Empirical analysis of the cyberattacks of the Russian–Ukrainian war

This research study aims to empirically analyze the cyberattacks that occurred in the context of the Russian–Ukrainian conflict between 2022 and 2023, with a specific focus on the impact of these attacks on civilian infrastructure and institutions. The data collection for this study is based on publicly available sources from the Cyber-Peace Institute, taking into account various types of incidents such as malware, distributed denial of service (DDoS) attacks, spam, information operations, and website defacements. The study employs a network theory approach to examine the structure and dynamics of incidents and campaigns, while additional statistical methods and trend analysis are used to assess sector-specific and geographic patterns, as well as changes in attack frequency and severity. The research aims to contribute to the existing literature on cyber warfare and to provide valuable insights into the cyber threats faced by civilian infrastructure and institutions during times of conflict.

Keywords: *Russian–Ukranian war, cyberattacks, network analysis, sector analysis*

Acknowledgments

This research has been carried out as part of project no. TKP2021-NKTA-51, implemented with support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

Author Information

Péter Bányász, University of Public Service
https://orcid.org/0000-0002-7308-9304
Adrienn Kiss, University of Public Service
https://orcid.org/0000-0003-4953-5367
Sándor Magyar, University of Public Service
https://orcid.org/0000-0002-6085-0598
Dávid Kiss, University of Public Service
https://orcid.org/0009-0004-2034-2734

How to cite this article:

Bányász, Péter, Adrienn Kiss, Sándor Magyar, Dávid Kiss. “Empirical analysis of the cyberattacks of the Russian–Ukrainian war”.
Információs Társadalom XXIV, no. 2 (2024): 9–32.
https://dx.doi.org/10.22503/inftars.XXIV.2024.2.1

1. Introduction

The impact of information technology (IT) has been growing not only in the lives of individuals but also in the operations of organizations. As far back as the 2000s, some research was already looking into the future of the information society. According to studies published in recent years on the information society, human knowledge has become the most important factor of development in the information society, and among capital goods, human resources have become the most prominent (Majó 2006). There was a time when the drivers of technological development were general education and technological innovation, but these drivers have disappeared over time (Karvalics 2007). With an increasing dependence on IT services in the digital ecosystem, the ease and convenience they provide are accompanied by a growing threat of service outages and cyberattacks. Information is power, and its importance is indisputable. The complexity of information is judged on subjective grounds, but information is a force that is nowadays used to launch various attacks (Krzanowski 2023). Given the well-defined target that IT systems and their users present, such attacks pose a significant challenge. During the Russia–Ukraine war, it became clear that these attacks could affect both local and global digital ecosystems, emphasizing the importance of digital services for the continuity of operations in the region (Aviv and Ferri 2023). While emerging and disruptive technologies such as artificial intelligence, autonomous aerial vehicles, and hypersonic aircraft offer significant benefits for civilian and military domains, their potential for malicious use also poses a significant threat. As a result, cyber operations are taking on an increasingly important role alongside conventional warfare, which itself is evolving with new technologies and tactics.

As IT becomes increasingly essential for modern society, the potential impact of cyberattacks on a nation's security also increases. This is why cyberspace is now recognized as an important operational domain in contemporary warfare, including in the Russian–Ukrainian conflict. Hybrid warfare strategies further underscore the importance of these domains, as they provide a viable battlefield for all parties to achieve their strategic objectives, both in peacetime and in times of conflict. The choice of targets for cyberattacks can support military objectives, even at the strategic level, making it necessary for both the military and civilian sectors to develop appropriate protection against such attacks. The use of cyber operations in the Russian–Ukrainian conflict also revealed the capacity of cyberspace to conceal attackers' identities. The ability to collaborate with non-state actors can be an advantage for cyber attackers. On the Russian side, intelligence services have been primarily responsible for these activities, with support from non-state actors, including "patriotic" hackers and private companies (Miron and Thornton 2024).

In cyberspace, hidden attackers from third countries can be recruited or voluntarily join. Due to the difficulty of attribution in cyberspace, as a result, electronic information systems, including those in government agencies, public services, financial institutions, and critical infrastructure, have become established targets for state actors. These actors may cause significant damage through the use of hacker

groups funded by state actors or through services available on the dark web, such as "cybercrime as a service."

The wide range of cyberattack tools available to attackers provides them with significant opportunities. Electronic information systems' vulnerabilities can be exploited through various tactics, techniques, and procedures that are easily deployable. The availability of hacking tools is increasing, enabling a range of outcomes beyond attacks on the target country's territory, such as accessing adversary data, rendering systems inaccessible, and conducting reputation attacks. In addition, psychological operations against soldiers and the population accessible via cyberspace, particularly in the area of influence (disinformation, misinformation, malinformation), can also be highly effective and yield easier successes. As a result, many countries are dedicating significant attention to the development of offensive cyber-operational capabilities. The Russian–Ukrainian conflict has demonstrated that the cyber domain is evolving alongside changes in conventional warfare, and can deliver appropriate results on the battlefield, in the hinterland, and even more broadly in the international environment. In certain cases, it can even serve as a complement to or substitute for military operations.

In addition to the challenge of effectively attributing cyberattacks in the legal realm, such attacks may pose risks even in the absence of open armed conflict (Fiala and Worrall 2024). The Russian invasion of Ukraine serves as a prime example of a gray-zone contest in which nation-states' and other actors' main narratives – particularly their changing intensity and tone – affect diplomatic, economic, and military domains (Hoffman and Hofmann 2018). The political and military gains made in the gray-zone area are significant and contribute to the realization of conflict objectives without relying on arms. The scope of the impact of activities in cyberspace raises important questions about the development of international law for managing cyber conflicts and highlights cases that may require military responses.

The present study employs a comprehensive methodology to analyze documented cyberattacks during the Russian–Ukrainian conflict between 2022 and 2023. Since 2013, Russia has carried out various cyber operations targeting Ukraine on multiple occasions (Lunn 2023). Antecedent to the invasion, scholars had foreseen a widespread cyber conflict; however, the magnitude of the recorded cyberattacks has been limited, plausibly because of Ukraine's enhanced cyber defenses established through collaboration with Western allies (Lonergan et al. 2023; Kostyuk and Brantly 2022).

The research objectives were twofold:

- to conduct an empirical analysis of the characteristics and dynamics of cyberattacks that were documented during the Russian–Ukrainian conflict between 2022 and 2023;
- to identify the sector-specific attacks, as well as assessing the changes in the frequency of said attacks.

Consequently, the research study has identified the following research questions to be addressed:

- What were the most commonly occurring types of cyberattacks during the Russian–Ukrainian conflict?
- What is the distribution of cyberattack types between different sectors?
- How did the frequency of cyberattacks change during the course of the conflict?

In conclusion, the research study proposes the following hypotheses:

H1: Cyberattacks reach their peak during the winter months.

H2: The energy sector has been the most affected by cyberattacks due to its critical role in civil infrastructure.

H3: In terms of frequency, distributed denial of service (DDoS) attacks are the most common type of cyberattacks.

H4: The frequency of cyberattacks conducted by state-sponsored attack groups is significantly higher when compared to those perpetrated by smaller attack groups.

2. Methods

The data under analysis was gathered through the Cyber Conflicts project of the CyberPeace Institute (CyberPeace Institute 2023). The Institute was established with the aim of mitigating the negative impacts of cyberattacks, aiding vulnerable communities, and promoting responsible conduct in cyberspace. Cyber Conflicts concentrates primarily on cyberattacks that occurred during the Russian–Ukrainian war. Any incident that falls within the ambit of cyberattacks and operations defined by the CyberPeace Institute, especially those carried out by a threat actor with the intention of disrupting, disabling, destroying, manipulating, surveilling, controlling, or extracting computing environments/infrastructure and/or data using a computer network or system, is covered. These incidents include but are not limited to hack and leak, where the attacker aims to hack into the target's data and then steal and use critical information from the victim (Traficom 2023); DDoS, in which an attacker floods a server with internet traffic to prevent users from accessing related online services (Fortinet 2024); and defacement, which is an attack on a website that alters its informational content or visual appearance (Kaspersky Lab 2024).

The Institute refers to incidents as campaigns if they satisfy all of the following conditions:

- The incident is linked to the same threat actor and happened within an eight-hour period targeting more than two entities at the same time within the same country or one entity more than twice.
- The incident targeted the same entity over two consecutive days.
- The incident that targeted more than two entities in more than two countries is linked to the same threat actor using the same modus operandi.

Where a threat actor targeted entities in various sectors during a campaign, the Institute creates an incident record for each sector, not for each targeted entity. The primary focus for data collection is on cyber incidents that affect institutions and facilities in the sectors listed in the United Nations International Standard Industrial

Classification of All Economic Activities. Data collection pertains to cyber incidents in the context of the Russian–Ukrainian war, including incidents in Ukraine, the Russian Federation, and other countries. It is worth noting that confirming incidents, especially in the Russian Federation and Belarus, presents particular challenges.

Although it is not always possible to determine if a specific cyberattack or operation was carried out with political, military, activist, and/or strategic motives related to the conflict, this forms the basis of the data collection scope. For instance, incidents are documented relating to the leak of data from Russian organizations committed in the name of pro-Ukrainian activism, the disruption of services after a country took a public political or economic position on the conflict or provided military aid, and collateral damage in a third country that spills over from an incident originally targeting an entity in either the Russian Federation or Ukraine.

For the timeline's purpose, the Institute collects information on cyberattacks that is available publicly (open source) by monitoring news/media outlets, government, cybersecurity companies, computer emergency response teams (CERTs), and civil society organizations' reports, advisories, blogs, and social media feeds, among other sources. Every identified incident and associated content is reviewed by at least two internal analysts, and wherever possible, the incident is linked to at least two distinct sources of information. The Institute continuously scans for information on previous incidents to update the timeline on societal harm and attribution, which is often reported significantly after the actual incident. As publicly available data is relied upon, documented cyberattacks have been assigned a classification of certainty based on the reliability of the information source. The classification levels are as follows:

- Confirmed: Attacks in this category are based on official government reports/records, official press releases by the targeted organization, official letters addressed to customers by the target organization or the government, or social media communication by the targeted organization. If an incident has been self-attributed by a threat actor, and a government entity has confirmed the attack, it will be classified as confirmed.
- Probable: Attacks in this category are based on media reports of a press conference by the targeted organization, social media communication by the targeted organization, or quotes from the targeted organization's staff in media articles. If an incident has been self-attributed by a threat actor, and the attack has been corroborated by a third party through independent research or the analysis of stolen data, this is also classified as a probable incident. Incidents identified and reported on as a result of a technical/forensics investigation will also be classified as probable.
- Possible: Attacks in this category are based on media reports with no direct reference to primary source information. This can be in the form of a news article that mentions a letter sent to patients or a blog post that references a statement published by the targeted organization, but no direct record of this material is available. This category also includes data published by a threat actor online with no further corroborating information.

Based on the gathered data, 187 cases were confirmed, 117 were classified as probable, and 655 were deemed to be possible. The CyberPeace Institute does not

publicly document data related to "hearsay" incidents, which contains uncorroborated information originating from a third party, that is, as a result of media reporting of the allegation by a third party (CyberPeace Institute 2023).

Our methodology for investigating cyberattacks integrates five main techniques – time-series analysis, trend analysis, heat-map visualization, cluster analysis, and network analysis. Time-series analysis is used to examine the temporal distribution of cyberattacks, while trend analysis focuses on the evolving nature of attacks in different sectors and the tactics used by threat actors. Heat-map visualization provides a clear and intuitive picture of the concentration and distribution of cyberattacks, while cluster analysis groups similar types of attacks based on various attributes. Finally, network analysis examines the relationships and interactions between different entities involved in cyberattacks. Together, these methods offer insights into temporal trends, sectoral vulnerabilities, geographic hotspots, common attack patterns, and the complex web of relationships between different stakeholders in the cyber domain, serving as the foundation for developing informed cybersecurity strategies and policies.

3. Results

As an initial step in the time analysis, we examined the monthly frequency of attacks between 13 January 2022 and 31 December 2023. The cyberattacks that occurred during the initial period of the conflict are as follows:

- January 2022: 6 attacks
- February 2022: 33 attacks
- March 2022: 61 attacks
- April 2022: 47 attacks
- May 2022: 19 attacks.

The aforementioned data indicates a significant increase in the number of attacks in February, with a peak in March, followed by a decline in April and a further decrease in May.

The frequency of cyberattacks exhibits a periodicity that can be delineated into approximately six-month cycles. Specifically, the second cycle spans from May 2022 to the conclusion of November 2022, whereas the third cycle encompasses December 2022 to April 2023. Subsequently, a diminishing trend is observed during the fourth cycle from April 2023 to January 2023. In each cycle, a discernible pattern emerges, characterized by a gradual increase in the frequency of attacks, followed by a peak and a subsequent decline. This pattern can be attributed to the constraints imposed by the attackers' capacity and resource limitations, which allow for approximately six months of preparation and activation. When examining the trend in the number of attacks averaged over time, a minimal upward trend is observed, indicating that the attackers are either unable or unwilling to execute large-scale attacks even after a considerable length of time has elapsed.

Subsequently, we employed visualization techniques to better understand the dynamics and possible patterns of monthly attacks over the entire period (see Figure 1).

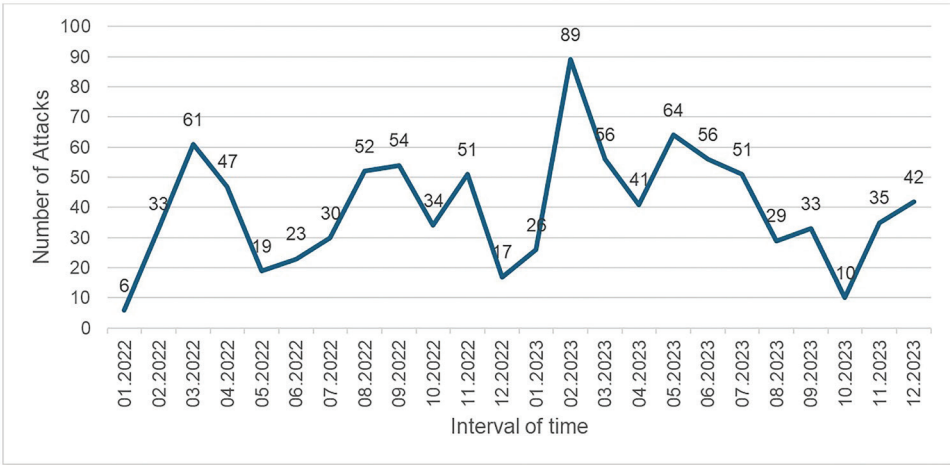

Figure 1. Distribution of cyberattacks during the period of analysis (own edition based on CyberPeace Institute database)

In total, 959 cyberattacks were identified during the period of analysis. In February 2022, as the Russian military advanced toward the Ukrainian border, experts in cybersecurity began to envision the potential employment of cyberattacks by the Russian government to undermine the Ukrainian defenses. Various governmental agencies and private sector entities predicted that the Russian forces would unleash a rapid and devastating series of electronic assaults aimed at disrupting the country's critical infrastructure, including power plants and air traffic control networks, thereby causing widespread destruction. However, while cyberattacks from Russian sources have indeed been a factor in the conflict, their impact thus far has not been as substantial as anticipated by some analysts (Givens et al. 2023).

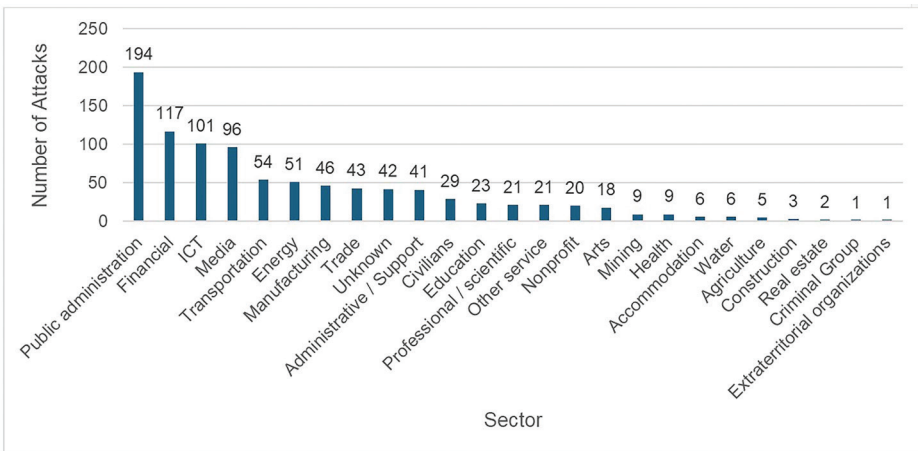

Figure 2. Distribution of attacks by sector (own edition based on CyberPeace Institute database)

We subsequently examined the sector-specific distribution of attacks to ascertain which sectors were most impacted during this period. The findings are depicted in Figure 2.

The aforementioned distribution indicates that the public administration, finance, information and communication technology (ICT), and media sectors were the most impacted by attacks during the period under analysis. These sectors offer critical infrastructure and services, which may elucidate why they were coveted targets for attackers.

The next part of our analysis focused on the types of attacks. First, we examined the frequency of attack types in the general context (see Figure 3), and second, we looked at the distribution of these attack types across sectors, which, in view of the attacks that have occurred, we limited to the 10 sectors that have suffered the most attacks (see Figure 4).

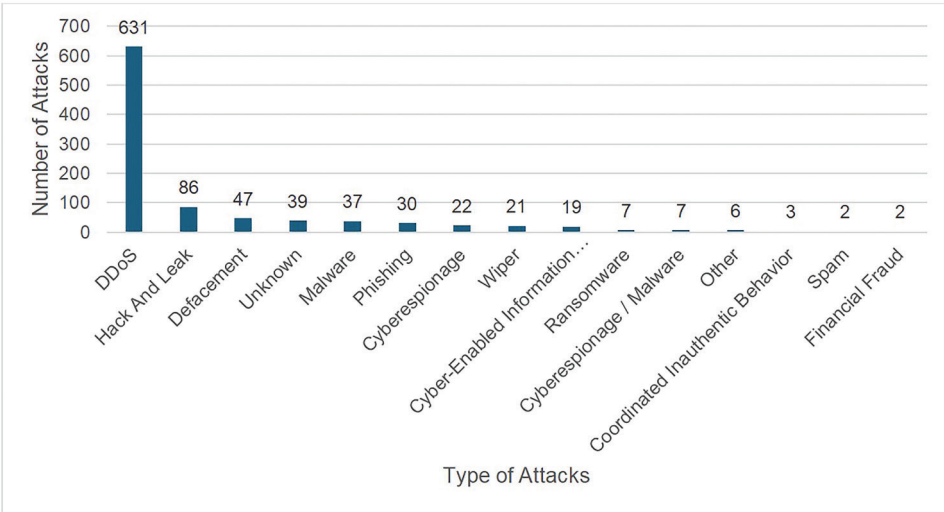

Figure 3. Distribution of attack types
(own edition based on CyberPeace Institute database)

The aforementioned distribution demonstrates that DDoS attacks (631) were the most prevalent during this period, substantially outnumbering other types of attacks. Hack and leak (86) and defacement (47) attacks also constituted a considerable number of incidents, while the other attack types occurred relatively less frequently. This analysis can aid in comprehending the attack techniques that attackers favor and emphasize the priorities for cybersecurity defenses.

Figure 4 reveals that the public administration (194) sector experienced the highest number of security breaches, succeeded by the financial (117) and ICT sectors (101). The DDoS attacks emerged as the most prevalent form of security intrusion across all the three sectors (public administration 118, financial 95, ICT 65). The term "sectors" encompasses not only traditional sectors but also criminal groups. This is

due to the fact that multiple hacktivist groups, which support either Ukraine or Russia, have launched attacks against each other, resulting in the exposure of sensitive information about the groups' operations or members, and in some cases leading to arrests. As evidence, three indictments in distinct federal jurisdictions have been unveiled, accusing multiple Russian cybercrime actors associated with the Trickbot malware and Conti ransomware stratagems (2023).

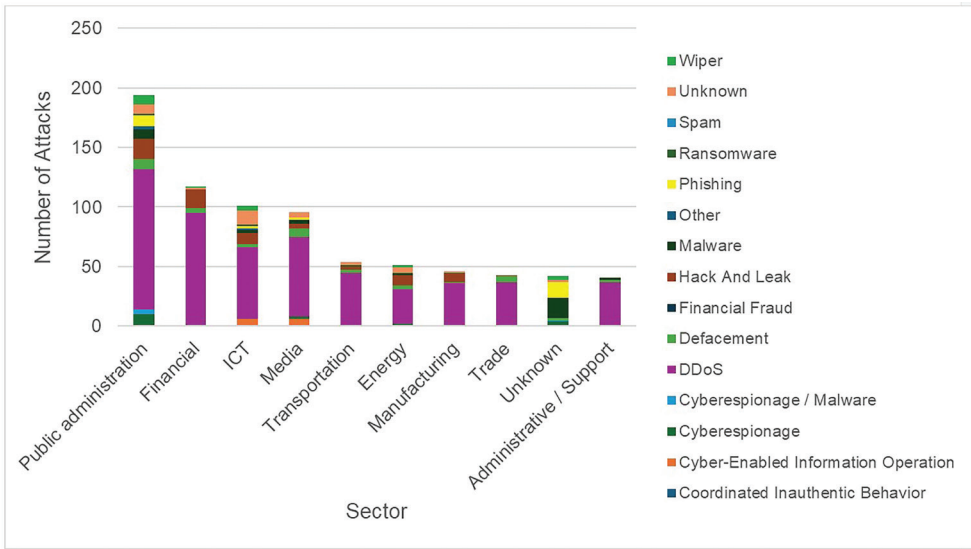

Figure 4. Distribution of the 10 most attacked sectors by attack types (own edition based on CyberPeace Institute database)

The graphical representation in Figure 5 illustrates the top 10 attack groups along with their frequently employed attack types. The data reveals that certain attackers prefer a diverse range of attack methods, whereas others concentrate on specific techniques. The majority of the attacks can be linked to the People's Cyber Army (249), known to have ties with Russia, which surpasses the number of attacks conducted by the Ukrainian IT Army (85), the second most active group, by almost three times. It is noteworthy that the IT Army occupies the third position in the chart, as the perpetrator of 107 attacks could not be ascertained. Despite being a group linked to Russia, the People's Cyber Army has surprisingly launched attacks on four occasions against Russian targets. Furthermore, six identified groups have attacked both Russian and Ukrainian targets, namely Anonymous Russia, Phoenix, Mirai, KillNet, and GURMO. With the exception of GURMO, the majority of these groups have primarily targeted Ukraine and are commonly associated with Russia. As GURMO is the Ukraine's Military Intelligence Service, consequently the one attack executed a cyber-enabled information operation against Russian television channels broadcasting in Crimea, which targeted Ukraine. Crimea has been occupied by Russia since 2014 (Lunn 2023).

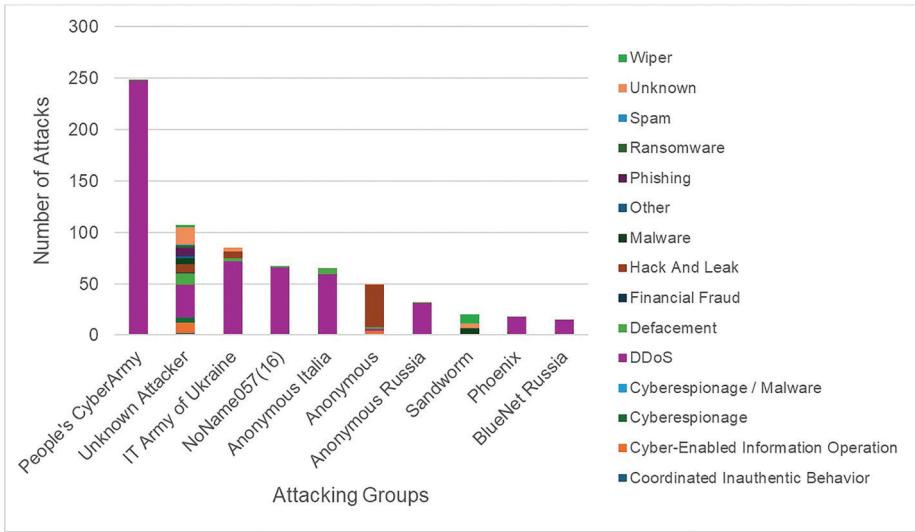

Figure 5. Distribution of the 10 most active attacking groups by attack types (own edition based on CyberPeace Institute database)

The conflict between Ukraine and Russia has spurred the involvement of young hackers in hacktivist groups, which have carried out cyberattacks against Russia (Security Alliance Limited 2022). The cyber facet of the conflict has observed a considerable quantity and heterogeneity of cyber occurrences; nonetheless, the participation of non-state actors and their readiness to carry out cyberattacks outside the domain of military operations had not been predicted (Chukhua 2023). The initial majority of pro-Ukraine groups has shifted over time, with pro-Russia groups taking the lead. This shift can be attributed to various factors, including the establishment of the IT Army by the Ukrainian government. Furthermore, the outrage of pro-Ukraine groups regarding other geopolitical events has diverted their attention to other political targets. Additionally, frequent rivalries among pro-Ukraine groups have led to divisions and the suspension of their operations. Notably, some groups supporting Russia have been identified as Russian cybercriminal groups. It is widely believed that there exists an unspoken agreement between Russian national security services and Russian cybercriminal groups, whereby cybercriminals are permitted to operate, provided that they do not target Russian interests (Miron and Thornton 2024). Alternatively, if the interests of the Russian state require it, these groups may carry out their activities in accordance with Russian interests.

As per the Ukrainian government, the IT Army boasts over 200,000 active members. However, this number is believed to be overstated. Nonetheless, a significant number of cyber volunteers are involved on both sides of the conflict (Willett 2022), with most of them aged between 13 and 25 years. The duration and outcome of the war remain uncertain. However, one of the primary concerns is the future actions of the hundreds of thousands of cyber volunteers who have participated or are participating in the attacks. These young individuals have acquired skills in penetrating

secure systems and concealing their identities. While there is a great need for ethical hackers to ensure a safer cyberspace, there is apprehension that most of these volunteers will opt for the easier route of pursuing illicit activities for financial gain (Feledy and Virág 2022).

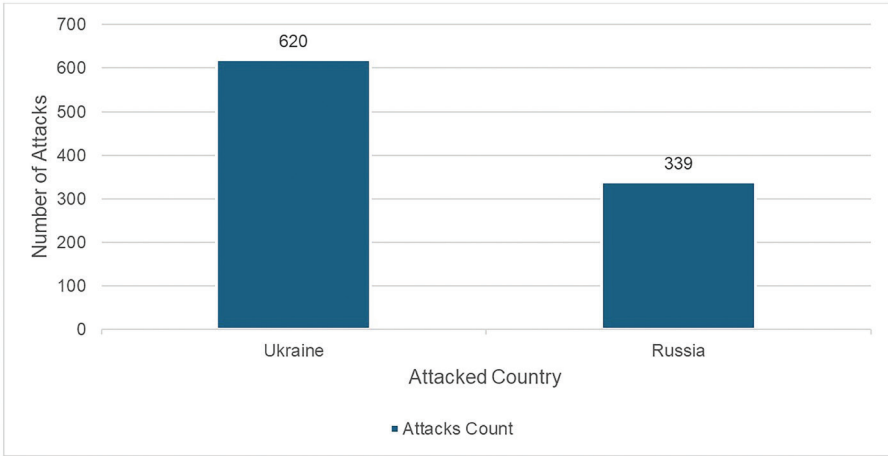

Figure 6. Distribution of attacks by country
(own edition based on CyberPeace Institute database)

Figure 6 depicts the distribution of attacks targeting both Russia and Ukraine, while Figure 7 provides a visual representation of the distribution of the attacks over time.

During the period under review, Ukraine suffered almost twice as many cyberattacks as Russia.

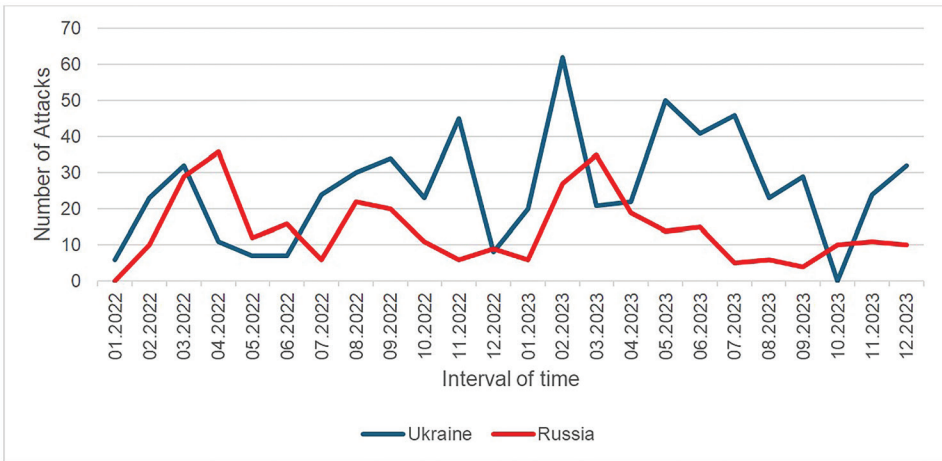

Figure 7. Distribution of attacks by country over time
(own edition based on CyberPeace Institute database)

As the graphical representation shows, the month of February 2023 witnessed the highest number of cyberattacks in Ukraine among all the months, while October 2023 was the only month devoid of any such incidents.

Examination of the dispersion of affected industry sectors by nation accentuates the extensive array of economic and societal sectors that have been impacted by cyber intrusions in both Ukraine and Russia (see Figure 8). The findings indicate that:

In the instance of Ukraine, a majority of the attacks were directed toward the public administration, energy, trade, and transport sectors, denoting the strategic significance of these domains in the conflict.

In Russia, the administration, energy, and transport sectors were the most prominently impacted; however, it is of significant note that the agricultural and mining sectors were also targeted.

These results can help us better understand the dynamics of cyber conflict and how attackers choose their targets in each country.

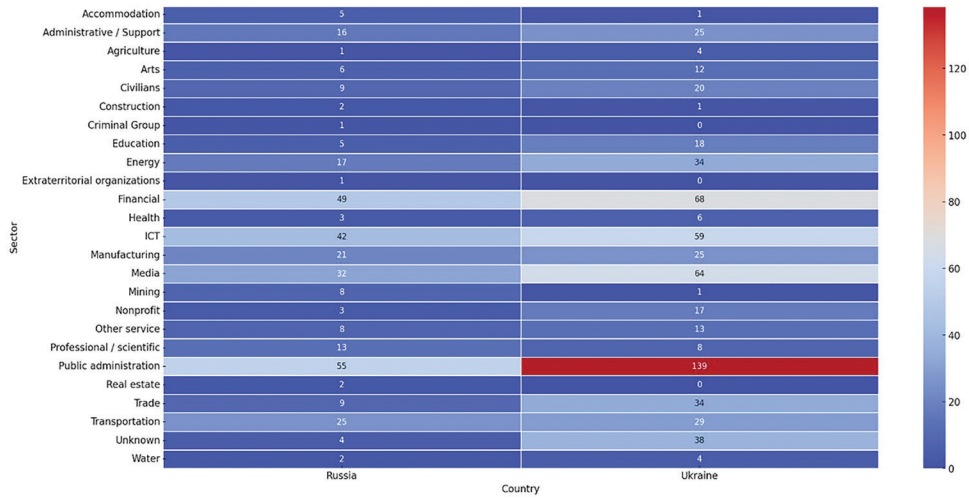

Figure 8. Distribution of sectors affected by the attack by country (own editing in Python, based on CyberPeace Institute database)

The presented heat map provides a detailed analysis of the distribution of cyberattacks across various sectors in Russia and Ukraine. The color saturation within each individual cell represents the frequency of attacks, providing a clear and concise evaluation of the affected sectors in both nations. The findings of the analysis confirm the notable targeting of specific sectors, including public administration, energy, and transportation in both countries, which was previously observed. The heat map also allows for the identification of additional intricacies, such as the relative susceptibility of different sectors and variations between the two countries in terms of the most targeted sectors. The data highlights the need for increased cybersecurity measures in these specific sectors, particularly in public administration, energy, and transportation, to mitigate the risks of cyberattacks.

Furthermore, we have exhibited the relationships among attackers and the affected industries (Figure 9), as well as between attackers and their frequently used attack techniques (Figure 10), through the use of heat maps. Such a graphical representation can potentially facilitate comprehension of the interconnections between perpetrators and their intended victims, as well as their modus operandi.

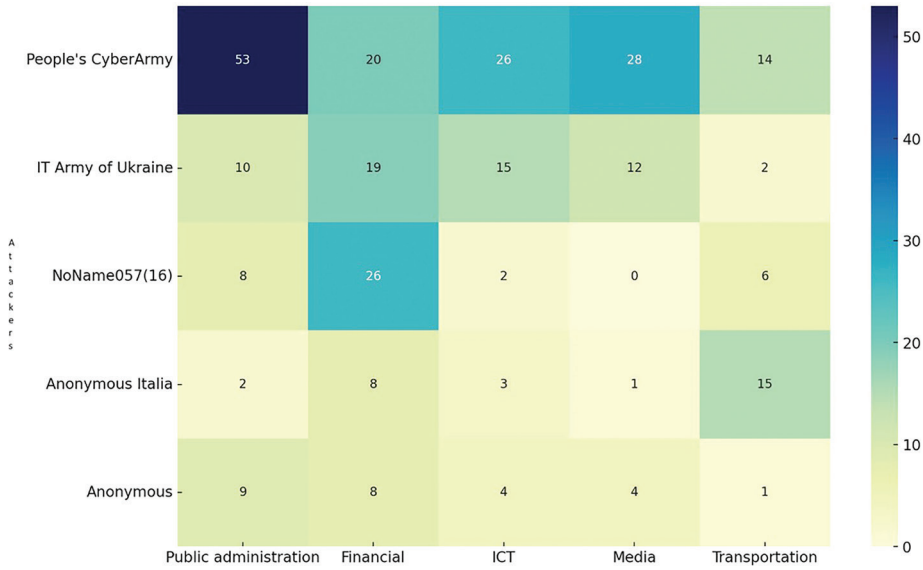

Figure 9. Distribution of sectors most frequently targeted by attackers (own editing in Python, based on CyberPeace Institute database)

Figure 9 presents a heat map that provides a visual representation of the frequency of cyberattacks in different sectors. The chromatic intensity within each discrete unit signifies the rate of occurrences of assaults, with darker shades indicating a higher frequency of attacks. The results of the heat-map analysis reveal that public administration is the most vulnerable sector to cyberattacks, followed by the financial, ICT, and media sectors. The correlation between the previous analyses and the heat-map data highlights the need for increased cybersecurity measures in these sectors to protect against the growing threat of cyberattacks. Figure 10 corroborates the previous analyses, indicating that DDoS attacks are the most prevalent among all types of cyberattacks, and they are predominantly carried out by a specific group of threat actors. The figure provides a clear visual representation of the distribution of attack types and the groups responsible for them. The data reveals that DDoS attacks stand out significantly, with a considerably higher frequency than other forms of cyberattacks. Furthermore, the figure illustrates that a select group of attackers is responsible for the majority of these attacks, which highlights the need for targeted measures to combat this specific threat. It is clear that DDoS attacks pose a significant risk to organizations, and identifying the responsible groups should be a priority in developing effective strategies to mitigate the risk of such attacks.

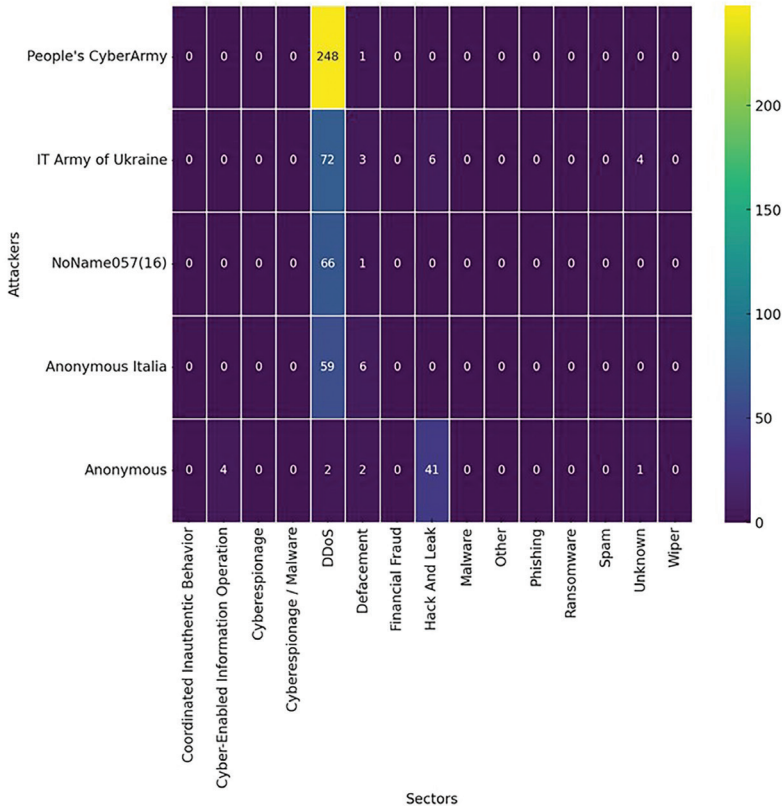

Figure 10. Distribution of the most common types of attacks used by attackers (own editing in Python, based on CyberPeace Institute database)

In order to attain a more comprehensive understanding of the attacks' nature, it is advisable to employ supplementary methodological approaches in analyzing the accessible data. Network analysis offers the possibility to visually represent the connection between the attackers and the attacked sectors, therefore enabling us to draw further inferences. To establish the foundation of our network, we must first define its structural principles. Within this network, we interpret all attackers and attacked sectors as nodes. Specifically, there are 25 sectors and 95 attackers represented as nodes in this case. It is crucial to note that we do not segregate the Russian and Ukrainian sectors from each other, but rather consider the direction of the attack, i.e., the sector itself, as a node in the network, following a general principle. To elaborate, the network's disassociation from the targeted country of attacks is crucial, as it enables us to focus on the attacks' essence. Extracting data from the database, we treated all attacks directed from an unidentified attacker or toward an unidentified target as a single point, labeled as Unknown Sector and Unknown Attacker. This is a critical component of our analysis and warrants emphasis. The

next fundamental element of the network is its connection scheme, which entails the determination of links or edges. A link between two points is established when an attacker has targeted that specific sector at least once during the analysis period.

A representation of the fundamental network based on these principles is depicted in Figure 11. All the network diagrams were generated employing the Gephi data visualization software.

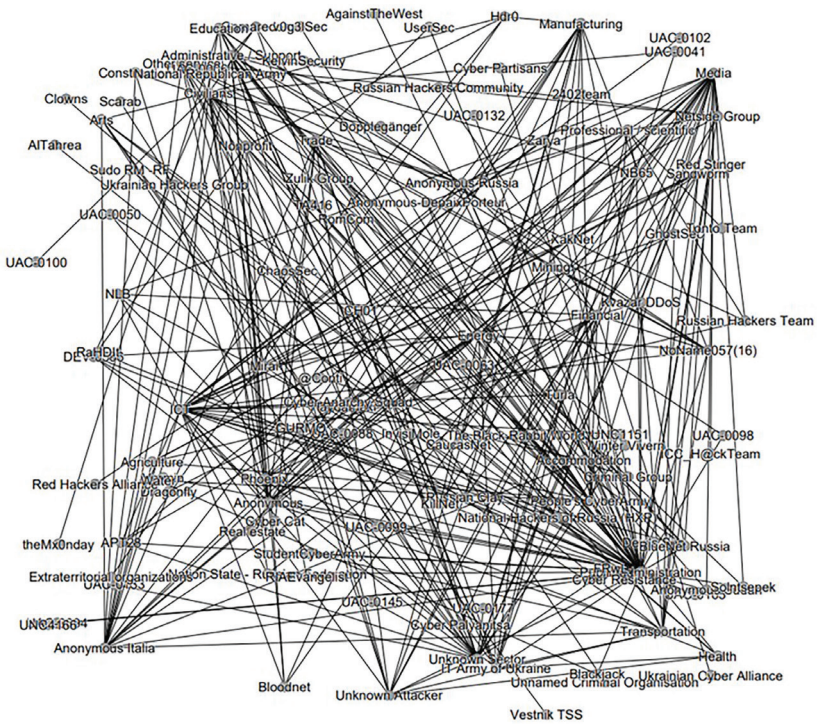

Figure 11. Network of cyberattacks by sector and by attacker (own editing in Gephi, based on CyberPeace Institute database)

The network structure, in its present state, remains incomplete. In addition to defining connections between nodes, we must also determine whether or not the edges in our network are directed. As attacks toward a sector have an evident directionality (given that the sector cannot retaliate), we have designated our network as directed, with links always originating from the attacker and terminating at the sector. Both analysis and interpretation can be further enhanced through the color-coding and weighting of edges and nodes. While many criteria can be used to weigh the relationship between nodes, such as the extent of damage or the resources utilized to execute an attack, this study utilized a coherent system where the weights represent the number of attacks. In other words, each additional attack toward a given sector resulted in a one-unit increase in the attacker's value toward that sector, regardless

of whether the attack targeted a Russian or a Ukrainian sector. For nodes, a similar weighting system was employed based on the number of degrees, i.e., the number of edges entering or leaving a node. The size of a sector node in the network corresponds to the number of attacks it sustained, while an attacker node's size reflects the number of attacks it executed. Building on the edge weighting system, we also factored in edge weight when determining node size rather than simply considering the number of edges. Consequently, the size of each node was determined based on its respective weighted degree.

The introduction of these criteria has resulted in a significant transformation of our network, as demonstrated in Figure 12.

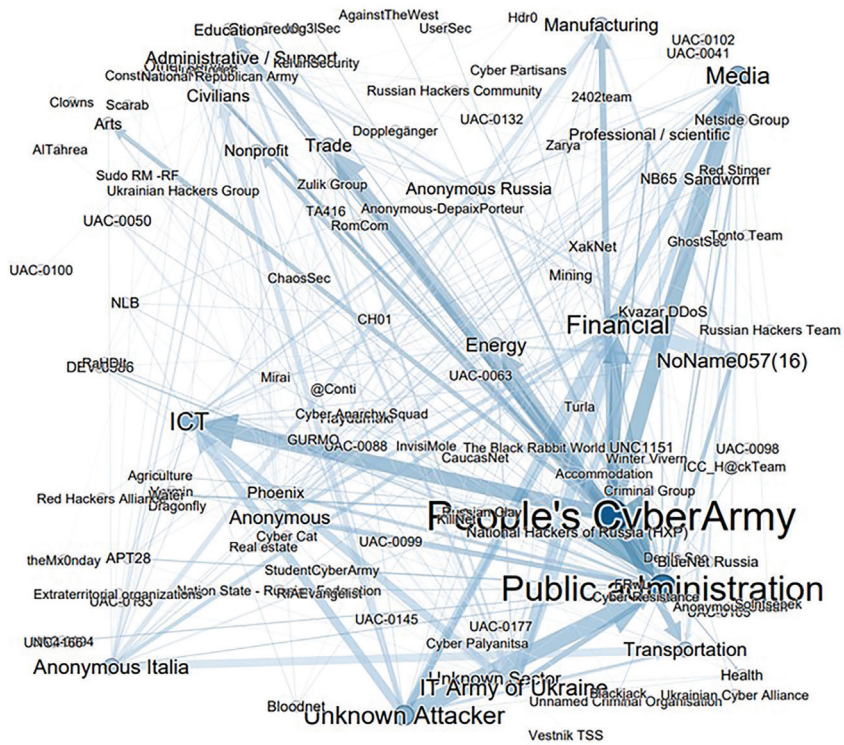

Figure 12. Distribution of the weighted network of cyberattacks by sector and attacker (own editing in Gephi, based on CyberPeace Institute database)

Figure 12 displays the network nodes in the same position as in Figure 11; however, the application of color-coding and weighting has emphasized the network's crucial nodes, namely, the attackers with the most attacks and the sectors that sustained the most damage.

Following the weighting process, it is crucial to identify the network's primary features. The network is classified as a bipartite graph, meaning that its nodes can

be categorized into two distinct sets (attackers and sectors), where nodes within each set are never connected to each other, but solely to nodes in the other set. To illustrate this grouping of nodes, an additional criterion can be incorporated, which, when used in conjunction with the visualization tools and layouts provided by Gephi, can yield a representative depiction of the network's nodes in terms of both color-coding and positioning (as evidenced in Figure 13).

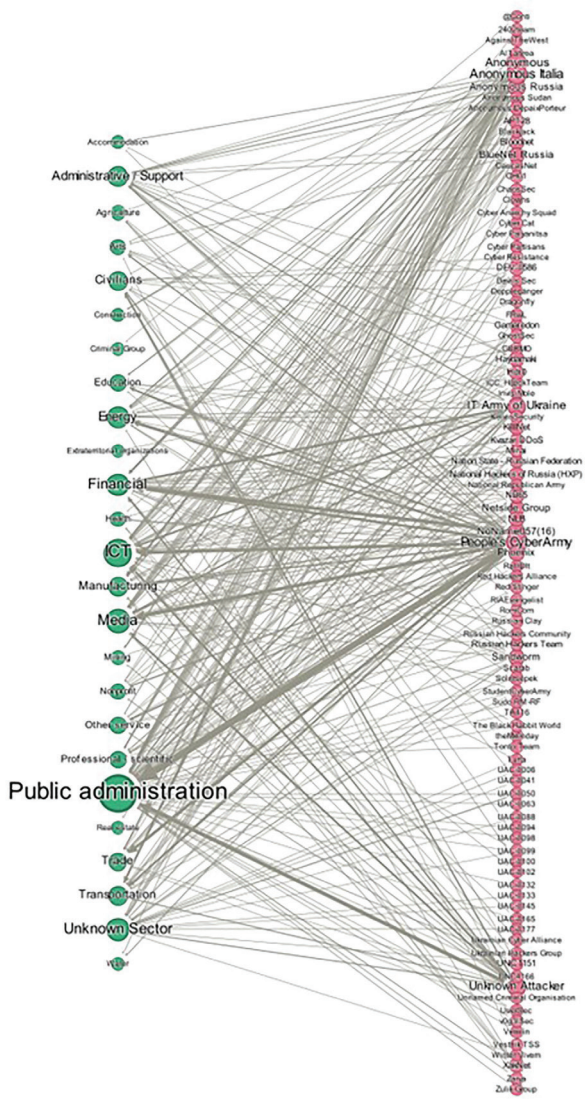

Figure 13. Network of cyberattacks, categorized by both sector and attacker, with weights assigned to each node and edge
(own editing in Gephi, based on CyberPeace Institute database)

It is noteworthy that the network comprises two distinct components, implying that points within the network are not entirely traversable; in mathematical terms, it is not fully walkable. One of these components pertains to the attack orchestrated by the @Conti group, which was specifically targeted at a criminal group. This attack was unrepeatable and did not extend to other sectors during the observation period, nor did it involve any future assaults on the criminal group, which has been categorized as a sector. Therefore, these two points can be regarded as entirely independent in the network.

Given that the diameter of the bipartite graph, which represents the distance between the two farthest points in the network, is 1, and the average path length, which denotes the average distance between the points, is also 1, this statistical measure does not offer any additional insights into the current network. However, the distribution of the weighted degree number indicates a scale-independent pattern (Jeong et al. 2000), signifying that a majority of the nodes have only one connection, while the number of nodes in the network decreases as the number of connections increases (Figure 14). Specifically, 43.16% of the attackers are found to have only one connection, 71.58% have fewer than six connections, and only 13.68% of the attackers have more than 10 connections.

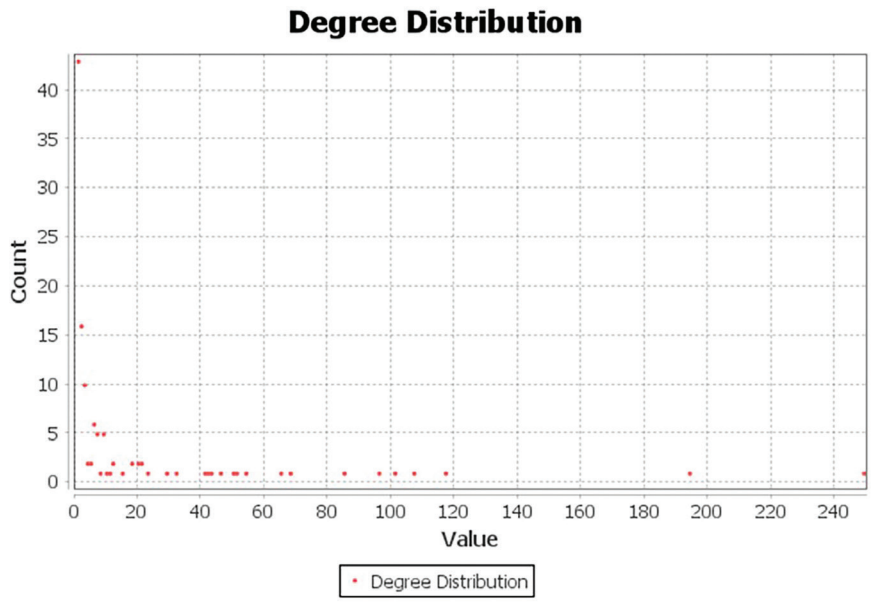

Figure 14. Distribution of the weighted degree number of points in the network (own editing in Gephi, based on CyberPeace Institute database)

In the context of the network's content, the aforementioned observations suggest that the cyberattacks examined are often sporadic and occasional, orchestrated by a single organization, and that just a few organizations have undertaken systematic and organized attacks targeting one or more sectors during the given period. From a

numerical standpoint, this implies that the top 10 organizations responsible for the most attacks constitute over 70% of the total attacks—73.9% to be exact.

In order to gain a more comprehensive understanding of the key components within the network, an alternative visual tool in Gephi is employed. The Force Atlas layout organizes the points in the network based on their weighted degree number, thereby highlighting the strategically significant elements of the network (as depicted in Figure 15).

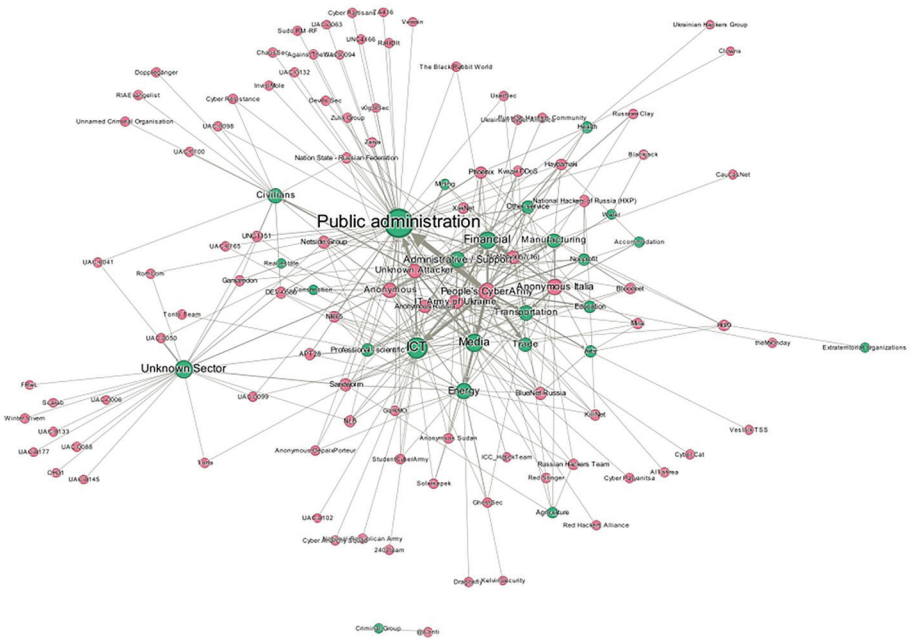

Figure 15. Weighted network of cyberattacks by sector and by attacker, focusing on the key elements of the network
(own editing in Gephi, based on CyberPeace Institute database)

Although the centrality, which quantifies the role and significance of each node in the network, can be computed for bipartite graphs, it does not provide relevant information such as distance and diameter. However, the distribution of the weighted degree number can be leveraged to sort the network based on the nodes with the highest weighted degree number. In this regard, Gephi utilizes this criterion to center the network on the sectors that have been consistently targeted by a greater number of cyberattacks (in descending order of weighted degree: public administration—194, financial—117, ICT—101, media—96, transportation—54) as well as the attackers that have carried out the most attacks during the observation period (in descending order of weighted degree: People's Cyber Army—249, Unknown Attacker—107, IT Army of Ukraine—85, NoName057(16)—67, Anonymous Italia—65). This information facilitates identification of the most targeted sectors and the most active attackers. Notably, Gephi's ordered graph layout illustrates the network's most

significant points from left to right, based on their weighted degree numbers (refer to Figure 16).

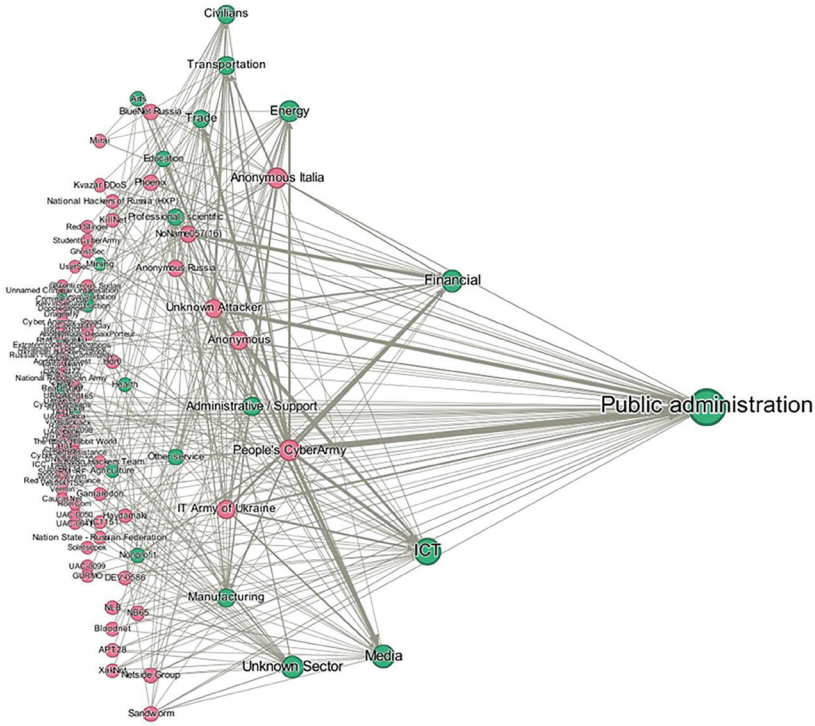

Figure 16. Weighted network of cyberattacks grouped by sector and by attacker, with the network's priority points ranked from left to right (own editing in Gephi, based on CyberPeace Institute database)

However, in order to investigate the characteristics and patterns of the attacks, it is necessary to cluster the points by computing their clustering indices. Gephi facilitates this computation and the resulting network map that visualizes the clusters with ease (as shown in Figure 17).

The program allocates a "branch" to each cluster within the network, resulting in a total of six separate clusters. One of these comprises the two nodes mentioned earlier, representing a distinct component of the network. In the remaining five clusters, it is evident that each cluster terminates in a sector with a high degree number (i.e., the farthest point on the branch from the center of the network), which is also the highest degree number point within the cluster. Subsequently, the points gradually exhibit fewer degree numbers as they approach the center of the network. The primary principle underlying clustering is to group points that are most strongly connected to each other. Thus, in the present network, all the most connected sectors and attackers are grouped together in a cluster. To elaborate, the most frequent

attacker targeting a sector is placed in the same cluster. If an attacker targets multiple sectors and is the most dominant among them, the corresponding sectors are also clustered together.

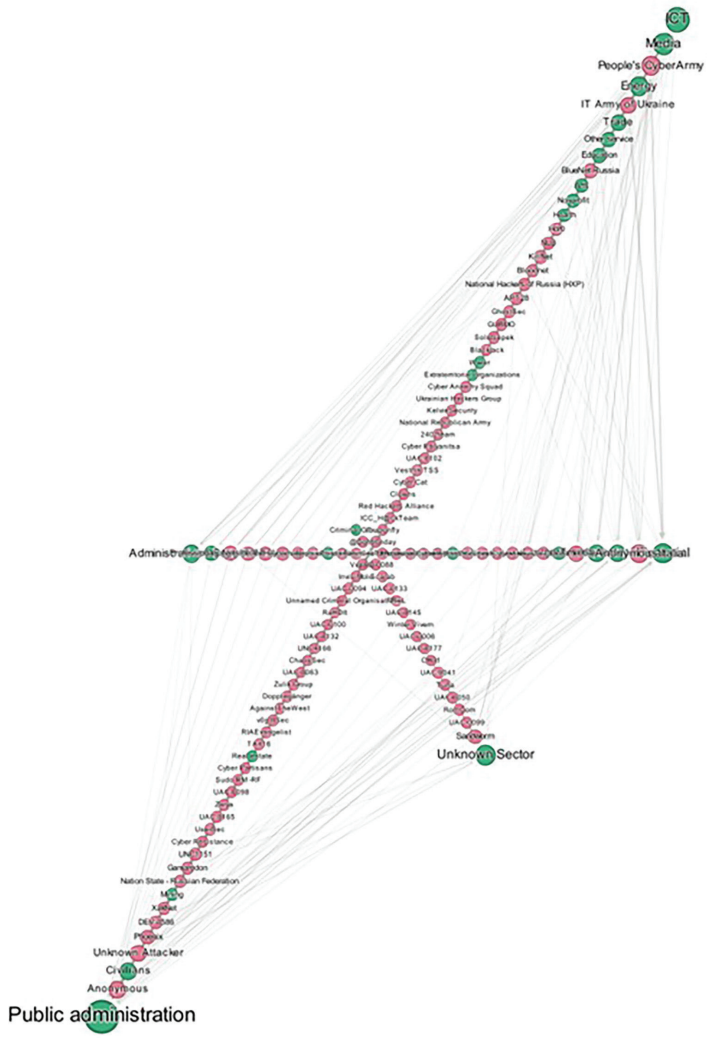

Figure 17. Weighted network of cyberattacks by clusters (own editing in Gephi, based on CyberPeace Institute database)

Clusters offer insights into the nature of attackers and their attacks by highlighting the most vulnerable sectors and those that are collectively susceptible to the same group of attackers. This, in turn, reveals the characteristics and patterns of the attacks and the attackers perpetrating them.

4. Discussion

In contemporary society, the crucial role of IT services in maintaining the operation of critical infrastructures has been widely acknowledged. As a result, cyberattacks targeting IT services have the potential to cause significant disruption to critical infrastructure operations. The Russia–Ukraine conflict has provided a stark illustration of the impact of cyberattacks on critical infrastructures and the security measures available to safeguard these systems. Against this backdrop, the present study aims to analyze the documented cyberattacks that occurred during the Russia–Ukraine conflict between 2022 and 2023, identify sector-specific patterns of cyberattacks, and assess any changes in the frequency and severity of these attacks. To achieve this research objective and test the formulated hypotheses regarding the sectors most vulnerable to cyberattacks and the potential frequency and severity of these attacks, a range of scientific research methods was employed.

Drawing on the conducted studies, our results are as follows:

R1: The data analysis indicates a semiannual periodicity in the frequency of attacks during the study period. It can be inferred that the winter season of 2023 witnessed the highest number of attacks, distributed monthly, compared to the other periods under consideration.

R2: As the sector-wise analysis shows, the majority of the cyberattacks were directed toward the public administration sector.

R3: The analysis conducted during the reviewed period predominantly identified DDoS attacks.

R4: The results of our research indicate that state-sponsored groups have perpetrated cyberattacks with greater frequency and diversity.

This paper aims to enhance our understanding of attackers' preferences for different methods of cyberattacks and to identify the most critical sectors that require protection. Additionally, it provides valuable insights into the attack patterns and networks of attackers, while also offering a forecast of the attack trends likely to emerge during the years 2022 and 2023 of the Russia–Ukraine conflict.

References

Aviv, Itzhak, and Uri Ferri. "Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem." *International Journal of Critical Infrastructure Protection* 43 (2023): 1–31. https://doi.org/10.1016/j.ijcip.2023.100637

Chukhua, Ilona. "Russian Aggressive Cyber-Policy during Russia-Ukraine War." In *Cyber Security Policies and Strategies of the World's Leading States*, edited by Nika Chitadze, 224–238. Hershey, PA: IGI Global, 2023.

CyberPeace Institute. 2023. "Cyber Attacks in Times of Conflict." Accessed March 10, 2024. https://cyberconflicts.cyberpeaceinstitute.org/

CyberPeace Institute. 2023. "Data & Methodology." Accessed March 10, 2024. https://cyberconflicts.cyberpeaceinstitute.org/

Feledy, Botond, and Csaba Virág. "An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies." *Scientia et Securitas* 3, no. 1 (2022): 12–18. https://doi.org/10.1556/112.2022.00091

Fiala, Otto C., and Jim Worrall. "Unconventional Warfare in the Information Environment." In *Great Power Cyber Competition: Competing and Winning in the Information Environment*, edited by David V. Gioe and Margaret W. Smith, 157–172. Abingdon, UK: Routledge, 2024.

Fortinet. 2024. "What Is DDOS Attack?" Accessed March 10, 2024. www.fortinet.com/resources/cyberglossary/ddos-attack

Givens, Austen, Max Gorbachevsky, and Anita Biernat. "How Putin's Cyberwar Failed in Ukraine." *Journal of Strategic Security* 16, no. 2 (2023): 96–121. https://doi.org/10.5038/1944-0472.16.2.2099

Hoffman, Mark, and Martin O. Hofmann. "Challenges and Opportunities in Gray Zone 'Combat'." In *Advances in Cross-Cultural Decision-Making: Proceedings of the AHFE 2017 International Conference on Cross-Cultural Decision Making, July 17–21, The Westin Bonaventure Hotel, Los Angeles, California, USA*, edited by Mark, Hoffman, part of the series Advances in Intelligent Systems and Computing (AISC, vol. 610), 156–166. Cham: Springer, 2018.

Jeong, Hawoong, Bálint Tombor, Réka Albert, Zoltán Oltvai, and Albert Barabási. "The Large-Scale Organization of Metabolic Networks." *Nature* 407, no. 6804 (2000): 651–654. https://doi.org/10.1038/35036627

Karvalics, László. "Az információs társadalom gondolatának európai szálláscsinálója." *Információs Társadalom* VII, no. 1 (2007): 124–136. https://dx.doi.org/10.22503/inftars.VII.2007.1.13

Kaspersky Lab. 2024. "Website Defacement." Accessed March 10, 2024. https://encyclopedia.kaspersky.com/glossary/deface/

Kostyuk, Nadiya, and Aaron Brantly. "War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation." *Contemporary Security Policy* 43, no. 3 (2022): 498–515. https://doi.org/10.1080/13523260.2022.2093587

Krzanowski, Roman. "Information: Modern Concepts." *Információs Társadalom* XXIII, no. 4 (2023): 73–91. https://dx.doi.org/10.22503/inftars.XXIII.2023.4.5

Lonergan, Erica, Margaret Smith, and Grace Mueller. "Evaluating Assumptions about the Role of Cyberspace in Warfighting: Evidence from Ukraine." In *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 85–102. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2023. https://doi.org/10.23919/CyCon58705.2023.10182101

Lunn, Stephen. "Human Security and the Digital Threat: Russia and Ukraine." In *Perspectives on Justice, Indigeneity, Gender, and Security in Human Rights Research*, edited by Laura E. Reimer and Katerina Standish, 263–283. Singapore: Springer Nature, 2023.

Majó, Zoltán. "Úton az információs társadalom felé: tudjuk-e, hová tartunk?" *Információs Társadalom* VI, no. 1 (2006): 30–39. https://dx.doi.org/10.22503/inftars.VI.2006.1.4

Miron, Marina, and Rod Thornton. "Russian Cyberspace Operations Against Ukraine in the 2022 War: How Effective Have They Been and What Lessons for NATO Can Be Drawn?" In

Great Power Cyber Competition: Competing and Winning in the Information Environment, edited by David V. Gioe and Margaret W. Smith, 57–72. Abingdon, UK: Routledge, 2024.

Traficom (Finnish Transport and Communications Agency National Cyber Security Centre). 2023. "Cyber and Information Influence Activities Come Together in the Hack and Leak Phenomenon." Accessed March 10, 2024. www.kyberturvallisuuskeskus.fi/en/ajankohtaista/hack-and-leak

Office of Public Affairs, United States Department of Justice. 2023. "Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies." Accessed March 10, 2024. www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware?fbclid=IwAR0hcMYb-92uYkmevnCXcScdeQXHO2iFTFJhVA6h-1U6YdipSms87J7I-uk

Security Alliance Limited. 2022. "The Changing Landscape of Hacktivism." Accessed March 10, 2024. www.secalliance.com/blog/the-changing-landscape-of-hacktivism?fbclid=IwAR2S5nByA9uV_rP5AuBwHR7m2lDyZcDEl7lCkGz3FzWunWSPrLcRQcuUtNA

Willett, Marcus. "The Cyber Dimension of the Russia–Ukraine War." *Survival* 64, no. 5 (2022): 7–26. https://doi.org/10.1080/00396338.2022.2126193