the activities of this threat actor: Lorec53, SaintBear, UAC-0056, Nodaria, UNC2589, TA471, Ember Bear.

[8] Threat Hunter Team. (2023) ‘Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine’. Symantec. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer (Accessed: 4 April 2023).

[9] CERT-UA. (2023) ‘Kiberataka, sprjamovana na porushennja cilisnosti ta dostupnosti derzhavnih informacijnih resursiv (CERT-UA#6060)’. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/3947787 (Accessed: 4 April 2023).

[10] ESET. (2023) ‘SwiftSlicer: New destructive wiper malware strikes Ukraine’. ESET. Available at: https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/ (Accessed: 3 April 2023).

[11] 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).

[12] Threat Hunter Team. (2023) ‘Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine’. Symantec. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer (Accessed: 4 April 2023).

[13] Microsoft Threat Intelligence. (2023) ‘A year of Russian hybrid warfare in Ukraine’. Microsoft. Available at: https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed: 18 April 2023).

[14] CERT-UA. (2023)) ‘Kiberataka na informacijno-komunikacijnu sistemu Ukrinform (CERT-UA#5850)’. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/article/3718487 (Accessed: 4 April 2023).

[15] ESET (2022) [Twitter] 14 March. Available at: https://twitter.com/ESETresearch/status/1503436423818534915 (Accessed: 4 April 2023).

[16] Radware. (2022) ‘Killnet’. Available at: https://www.radware.com/cyberpedia/ddos-attacks/killnet/ (Accessed: 11 April 2023).

[17] Kil’djushkin, R. (2023) ‘Russkie hakery iz KillNet nachali «kollektivnuju kiberataku» na Germaniju’. Available at: https://www.gazeta.ru/tech/news/2023/01/25/19571683.shtml?updated (Accessed: 12 April 2023).

[18] NetSide Group (2023) [Telegram] 26 January. Available at: https://t.me/NetSide_official/35 (Accessed: 12 April 2023)

[19] Ibid.

[20] WE ARE RUSSIAN CLAY (2023) [Telegram] 15 February. Available at: https://t.me/WEARERUSSIANCLAY/187 (Accessed: 12 April 2023)

[21] WE ARE RUSSIAN CLAY (2023) [Telegram] 2 April. Available at: https://t.me/WEARERUSSIANCLAYNEW/80 (Accessed: 12 April 2023)

[22] Russian Clay (2023) Obrashhenie ot russkih hakerov "RUSSIAN CLAY". [online video] Available at: https://www.youtube.com/watch?v=T_Kzqe8f3xw (Accessed: 12 April 2023)

[23] Nacional'ni informacijni sistemi (2023) [Facebook] 17 March. Available at: https://www.facebook.com/nais.gov/posts (Accessed: 10 April 2023).

[24] S.T.A.L.K.E.R OFFICIAL (2023) [Twitter] 12 March. Available at: https://twitter.com/stalker_thegame/status/1634939872317411329?ref_

[25] Anonymous Italia. Available at: https://anonsecita.wordpress.com/ (Accessed: 12 April 2023)

[26] Anonymous Italia. (2023) 'Gli Oligarchi e l'ombra di Putin: Vladimir Potanin'. Available at: https://anonsecita.wordpress.com/2023/03/21/gli-oligarchi-e-lombra-di-putin-vladimir-potanin/ (Accessed: 12 April 2023)

[27] KillNet (2023) [Telegram] 1 March. Available at:https://t.me/killnet_reservs/5539 (Accessed: 24 April 2023).

[28] Hakanunye[.]RU (2023) [Telegram] 1 March. Available at: https://t.me/nakanuneru/11006 (Accessed: 24 April 2023).

[29] Bank UBRiR (2023) [Telegram] 14 March. Available at: https://t.me/bank_ubrir/673 (Accessed: 11 April 2023).

[30] Pravitel'stvo Belgorodskoj oblasti (2023) [Telegram] 25 January. Available at: https://t.me/belregion_ru/4699 (Accessed: 11 April 2023).

[31] MChS Rossii (2023) [Telegram] 22 February. Available at: https://t.me/mchs_official/7448 (Accessed: 11 April 2023).

[32] MChS Rossii (2023) [Telegram] 28 February. Available at: https://t.me/mchs_official/7516 (Accessed: 11 April 2023).

[33] Operativnyj shtab - Krasnodarskij kraj (2023) [Telegram] 6 March. Available at: https://t.me/opershtab23/6713 (Accessed: 11 April 2023).

[34] Operativnyj shtab - Krasnodarskij kraj (2023) [Telegram] 9 March. Available at: https://t.me/opershtab23/6718 (Accessed: 11 April 2023).

[35] Anonymous Sudan (2023) [Telegram] 20 February. Available at: https://t.me/AnonymousSudan/190 (Accessed: 12 April 2023).

[36] Anonymous Sudan (2023) [Telegram] 19 February. Available at: https://t.me/killnet_reservs/5388 (Accessed: 12 April 2023).

[37] Wahlen M. (2023) Anonymous Sudan. Threat Intelligence Report. Truesec. Available at: https://www.google.com/url?q=https://www.truesec.com/hub/blog/what-is-anonymous-sudan&sa=D&source=editors&ust=1683109554073881&usg=AOvVaw1eu8BUlXXpnwunxerI9nCi (Accessed [12] April 2023).

[38] Ibid.

[39] Bolton, T. (2023) 'Which countries are sending heavy weapons to Ukraine, and is it enough?'. Available at: https://www.euronews.com/2023/03/05/which-countries-are-sending-heavy-weapons-to-ukraine-and-is-it-enough (Accessed: 18 April 2023).

[40] Ibid.

[41] Camut, N. (2023) 'Germany to send 88 Leopard I tanks to Ukraine'. Politico. Available at: https://www.politico.eu/article/germany-send-leopard-tanks-ukraine-russia-war-rheinmetall/ (Accessed: 18 April 2023).

[42] Le Monde. (2023) 'Poland, Belgium offer additional military aid to Ukraine'. Le Monde. Available at: https://www.lemonde.fr/en/europe/article/2023/01/27/poland-belgium-offer-additional-military-aid-to-ukraine_6013346_143.html (Accessed: 18 April 2023).

[42] Francis, D. (2023) ‘Poland is leaving Europe’s response to the Russian invasion of Ukraine’. Atlantic Council. Available at: https://www.lemonde.fr/en/europe/article/2023/01/27/poland-belgium-offer-additional-military-aid-to-ukraine_6013346_143.html (Accessed: 18 April 2023).

[43] Le Monde. (2023) ‘Poland, Belgium offer additional military aid to Ukraine’. Le Monde. Available at: https://www.lemonde.fr/en/europe/article/2023/01/27/poland-belgium-offer-additional-military-aid-to-ukraine_6013346_143.html (Accessed: 18 April 2023).

[44] Mortensen, A., Mendonca D., McGee, L., and Liptak, K. (2023). ‘Poland becomes first to pledge fighter jets to Ukraine’. CNN. Available at: https://edition.cnn.com/2023/03/16/europe/poland-fighter-jets-ukraine-intl/index.html (Accessed: 18 April 2023).

[45] SOCRadar. (2023) ‘APT Profile: Cozy Bear / APT29’. SOCRadar. Available at: https://socradar.io/apt-profile-cozy-bear-apt29/ (Accessed 24 April 2023).
Alternative identifiers used by other organizations related to the activities of this threat actor: APT 29, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, UNC2452, Dark Halo, SolarStorm, StellarParticle, Nobelium, Iron Ritual, Cloaked Ursa

[46] BlackBerry Research & Intelligence Team. (2023) ‘NOBELIUM Uses Poland's Ambassador’s Visit to the U.S. to Target EU Governments Assisting Ukraine’. BlackBerry. Available at: https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine (Accessed: 19 April 2023).

[47] Anonymous Sudan (2023) [Telegram] 28 January. Available at: https://t.me/AnonymousSudan/40 (Accessed: 1 February 2023).

[48] Anonymous Sudan (2023) [Telegram] 28 January. Available at: https://t.me/AnonymousSudan/41 (Accessed: 1 February 2023)

[49] Anonymous Sudan (2023) [Telegram] 28 January. Available at: https://t.me/AnonymousSudan/42 (Accessed: 1 February 2023)

[50] NLTimes. (2023). ‘More hospitals, cybersecurity firm also targeted in pro-Russian cyberattack’. NLTimes. Available at: https://nltimes.nl/2023/01/31/hospitals-cybersecurity-firm-also-targeted-pro-russia-cyberattack (Accessed: 31 January 2023).

[51] Z-CERT. (2023) ‘DDoS-aanvallen treffen aantal ziekenhuizen’. Computer Emergency Response Team voor de zorg. Available at: https://www.z-cert.nl/nieuws/ddos-aanvallen-treffen-aantal-ziekenhuizen/ (Accessed: 18 April 2023).

[52] NoName057(16) (2023) [Telegram]. 27 March. Available at: https://t.me/noname05716/2523 (Accessed: 27 March 2023).

[53] NoName057(16) (2023) [Telegram]. 27 March. Available at: https://t.me/noname05716/2524 (Accessed: 27 March 2023).

[54] Assemblée nationale. (2023) ‘Attaque informatique sur le site internet de l’Assemblée’. La Présidence de l’Assemblée nationale. Available at: https://presidence.assemblee-nationale.fr/activites/presse/31927 (Accessed: 19 April 2023).

[55] Hathaway, M. (2023) ‘AI Cyber Lunch: Melissa Hathaway on "Malicious Cyber Activities: Russia-Ukraine and the Surrounding Territories’. Harvard Kennedy School. Available at: https://www.hks.harvard.edu/events/ai-cyber-lunch-melissa-hathaway-malicious-cyber-activities-russia-ukraine-and-surrounding (Accessed: 22 March 2023).

[56] Karnitschnig, M. (2023) ‘Ukraine is fighting Western war fatigue, minister says’. Politico. Available at: https://www.politico.eu/article/ukraine-russia-war-volodymyr-zelenskyy-vladimir-putin-is-fighting-western-war-fatigue-minister-says/ (Accessed: 18 April 2023).

[57] Hathaway, M. (2023) ‘AI Cyber Lunch: Melissa Hathaway on "Malicious Cyber Activities: Russia-Ukraine and the Surrounding Territories’. Harvard Kennedy School. Available at: https://www.hks.harvard.edu/events/ai-cyber-lunch-melissa-hathaway-malicious-cyber-activities-russia-ukraine-and-surrounding (Accessed: 22 March 2023).

[58] Bada, M. and Nurse, J.R.C. (2019). ‘The Social and Psychological Impact of Cyber-Attacks’. Emerging Cyber Threats and Cognitive Vulnerabilities. Available at: https://www.researchgate.net/publication/336149510_The_Social_and_Psychological_Impact_of_Cyber-Attacks (Accessed: 20 March 2023).

[59] Ibid.

[60] Insikt Group. (2023) ‘Russia’s War Against Ukraine Disrupts the Cybercriminal Ecosystem’. RecordedFuture. Available

at: https://www.recordedfuture.com/russias-war-against-ukraine-disrupts-cybercriminal-ecosystem (Accessed: 18 April 2023).

[61] Waterman, S. (2023) 'Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army'. Newsweek. Available at: https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814 (Accessed: 28 March 2023).

[62] Evseevich, A. (2023) 'Hinshtejn zajavil, chto dejstvujushhih v interesah RF hakerov nado osvobodit' ot otvetstvennosti'. TASS. Available at: https://tass.ru/obschestvo/17021313 (Accessed: 13 February 2023).

[63] Slawson, N. (2023) 'First thing: Ukraine marks first anniversary of Russia's invasion'. The Guardian. Available at: https://www.theguardian.com/us-news/2023/feb/24/first-thing-ukraine-marks-first-anniversary-of-russias-invasion (Accessed: 24 February 2023).

[64] AlJazeera. (2023) 'Joe Biden's surprise visit to wartime Kyiv'. AlJazeera. Available at: https://www.aljazeera.com/gallery/2023/2/20/photos-bidens-surprise-visit-to-kyiv-ukraine (Accessed: 21 February 2023).

[65] Schmitz, R. and Tanis, F. (2023) 'Turkey says it will ratify Finland's bid to join NATO'. NPR. Available at: https://www.npr.org/2023/03/17/1164236651/turkey-finland-nato-erdogan-sweden#:~:text=Turkish%20President%20Recep%20Tayyip%20Erdogan%20says%20his%20country%20will%20start,a%20decision%20on%20the%20matter (Accessed: 20 March 2023).

[66] ICC. (2023) 'Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova'. International Criminal Court. Available at: https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and (Accessed: 20 March 2023).

[67] Reuters. (2023) 'Putin visits Crimea on anniversary of its annexation from Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/putin-visits-crimea-anniversary-its-annexation-ukraine-2023-03-18/ (Accessed: 20 March 2023).

[68] Fowler, S. and Landale, J. (2023) 'Putin in Mariupol: What the Russian president saw on his visit'. BBC. Available at: https://www.bbc.com/news/world-europe-65007289 (Accessed: 20 March 2023).

[69] U.S. Department of the Treasury (2023). 'Treasury Targets Global Sanctions Evasion Network Supporting Russia's Military-Industrial Complex.'The Department of the Treasury. Available at: https://home.treasury.gov/news/press-releases/jy1241 [Accessed 28 April 2023].

[70] HM Treasury (2023). 'UK and coalition announce price caps on Russian oil products'. GOV[.]UK. Available at: https://www.gov.uk/government/news/uk-and-coalition-partners-announce-price-caps-on-russian-oil-products [Accessed 25 April 2023].

[71] U.S. Department of the Treasury (2023). 'Targeting Key Sectors, Evasion Efforts, and Military Supplies Treasury Expands and Intensifies Sanctions Against Russia'. The Department of the Treasury. Available at: https://home.treasury.gov/news/press-releases/jy1296 [Accessed 28 April 2023].

[72] HM Treasury (2023). 'New sanctions ban every item Russia is using on the battlefield'. GOV[.]UK. Available at: https://www.gov.uk/government/news/new-sanctions-ban-every-item-russia-is-using-on-the-battlefield [Accessed 28 April 2023]

[73] European Council (2023). 'One year of Russia's full-scale invasion and war of the aggression against Ukraine, EU adopts its 10th package of economic and individual sanctions'. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/02/25/one-year-of-russia-s-full-scale-invasion-and-war-of-aggression-against-ukraine-eu-adopts-its-10th-package-of-economic-and-individual-sanctions/ [Accessed 25 April 2033].

[74] European Parliament (2023). EU Sanctions on Russia: Overview, impact, challenges. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739366/EPRS_BRI(2023)739366_EN.pdf [Accessed 25 April 2023].

[75] Ministry of Foreign Affairs of Japan (2023). 'Measures based on the Foreign Exchange and Foreign Trade Act regarding the situation surrounding Ukraine'. Ministry of Foreign Affairs of Japan. Available at: https://www.mofa.go.jp/press/release/press4e_003209.html [Accessed 28 April 2023].

[76] Ministry of Foreign Affairs of Japan (2023). 'Measures based on the Foreign Exchange and Foreign Trade Act regarding

the situation surrounding Ukraine'. Ministry of Foreign Affairs of Japan. Available at: https://www.mofa.go.jp/press/release/press4e_003221.html [Accessed 28 April 2023].

[77] Holden, M. (2023) 'Britain to send 14 of its main battle tanks to Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/uk-has-ambition-send-tanks-ukraine-pm-sunak-tells-zelenskiy-2023-01-14/ (Accessed: 16 January 2023).

[78] Lopez, C.T. (2023) 'Ukrainian to Get U.S. Tanks by Fall'. U.S. Department of Defense. Available at: https://www.defense.gov/News/News-Stories/Article/Article/3336826/ukrainians-to-get-us-tanks-by-fall/#:~:text=The%20Defense%20Department%20announced%20in,year%20to%20make%20that%20happen (Accessed: 27 March 2023).

[79] Schmitz, R., Maynes C., and Kakissis, J. (2023) 'Germany agrees to send its Leopard battle tanks to Ukraine after weeks of pressure'. NPR. Available at: https://www.npr.org/2023/01/25/1150759498/germany-leopard-2-tanks-ukraine#:~:text=BERLIN%20%E2%80%94%20After%20weeks%20of%20intense,help%20the%20country%20fight%20Russia (Accessed: 18 April 2023).

[80] Le Monde. (2023) 'Canada to send four Leopard tanks to Ukraine'. Le Monde. Available at: https://www.lemonde.fr/en/international/article/2023/01/26/canada-to-send-four-leopard-tanks-to-ukraine_6013235_4.html (Accessed: [20] April 2023).

[81] Carreño, B. (2023) 'Spain says it is open to sending Leopard tanks to Ukraine'. Euronews. Available at: https://www.euronews.com/2023/01/26/ukraine-crisis-spain-tanks (Accessed: 20 April 2023).

[82] República Portuguesa. (2023) 'Portugal will provide Ukraine with main battle tanks'. Governo da República Portuguesa. Available at: https://www.portugal.gov.pt/en/gc23/communication/news-item?i=portugal-will-provide-ukraine-with-combat-vehicles (Accessed: 20 April 2023).

[83] Ministry of Defence. (2023) 'Netherlands to purchase Leopard 1 tanks for Ukraine'. Ministry of Defence of the Kingdom of the Netherlands. Available at: https://english.defensie.nl/latest/news/2023/02/07/netherlands-to-purchase-leopard-1-tanks-for-ukraine (Accessed: 20 April 2023).

[84] Dåsnes, I. (2023) 'Norway with comprehensive tanks-package to Ukraine'. Ministry of Defence of Norway. Available at: https://www.regjeringen.no/en/aktuelt/brusselnyhet/id2963053/?utm_source=regjeringen.no&utm_medium=email&utm_campaign=nyhetsvarsel20230214-1:16%20PM (Accessed: 20 April 2023).

[85] The Defense Post. (2023) 'Norway Army Says Delivered Eight Tanks to Ukraine'. The Defense Post. Available at: https://www.thedefensepost.com/2023/03/21/norway-delivered-tanks-ukraine/ (Accessed: 20 April 2023).

[86] Reuters. (2023) 'Finland to send three Leopard tanks to Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/finland-send-three-leopard-tanks-ukraine-2023-02-23/ (Accessed: 20 April 2023).

[87] Reuters. (2023_'Sweden to send up to 10 Leopard tanks to Ukraine'. Reuters. Available at: https://www.reuters.com/world/europe/sweden-send-up-10-leopard-tanks-ukraine-2023-02-24/ (Accessed: 21 April 2023).

[88] Hinshaw, D. and Ojewska, N. (2023) 'Poland Has Sent More Than 200 Tanks to Ukraine'. The Wall Street Journal. Available at: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-29/card/poland-has-sent-more-than-200-tanks-to-ukraine-Krwar3DCPzHJJk4UMVh4(Accessed: 20 April 2023).

[89] Reuters. (2023) 'Poland to send 60 modernised tanks to Ukraine in addition to Leopards'. Reuters. Available at: https://www.reuters.com/world/europe/poland-send-60-modernised-tanks-ukraine-addition-leopards-2023-01-27/ (Accessed: 20 April 2023).

[90] Le Monde. (2023) 'Poland delivers first Leopard 2 tanks to Ukraine'. Le Monde. Available at: https://www.lemonde.fr/en/international/article/2023/02/24/poland-delivers-first-leopard-2-tanks-to-ukraine_6017131_4.html (Accessed: 21 April 2023).

[91] Pietralunga, C. (2023) 'Poland will be the first NATO country to deliver fighter jets to Ukraine'. Le Monde. Available at: https://www.lemonde.fr/en/europe/article/2023/03/17/poland-will-be-the-first-nato-country-to-deliver-fighter-jets-to-ukraine_6019709_143.html(Accessed: 20 April 2023).

[92] Heger, E. (2023) [Twitter] 17 March. Available at: https://twitter.com/eduardheger/status/1636656042057539584?s=20 (Accessed: 24 April 2023).

[93] Quinn, B. (2023) 'Ukrainian troops return home after Challenger 2 tank training in UK'. The Guardian. Available at:

https://www.theguardian.com/world/2023/mar/27/ukrainian-troops-return-home-after-challenger-2-tank-training-in-uk (Accessed: 24 April 2023).

[94] Reznikov, O. (2023) [Twitter] 28 March. Available at: https://twitter.com/oleksiireznikov/status/1640595102119735297 (Accessed: 24 April 2023).

[95] Hegel, T. and Milenkovski, A. (2023) 'NoName057(16) - The Pro-Russian Hacktivist Group Targeting NATO'. Sentinel Labs. Available at: https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/ (Accessed: 18 April 2023).

[96] SSSCIP. (2023) 'Russia's Cyber Tactics: Lessons Learned 2022'. State Service of Special Communications and Information Protection of Ukraine. Available at: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine (Accessed: 21 April 2023).

[97] Insikt Group. (2023) 'Russia's War Against Ukraine Disrupts the Cybercriminal Ecosystem'. RecordedFuture. Available at: https://www.recordedfuture.com/russias-war-against-ukraine-disrupts-cybercriminal-ecosystem (Accessed: 18 April 2023).

[98] CERT-EU. (2023) 'Russia's war on Ukraine: One year of cyber operations'. Computer Emergency Response Team of the European Union. Available at: https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf(Accessed: 18 April 2023).

[99] Schroeder, E. and Dack, S. (2023) 'A parallel terrain: Public-private defense of the Ukrainian information environment'. Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/#keytakeaways (Accessed: 18 April 2023).

[100] Microsoft Threat Intelligence. (2023) 'A year of Russian hybrid warfare in Ukraine'. Microsoft. Available at: https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed: 18 April 2023).

[101] Thales Cyber Threat Intelligence Team. (2023) '2022-2023 : A year of Cyber Conflict in Ukraine". Thales. Available at: http://iddeuxpoints.com/pro/thales/Extensive_Report_CyberConflict_UkraineTHALES23.pdf (Accessed: 21 April 2023).

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

[103] Ibid.

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

[105] Ibid.

[106] 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)