The Realities of Cyberwar as Perceived in Ukrainian Society: Sociological Analysis

UDC: 316.485.26; 316.772.5; 355.01 DOI: https://doi.org/10.15421/172367

Shelomovska Oksana
Ph.D., Assoc. Prof., https://orcid.org/0000-0003-3409-9435, o_nix@ukr.net
Sorokina Liudmyla
Ph.D., Assoc. Prof., https://orcid.org/0000-0003-4875-2896, sludmila1906@gmail.com
Dniprovsky State Technical University (Kamianske, Ukraine)

Abstract

The topic is relevant due to insufficient conceptual development of the problems of cyberwar as a social phenomenon and the lack of comprehensive sociological analysis of the perception of its realities by modern Ukrainian society based on empirical material. The paper presents and analyzes the results of a sociological survey on the impact of cyberwar on Ukrainianhood. The authors discuss the essence and provide definitions of the concepts "cyberwar", "cyberweapons" and "military cyberattack". The research discusses the threats to cyber security of Ukraine and it has been found that cyber war is perceived by the population as one of the components of the Russian-Ukrainian war. The research considers cybervandalism, propaganda attacks, information gathering, service denial attacks, interference with the operation of equipment, and critical infrastructure objects as acts of hostilities in cyberspace. The survey conducted allowed the authors to determine the level of awareness about them and the consequences of their perception by society. The importance of the human factor in cyber warfare is emphasized and informational and psychological special operations are identified as one of its directions. The paper establishes the level of influence of information and psychological special operations on the population, as well as presents and analyzes statistical data on cyber attacks in Ukraine and globally. The results of the study indicate that almost 70% of Ukrainians have personally encountered propaganda attacks, and more than half of the respondents – unauthorized collection of information and service failure. Almost every second Ukrainian has been a victim of a mass software, application or other resource failure on the Internet once or number of times. Almost two-thirds of Ukrainians have at least once become a victim of information warfare operation, with more than 90% of the people realizing the level of threats from them and their negative impact on moral and psychological state of the population. It was established that the efforts of the Ukrainian cyber army are highly evaluated by the population. It is emphasized that cyber warfare is an important factor in all modern and future military conflicts, and the majority of the world population is aware of this.

Keywords: cyberwar, cyberattack, cyberweapons, cyberspace, cyber threat, propaganda, information and psychological special operations, cyber army

Реалії кібервійни в сприйнятті українського соціуму: соціологічний аналіз

Шеломовська Оксана, Сорокіна Людмила
Дніпровський державний технічний університет (Кам'янське, Україна)

Анотація

Актуальність теми зумовлена недостатньою концептуальною розробкою проблем кібервійни як соціального феномена та відсутністю комплексного соціологічного аналізу сприйняття її реалій сучасним українським соціумом на основі емпіричного матеріалу. Представлено та проаналізовано результати соціологічного опитування щодо впливу кібервійни на українство. Розглянуто сутність і надано авторські дефініції поняттям «кібервійна», «кіберзброя» і «військова кібератака». Досліджено реальні загрози кібербезпеці, з якими стикається Україна і виявлено, що кібервійна усвідомлюється населенням одним з напрямків російсько-української війни. Розглянуто кібервандалізм, пропагандистські атаки, збір інформації, атаки типу відмови в обслуговуванні, втручання в роботу обладнання та таки на об'єкти критичної інфраструктури як акти бойових дій в кіберпросторі. За результатами анкетування встановлено рівень проінформованості про них та наслідки сприйняття їх соціумом. Наголошено на значенні людського чинника у кібервійні та визначено інформаційно-психологічні спецопереації одним з її напрямків. Встановлено рівень поширення впливу інформаційно-психологічних спецоперацій на населення. Наведено і проаналізовано статистичні дані щодо кібератак в Україні та світі. Результати дослідження свідчать, що майже 70% українців особисто стикалися з пропагандистськими атаками, а більше половини опитаних – з несанкціонованим збором інформації та відмовою сервісів. Практично кожен другий українець один чи декілька разів був жертвами масового збою програмного забезпечення, додатків або інших ресурсів у мережі інтернет. Маже дві третини українців хоча б раз ставали жертвою ІПСО, але при цьому більш ніж 90% розуміє рівень загроз від ІПСО і їх негативний вплив на морально-психологічний стан населення. Встановлено, що діяльність українського кібервійська дуже позитивно оцінюється населенням. Наголошено, кібервійна є важливим фактором в усіх сучасних і майбутніх військових конфліктах і це усвідомлює більшість світового населення.

Ключові слова: кібервійна, кібератака, кіберзброя, кіберпростір, кіберзагроза, пропаганда, інформаційно-психологічні спецоперації, кіберармія

Стаття надійшла / Article arrived: 16.06.2023 Схвалено до друку / Accepted: 31.08.2023

Introduction.

The issue of cyber warfare is extremely relevant in modern conditions, since the full-scale Russian-Ukrainian war is the largest military conflict of the 21st century, which, along with combat operations at the front, also includes large-scale cyber operations on both sides. Cyber attacks on critical infrastructure, cyber espionage and cyber propaganda are all modern realities that have become almost commonplace and are actively used within the framework of the conflict. Today, the cyber attacks, including those aimed at various objects of critical infrastructure, are carried out every minute, and their intensity is constantly increasing. Every year sees them become more and more sophisticated and destructive for the counties, organizations and citizens of the world. The British magazine The Economist already defines cyberspace as the fifth sphere of war, after land, sea, air and space, and paraphrasing K. Clausewitz, it can be argued that cyberwar is a modern tool of the enemy to make the adversary submit to their will.

The topic of cyberwar is extremely topical, but its conceptual scope is yet to be elaborated. Despite its considerable relevance, in the modern scientific space there are practically no scientific publications dedicated to the sociological dimension of cyberwar and its specific aspects. The available articles focus mostly on its normalization in the legal field, highlighting the essence of the phenomenon of cyberwar and its features, analyzing the most famous cyberattacks, etc. It is only recently that scientific investigations of this phenomenon began to appear in sociological and political discourses. In this context it is worth mentioning the works by D. Dubov, M. Yenin, Yu. Zavhorodnaya, O. Zaporozhets, M. Kuts, Yu. Seda, A. Slobodianyuk, M. Trebin, O. Severynchik, P. Fedorchenko-Kutuyev, and others. Paying tribute to the scientific work of all researchers, we note that at the moment, the topic of cyber warfare has not been considered comprehensively, and its practical sociological studies are practically absent. A comprehensive analysis of the realities of cyber warfare as perceived in modern Ukrainian society is important for understanding the impact of this phenomenon on various spheres of social life.

Thus, the **purpose of our article** is to provide a comprehensive study of cyberwar as a social phenomenon and conduct a sociological analysis of the perception of its realities by modern Ukrainian society based on empirical material.

Results.

In modern scientific discourse, there is no unified interpretation of cyberwar as a social phenomenon, and it can be interpreted differently. Thus, one of the earliest interpretations defines cyber warfare as the conduct or preparation for the conduct of military operations in accordance with the principles of information influence and it was noted that it involves purposeful disruption of work or destruction of information and communication systems which also include elements of military culture (Arquilla & Ronfeldt, 1993). In contrast to this, it has become quite frequent to define cyberwarfare not as a synonym for information operations, but as their component, along with psychological operations, military cunning, security operations (Beidleman, 2009). From a practical point of view, cyber warfare is defined as the actions of one country aimed at penetrating the computers or networks of another country to cause damage or destruction (Clarke & Knake, 2011). Currently, the concept of cyber war is used both in a broad sense (as systematic actions of countries against each other in cyber and information space) and in a narrow sense, when it comes to a series of cyber attacks or acts of cyber vandalism.

In our research, we will proceed from the understanding of cyberwar as the highest degree of struggle of countries or other politically organized subjects in the virtual electronic space, which is embodied in a coordinated system of permanent mass actions using electronic and digital means, mainly related to information technologies (state weapons), on a sufficient scale and with a high level of intensity, for attacks on the appropriate means of the adversary, in order to cause damage or disrupt their functioning, undermine trust in the power structures and disrupt overall state's activities.

Today, military structures use cyberspace as a kind of a "parallel battlefield", and aggressive actions in information and cyber space are used to enhance the effect of traditional operations with the use of conventional offensive weapons. This is confirmed by statistical data on the number of cyber attacks. According to Microsoft, as of June 2021, the United States (46%), Ukraine (19%) and Great Britain (9%) lead the ranking of the countries most attacked by criminals from other countries and suffering the most from cyber attacks. The greatest threat among all countries is Russian hackers, carrying out 58% of all attacks (Special report: Ukraine, 2022).

Cyber attacks preceded the full-scale Russian-Ukrainian war. If in 2020, there were recorded 800 full-fledged cyber attacks in Ukraine, in 2021 - 1400, and in 2022 their number exceeded 4000. Immediately on the eve and at the beginning of the war, Russia carried out perhaps the world's largest salvo of destructive cyber attacks on hundreds of systems of power organs, IT sector, energy and financial companies. The purpose of these attacks was to obtain information for direct military operations and to undermine the authority of the Ukrainian government. According to the State Service for Special Communications and Information Protection, during 2022, Russia carried out 2194 cyber attacks on state bodies. A quarter of them targeted government agencies, while others attacked systems in the energy, security and defense sectors, telecommunications, financial sector, and logistics (Cyber warfare is a modern reality, 2023). At the same time, as a rule, cyber and military operations shared common goals – criminals engaged in cyber

attacks tended to choose the same geographic locations or sectors as Russian troops, and around the same time.

However, according to foreign intelligence, there were much more Russian cyber attacks against NATO and Ukraine than publicly disclosed, and Ukraine largely repelled them (Sakellariadis & Miller, 2023). As evidenced by Thales's Cyber Threat Intelligence data, a new geography of attacks has been formed over the past 12 months – if at the very beginning of a full-scale war, the majority of incidents concerned only Ukraine (50.4% in the first quarter of 2022 against 28.6% in the third quarter), EU countries observed a sharp increase in conflict incidents over the past six months – 46.5% against 9.8% of global attacks (From Ukraine to, 2023).

However, despite the fact that a purely cyber war remains unlikely for a long time, the majority of the Ukrainian population – almost 93% - considers cyberspace to be the new battlefield of confrontation between enemy countries, with 77.2% of the respondents noting that hostilities are already occurring in the plane of cyberspace. An even larger share of respondents, namely 81.5%, believes that cyber war is one of the directions of the Russian-Ukrainian war (Fig. 1). These data are the authors' own research coming from a sociological survey conducted by the questionnaire method (n=425 people) in January 2023.

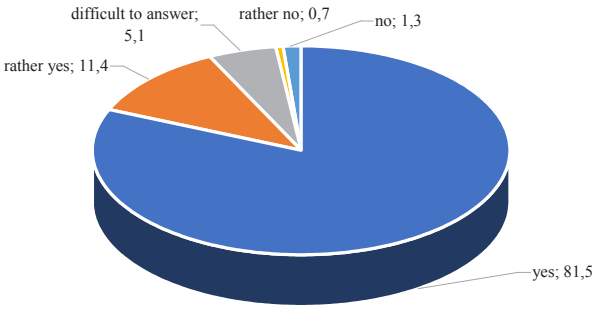

Figure 1. Distribution of respondents' answers to the question "Do you think the cyberwar is one of the directions of the ongoing Russian-Ukrainian war", in %

American experts are also convinced that the Russian-Ukrainian war is being waged in cyberspace and note that Ukraine has thwarted many of the Russian cyberattacks and was able to quickly recover from others, emphasizing the significant preparedness of Ukrainian cyber forces (Sakellariadis & Miller, 2023). Today, we cannot name a single fully successful Russian cyberattack other than the disruption of the Viasat satellite communications network, which disrupted communications across Europe. But no subsequent Russian cyber attack has had visible consequences of comparable military significance, and the rate of attacks plummeted just weeks into the war. In fact, the defense against attacks in cyberspace has proven to be much stronger than the attack.

Cyber threats faced by both ordinary "users" and the country on the whole can generally be divided into three groups: cybercrime, cyberterrorism, and cyberwar. The fundamental difference between these types of threats is that cybercrimes are committed by hackers to improve their financial status or reputation; they are manifestations of hooliganism and acts of vandalism in cyberspace. Cyber-terrorists see the intimidation of a specific country population and damage to the infrastructure for additional pressure on political and ideological opponents as their main goal. Cyber warfare involves coordinated special operations in cyberspace conducted by a certain state against another. According to Cobalt's 2022 Cybersecurity Statistics, 86% of all cyberattacks are motivated by financial gain, with government espionage the second leading motivator for cyberattacks. 560,000 new malware are discovered daily, and the number of malware infections has increased by 87% over the past 10 years (Cybersecurity Statistics, 2023). Such technical and software tools that aim to have a destructive effect on other information systems (viruses, zombie networks, DOS and DDOS attacks) are considered cyberweapons.

The open methods of cyber warfare include cyber attacks and cyber defense, while the covert ones include surveillance, traps and ambushes in cyberspace. Generally speaking, a cyber attack is a deliberate activity to alter, damage, undermine or destroy computer systems or networks used by an adversary, or the information and/or programs resident in them or transmitted through those systems or networks (Lin, 2012).

Cyberattacks can be offensive and defensive and are carried out using computer equipment in particular or the capabilities of cyberspace in general, and most often – with the use of specially developed means, that is, cyber weapons. In our opinion, cyber attacks can be defined as acts of military aggression if they are carried out with the direct participation or under the patronage of enemy states and are aimed at the destruction of various types of critical infrastructure objects, while the consequences of such acts of aggression can be extremely destructive and turn into real threats to people's lives. A special feature of cyber attacks in this case should be coordination and systematicity.

In the context of cyber warfare, the following types of attacks are usually distinguished:

- cybervandalism – involves changing or destroying the content of a website or page in social networks with the purpose of causing harm, for example, hacking a page and replacing its content with offensive or propaganda images, as well as targeted and permanent destruction of data with the purpose of causing harm;
- propaganda attacks – sending and posting of messages aimed at spreading among the public certain statements, facts, arguments in favor of the enemy, aimed at establishing control over the minds and thoughts of people;
- collection of information – hacking of private pages or servers to collect secret information or replace it with false information useful to another state;

- denial-of-service attacks (DoS, DDoS attacks) – attacks from various computers to disable the functioning of websites or computer systems; such attacks prevent legitimate users from accessing a website by flooding it with forged requests and forcing the website to process those requests;
- interference in the operation of equipment is an attack on computers that control the operation of civilian or military equipment, which leads to its shutdown or breakdown;
- attacks on critical infrastructure objects – attacks on computers, and automation systems, technological process management, which ensure the vital activity of cities, their infrastructure, such as telephone systems, water supply networks, electricity, fire protection, transport, etc.

Global statistics as of 2023 show that there take place more than 2200 attacks daily, which amounts to almost one cyberattack every 39 seconds. The most common cyber attack is hacking, its frequency being 45%. Errors as causal events and social attacks account for 22% each, malicious software – 17 %, misuse by authorized users – 8%, and physical attacks for 4% (Cybersecurity Statistics, 2023).

According to data of the sociological survey conducted by us, it was established that the vast majority of citizens are aware of all of the above types of attacks, but the undisputed leaders are propaganda attacks and information gathering – 84% and 77.3%, respectively (Table 1).

Table 1.
Awareness of cyber attacks and personal experience, in %, according to the author's survey

Kinds of attacks	Distribution of answers to the question: "Which of the presented kinds of attacks do you know", %	Distribution of answers to the question: "Which kinds of Internet attacks did you face personally?", %
Vandalism	64,7	34
Propaganda	84	69,3
Collection of information	77,3	52,7
Service failure	74	52
Interference in the functioning of equipment	49,3	15,3
Attacks on critical infrastructure	60	17,3

There is quite a large number of groups of people who are aware of such cyber attacks as service denial (74%), vandalism (64.7%) and attacks on critical infrastructure (60%). The smallest number of respondents are aware of cases of interference in the operation of equipment with the help of cyber tools, which, in our opinion, is due to the fact that typically the interference in the operation of equipment at current stage of the Russian-Ukrainian war is more connected with real physical destruction than with cyber influence.

Simultaneously, it was established that 69.3% of respondents personally encountered propaganda attacks, 52.7% did so with unauthorized collection of information, and 52% - with service denial. Almost one in three respondents encountered manifestations of vandalism, one in six with attacks on critical infrastructure, and one in seven with interference in the operation of equipment. At the same time, it was found that more than half of citizens, namely 55.3%, were victims of a mass failure of software, applications or other resources on the Internet one or multiple times. Some respondents witnessed attempts of DDoS attacks, for example, on applications or official websites of the country's leading banks. At the beginning of the war, thousands of volunteers participated in cyber actions against Russia and to protect Ukrainian network targets.

A fairly significant share of respondents have experienced attacks using malicious software – 60.7%, of which 52.7% of gadgets were attacked once or multiple times. Only every third of those surveyed noted the absence of virus attacks in their virtual life, which may indicate the effectiveness of anti-virus software and general awareness of cyber security issues.

While the tools of cyberspace conflict are technology-based, the methods are human-centered (Lin, 2012). Indeed, the real struggle for cyber security concerns not only technical issues, but also a struggle for proper human behavior. K. Clausewitz defined war as an act of human relations and emphasized the importance of the moral factor in war. According to Cybint, nearly 95% of all digital breaches are due to a human error (Cybersecurity Statistics, 2023). Obviously, modern military operations in the ICT environment are not limited only to informational and technical influence: informational humanitarian or cognitive influence on an individual or collective consciousness is also a part of them. In this context, it is worth paying attention to information and psychological special operations (IPSO) in cyberspace. The types of IPSO in cyberspace include the dissemination of pseudo-insider information, the publication of fake news about the achievements of the occupying forces, the publication of fake photos and video materials with the aim of discrediting the efforts of the Armed Forces and the country's leadership, as well as the distribution of materials openly intimidating the population and undermining the morale in the rear and on the front line.

The sociological survey permitted the authors to establish that 65.4% of respondents had at least once been a victim of IPSO, as opposed to 21.3% who were exposed to propaganda influence (Fig. 2).

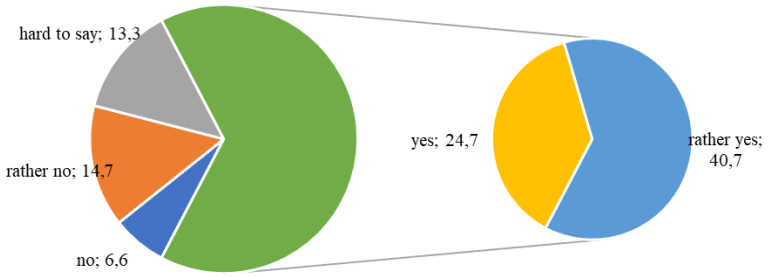

Figure 2. Distribution of answers to the question "Have you been a victim of information and psychological manipulation at least once since February 24, 2022?", in % according to the author's survey

It is quite positive that more than 90% of the population (70% - fully and 20.7% - rather so) are aware of the threat of IPSO and define it as a weapon aimed at undermining the moral and psychological state and, accordingly, select the information resources more consciously. Despite its skills and experience in disinformation, Russian propaganda failed to hide the indisputable evidence of aggression, violations of international law and horrific instances of human rights abuses that were made public on many non-governmental resources.

The scope and scale of penetration of information and communication technologies is growing steadily every minute and carries with it not only advantages, but also threats. Sociological studies show that cyber conflicts and cyber wars as their highest manifestation disturb not only the population of Ukraine, but also the one of such countries as the USA, Great Britain, Germany, etc. In particular, in April 2022, 93% of Americans fear that a foreign country may wage a cyber war against the United States. Conversely, only 19% of respondents were "100% confident" of the government's ability to protect citizens from the effects of cyber warfare. More than one-third of Americans (35%) are taking steps to prepare for cyber warfare (Konkel, 2022). About 75% of German citizens stress that they fear cyberwars, 55% fear cyberwars without military escalation, and 20% are concerned about cyberwars with subsequent military escalation (Opinions about fear, 2022).

It must be stressed that the confrontation of countries in global cyberspace is extremely active, as evidenced, in particular, by the creation of special cyber units in various countries and the accumulation of funds invested in ensuring cyber security. In the Ukrainian context, the cyber army welcomed to its ranks not only IT workers, but also many active ordinary citizens who, in the first months of the war, participated in attacks on Russian digital resources. Our sociological survey found that 88.5% of the surveyed respondents are well aware of the creation of the cyber army of Ukraine, however, the evaluations of its activities somewhat vary, although they are mostly positive. It was found that 33.8% of respondents evaluate the efforts of the Ukrainian cyber army unequivocally positively and 39.2% - rather positively. Negative evaluations are extremely rare and occur only in 2.7%. The nature of the answers may indicate insufficient awareness of the respondents and the specific nature of the activities of cyber activists. The most impressive thing about a military cyber attack is that it is invisible to the naked eye. If it succeeds, it becomes known that the site has stopped working. But the work of specialists on its detection and counteracttack in most cases remains invisible to ordinary citizens.

Conclusions.

Thus, our analysis allowed us to confirm that cyber war is a reality and Ukrainian society is fully aware of it. The numerous attacks that were directed at Ukraine before and during the full-scale invasion proved that cyberspace is indeed a recent field of military struggle. Cyber war is a set of actions of politically organized subjects in cyberspace with the use of cyber weapons in order to cause economic, informational and physical damage to the enemy. The vast majority of Ukrainians emphasize that hostilities are already taking place in cyberspace and believe that cyberwar is one of the directions of the Russian-Ukrainian war. The most common cyberattacks, and in fact, combat operations in cyberspace, are cyber vandalism, propaganda attacks, information gathering, denial-of-service attacks, interference with the operation of equipment, attacks on critical infrastructure objects. According to the results of the author's sociological survey, it was established that almost 70% of respondents personally encountered propaganda attacks, more than half of the respondents suffered from unauthorized collection of information and denial of services. Almost one in two Ukrainians has been a victim of a mass failure of software, applications or other resources on the Internet once or multiple times. Information attacks are carried out every day, both on government structures and on ordinary people through social engineering. Almost two-thirds of Ukrainians have at least once become a victim of IPSO, but at the same time, more than 90% realize the level of threats from IPSO and their negative impact on the moral and psychological state of the population. The statistics of attacks carried out around the world in the economic, political and other sectors is only growing, which indicates that the confrontation between the

world's leading political and economic structures has also moved into the plane of cyberspace.

Cyber weapons, along with disinformation, manipulation of public opinion, economic warfare, sabotage, etc., are already included in the arsenal of tools of war. In the context of ongoing Russian-Ukrainian war cyberattacks have turned out to be a new form of weapon, although they can change the situation in future conflicts dramatically. Typically, history shows that a new form of weaponry used in the current conflict becomes significantly more advanced, more sophisticated, and more destructive in the next major conflict. Paradoxically as it may seem, but should a cyberwar be waged without human participation, in which computer programs make their own decisions (if such a thing ever takes place), it would be much more brutal than human bloody confrontations. The ongoing Russian-Ukrainian war already showed how much more advanced cyber defense and cyber attack technologies have become. Ukrainian defenders and their partners did the hard work very well, deploying cyber defenses at an unprecedented scale and depth, responding quickly to a cyber attack, and Ukrainian society proved resilient, both on the physical and social battlefields.

REFERENCES

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar Is Coming! *Comparative Strategy*, 12/2, 141-65.

Beidleman, W. Scott. (2009). *Defining and deterring cyber war*. Retrieved from https://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf

Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Manhattan: ⁋Ecco.

Cybersecurity Statistics for 2023. (2022, December 27). Retrieved from https://www.cobalt.io/blog/cybersecurity-statistics-2023

Cyberwar is a modern reality: The loudest cyberattacks in Ukraine and the world and ways to protect against them. (2023, January 19). Retrieved from https://psm7.com/uk/security/kibervijna-ce-suchasna-realnist-najguchnishi-kiberataki-v-ukra%D1%97ni-ta-sviti-i-sposobi-zaxistu-vid-nix.html

From Ukraine to the whole of Europe: cyber conflict reaches a turning point. (2023, March 29). Retrieved from https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point

Konkel, F. (2022, May 9). *A consumer survey suggests Americans are taking some steps to prepare for possible cyber warfare*. Retrieved from https://www.nextgov.com/cybersecurity/2022/05/survey-93-americans-fear-cyber-warfare-against-us/366665/

Lin, H. (2012). Cyber conflict and international humanitarian law. International Review of the Red Cross. *Humanitarian debate: Law, policy, action*, 94(886), 515-531.

Opinions about fear of a cyber war in Germany in 2022. (2022). Retrieved from https://www.statista.com/statistics/1345556/fear-of-a-cyber-war-germany/

Sakellariadis, J., & Miller, M. (2023, February 25). *Ukraine gears up for new phase of cyber war with Russia*. Retrieved from https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429

Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. (2022, April 27). *Digital Security Unit*. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd