# CYBER OPERATIONS IN HYBRID CONFLICTS - LESSONS FROM THE WAR IN UKRAINE

**dr inż. Jakub SYTA**[1]

## Summary

This review article presents selected use cases where information technology was used during Russia's war with Ukraine in 2022. The analysis of these events allows to draw conclusions about the effectiveness of the various activities taking place in cyberspace, which may also be relevant in future conflicts. The conclusions relate to the provision of uninterrupted communications, cyber attacks destroying physical infrastructure elements, the use of mobile phones, the effectiveness of OSINT activities, and the effectiveness of disinformation and propaganda activities.

Keywords: cyber security, hybrid conflict, Ukraine

## INTRODUCTION

Despite earlier predictions, Russia's war on Ukraine which began on 24 February 2022, did not involve massive cyber attacks on essential services. Their paralysis was primarily related to a violent kinetic impact, often incidentally targeting civilians. However, it was possible to identify activities carried out in the information and IT domain - both IT (information technology) and OT (operations technology) systems.

The problem that needs a prompt resolution is how to prepare its essential services for the case of massive cyber attacks that could accompany future armed conflicts. This article aims to identify selected phenomena that the Author believes may be particularly relevant in future warfare. The work is written amid an ongoing war when neither the further fate of the war nor the actual consequences of the events described are known. It recalls events performed by the aggressor, the defenders of Ukraine, and their allies. Due to the ongoing struggle, this article heavily relies on news articles and company reports.

[1] Deputy Director of the Maritime Cyber Security Centre, Naval Academy, 69 Śmidowicza St., 81-127 Gdynia, Poland. ORCID: 0000-0002-0115-6432

## LITERATURE REVIEW

As more months of war pass, more studies appear showing the conflict from the perspective of activities carried out in cyberspace. The war in Ukraine is sometimes referred to as the 'first cyber war' because, as shown in this article, the amount of activity carried out in cyberspace is significant. However, the Author would particularly like to emphasise the hybrid nature of the war. It is being conducted not only with the use of regular armed forces, special forces and mercenaries, but there are psychological operations targeting the people of Ukraine, the people of Russia, and the people of countries that disagree with Kremlin policy. Activities carried out in the area of diplomacy are also visible, and economic blackmail plays a very significant role[2]. Therefore, cyber attacks and disinformation activities are only part of a broader whole. Thus, they should rather be seen as a complementary element[3] .

The first publication on upcoming - new developments within the RU-UA conflict appeared even before hostilities began. The use of wiper malware in unprecedented numbers[4,5] indicated that Russia had greatly developed its technical capabilities. Subsequent Russian activity in cyberspace, however, was not just about security breaches. Available studies indicate a significant concentration of activities in the information sphere[6,7] and also a significant involvement of activists who use their technical skills to attack enemies[8].

More than a year after the start of the war, it is clear that this conflict is different from what has taken place so far[9]. It, therefore, requires detailed analyses in

[2] Štrucl D., Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare. Contemporary Military Challenges 2022(2):103-123 2022. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6 https://www.researchgate.net/publication/361569176_russian_aggression_on_ukraine_cyber_operations_and_the_influence_of_cyberspace_on_modern_warfare

[3] Maschmeyer L., Cavelty M. D., Goodbye Cyberwar: Ukraine as Reality Check, Policy Perspectives Vol. 10/3, May 2022 Policy Perspectives Vol. 10/3, May 2022 https://doi.org/10.3929/ethz-b-000549252 https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/2/PP10-3_2022-EN.pdf

[4] Destructive malware targeting Ukrainian organisations, Microsoft 2021 https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[5] Ukraina 2022 na cyfrowym froncie. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzenie, 2023 https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf

[6] Kowalska-Sendek M., Ukraina na cybernetycznym froncie, Polska Zbrojna 2022 https://polska-zbrojna.pl/home/articleshow/36629?t=Ukraina-na-cybernetycznym-froncie

[7] Krzykowski P. Konsekwencje wojny na Ukrainie w wymiarze żywnościowym, ekonomicznym i energetycznym, Roczniki Nauk Społecznych T.15(50) nr 4, Akademia Sztuki Wojennej 2022 https://ojs.tnkul.pl/index.php/rns/article/view/17785/16759

[8] Vicens A., A year of cyberwar' with Russia: An inside look from a top Ukrainian cybersecurity officialm Cyberscoop 2023 https://cyberscoop.com/victor-zhora-ukraine-russia-cyber-war-one-year/

[9] Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape. Mandiant 2023 https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

order to recognise the effectiveness of individual actions and their limitations and also to prepare defensive as well as offensive capabilities in selected areas[10].

## OBSERVATIONS

### The attack on Viasat and the need for some communication

Viasat is the name of a US-registered company providing satellite internet services. Among its customers were the Ukrainian armed forces in February 2022[11]. On 24 February 2022, at around 5 am, just as Russian President Vladimir Putin announced an attack on Ukraine, a devastating cyber attack was launched on thousands of Viasat customers. It wiped the software on client modems, making them inoperable. As a result, the coordinated defence of Ukraine in the first moments of the war was largely hampered[12]. At the same time, thousands of businesses and individuals located in countries not involved in the conflict became victims of the aggression of cyber criminals working for the Russian military[13]. The paralysis lasted for several months, and a private company had to cover the costs associated with distributing thousands of modems and interrupted work.

There are fundamental lessons to be learned from this cyber attack. It showed that it is dangerous for significant organisations to rely on only one Internet provider. There is a need to ensure continuous communication using diverse technologies provided by diverse providers. It is worth mentioning here that after the appeal of the defenders of Ukraine for help and provision of satellite internet, individuals and organisations provided thousands of Starlink kits, and the company itself launched the service in the country in an express mode[14]. As a result, a few days later, advanced attacks were launched to destroy this method of satellite communication. However, Starlink's cyber-security experts managed to recover from this[15].

[10] Drążkiewicz A., Lekcja dla nas, poznajemy techniki przeciwnika. Gen. Molenda o działaniach Rosji w cyberprzestrzeni. Polskie Radio 24. 2022 https://polskieradio24.pl/130/4437/artykul/3088678,lekcja-dla-nas-poznajemy-techniki-przeciwnika-gen-molenda-o-dzialaniach-rosji-w-cyberprzestrzeni

[11] Corera G., Russia hacked Ukrainian satellite communications, officials believe, BBC 2022 https://www.bbc.com/news/technology-60796079

[12] Satter R., Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official, Reuters 2022 https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

[13] Haertle A., Tysiące terminali internetu satelitarnego poważnie uszkodzonych w dniu ataku na Ukrainę Zaufana Trzecia Strona 2022 https://zaufanatrzeciastrona.pl/post/tysiace-terminali-internetu-satelitarnego-powaznie-uszkodzonych-w-dniu-ataku-na-ukraine/

[14] Olszewski D., Elon Musk udostępnia Starlink na Ukrainie, Computerworld 2022 https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie,436628.html

[15] Dunhill J., Pentagon Impressed By StarLink's "Eye-Wateringly" Swift Shut Down Of Russian Cyberattack IFLScience 2022 https://www.iflscience.com/pentagon-impressed-by-starinks-eyewateringly-swift-shut-down-of-russian-cyberattack-63401

This support made the autumn news, in which Elon Musk threatened to shut down Starlink kits in Ukraine[16], all the more surprising. Although he eventually backed down from this, he proved by his behaviour that the means of connectivity provided by private organisations should not be trusted. At the very least, such a significant issue requires redundancy. Where coordination is needed, consideration should be given to using satellite internet, fibre optics, laser, radio links and even copper-based communications. Moreover, it is vital to ensure that communication does not rely solely on solutions that may cease to function overnight due to a business decision or even a whim.

**Cyber attacks destroying physical infrastructure**

"Wiper" is the term for malware that aims to permanently destroy the functioning of IT systems - preferably even physically or at least by damaging the boot sectors of devices to prevent them from being quickly reinstalled. Although such attacks have been known for many years, only isolated cases could be observed.

Just weeks before the invasion, Microsoft issued an urgent warning. It announced that it had managed to identify a number of wipers placed on various essential systems of Ukrainian key service providers[17]. The rapid response meant that they were able to update the software and remove the dangerous code. Had this not been the case, the war might have turned out differently. If the attack had succeeded in massively paralysing internet connectivity, power supply, water supply, and other essential services, Ukrainians would have found it even more challenging to resist massive enemy attacks. This case underlines the need for even more cyber-security monitoring of essential services - making even greater use of machine learning to identify anomalies. It should be emphasised that during the attack on Viasat described in the previous chapter, a wiper was also used, destroying this form of communication for many months.

A very interesting and, at the same time, significant cyber attack was carried out against the Belarusian railway. The Lukashenko government acceded to Russia's expectations and made its territory and infrastructure available to the aggressors to carry out the invasion. However, hackers from the group Belarusian Cyber Partisans succeeded in paralysing train traffic management systems and significantly delaying the transport of Russian tanks[18]. Protecting transport and logistics systems from cyber attacks thus becomes even more necessary.

[16] Khatsenkova S., Ukraine war: Backlash after Elon Musk says he can no longer fund Starlink satellites, Euronews 2022 https://www.euronews.com/2022/10/14/backlash-after-elon-musk-says-he-can-no-longer-fund-starlink-in-ukraine

[17] Destructive malware targeting Ukrainian organisations, Microsoft 2021 *op. cit.*

[18] Palczewski Sz. Białoruscy Cyberpartyzanci atakują systemy kolejowe. Utrudniają transport rosyjskich wojsk na Ukrainę, Cybersefence24 2022 https://cyberdefence24.pl/armia-i-sluzby/bialoruscy-cyberpartyzanci-pomagaja-ukrainie-utrudniaja-transport-sil-okupacyjnych-

The last example relates to a less strategic area but also demonstrates the destructive potential of functionalities built into IT systems - Based on published material, it would appear that Russian soldiers spent a considerable amount of energy looting. Reports available from the Internet are full of examples of situations where they stole all sorts of goods. Among others, several million dollars worth of agricultural equipment manufactured by John Deere was stolen and transported to Chechnya. After the stolen combines arrived at their destination in Chechnya, the thieves realised that they had remotely been permanently disabled using the so-called "kill switch" functionality[19]. Adding flavour to the story is the fact that the moment the tractors were stolen using a military truck marked 'Z', was reportedly recorded by a CCTV camera[20] .

**Mobile phones in the hands of soldiers**

The war resulted in a series of sanctions that, among other things, cut off Russians from many social media platforms. This led to an even greater flourishing of the native social media outlet Telegram. Soldiers' widespread use of mobile phones and the combined rush to appear on social media have led to many pathological situations. Ranks of thugs in Russian uniforms began documenting the war crimes they were committing[21]. Telegram was flooded with accounts of murders, rapes, torture... This, in turn, generated the need to identify these criminals.

Software such as Clearview[22] is considered very controversial. It can be used to identify demonstrators and is, therefore, rarely used in democratic states. However, the conflict in Ukraine has shown that it can be beneficial in certain situations, as the software has been used to identify war criminals. Some of them did not even try to hide their images when recording and reporting on war crimes. Sometimes, however, it was even possible to recognise masked bandits by their eyes or tattoos and thus reach their families with the true message about these 'heroes' mistreating civilians.

In response to the barbaric attack, the Ukrainians began publishing the corpses of the aggressors in varying degrees of decomposition so that the attackers knew what fate awaited them if they did not abandon the fighting. The material posted often ridiculed the fallen, publishing quotes from captured emails or social media posts or documenting the looting they had committed. Identification of killed Russian soldiers

[19] Roth E., Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment. The Verge 2022 https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere

[20] Kuśmierek M., Rosjanie nakradli sprzętu rolniczego za 5 mln dolarów. Wywieźli go do Czeczenii i nie potrafią uruchomić Spider's Web 2922 https://spidersweb.pl/2022/05/rosjanie-nakradli-sprzetu-rolniczego-za-5-mln-dolarow-wywiezli-go-do-czeczenii-i-nie-potrafia-uruchomi.html

[21] Macias A., UN report details horrifying Ukrainian accounts of rape, torture and executions by Russian troops CNBC 2022 https://www.cnbc.com/2022/10/28/russia-ukraine-war-un-report-details-accounts-of-rape-torture-and-executions.html

[22] Hart R., Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database. Forbes 2022 https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/

allowed contacting their friends and families[23] . Reporting the details of the deaths, often very far from the glorious and heroic narrative conveyed by the government media, must have had a significant impact on their loved ones.

At the same time, it is worth noting that other sources were also used to identify the perpetrators. Cases of protests against the attack on Ukraine were not frequent in Russia, but they were brutally suppressed every time. Those arrested were then long tortured, also in police stations[24]. Using data leaked from a popular food delivery app, it was possible to identify those torturing some of the Moscow protesters[25].

**The role of OPSEC and PERSEC**

Many of the actions described earlier were successful as a result of ongoing OSINT activities[26]. This means that their 'protagonists' did not take proper care to protect their identities or actions; in other words, they did not take care of OPSEC[27]. The indiscriminate use of social media directly during operations was one of the most characteristic elements of the war. However, it led to the betrayal of the location in which the material was produced[28,29], as did the material published by journalists[30]. And using fake profiles on dating sites identified the current location of the Russians[31].

The Ukrainian Armed Forces very quickly understood the dangers of sharing information about the location of their forces. They appealed very loudly not to spread information about the movements of their troops. At the same time, eBopor and Diia applications were developed, which allowed civilians to report the location of the

[23] Italiano L., Orecchio-Egresitz H., Ukraine and Russia have weaponised facial recognition - in very different ways. Insider 2022 https://www.businessinsider.com/ukraine-russia-have-both-weaponized-facial-recognition-2022-3?IR=T

[24] Vasilyeva N., Beatings and psychological torture: The fate that awaits Russian dissidents like Marina Ovsyannikova, The Telegraph 2022 https://www.telegraph.co.uk/world-news/2022/03/15/beatings-psychological-torture-fate-awaits-russian-dissidents/

[25] Ashley, How the food delivery app helped Russian women find torturers in the police station. News Rebeat 2022 https://newsrebeat.com/world-news/96916.html

[26] OSINT: Open source intelligence - a way of gathering information based on the use of publicly available data

[27] OPSEC: Operations security - preventing the disclosure of information allowing the identification of operations, including their location

[28] Stokel-Walker C., Russia and Ukraine are both weaponising mobile phones to track troops, New Scientist 2022 https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

[29] Davis B., Speedo-wearing Russian tourist inadvertently reveals the location of Putin's artillery in Crimea, Evening Standard 2022 https://www.standard.co.uk/news/uk/russian-tourist-ukraine-war-putin-target-geolocation-crimea-b1020094.html

[30] Ukraine hits Russian Wagner mercenary HQ in east, BBC 2022 https://www.bbc.com/news/world-europe-62547403

[31] Ankel S., Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up. Business Insider 2022 https://www.businessinsider.in/tech/news/ukrainian-hackers-created-fake-profiles-of-attractive-women-to-trick-russian-soldiers-into-sharing-their-location-report-says-days-later-the-base-was-blown-up-/articleshow/94009908.cms

aggressor's troops in real-time[32,33]. This enabled reconnaissance on a 'crowdsourcing' basis and facilitated the effective elimination of opponents[34].

The issue of eavesdropping on Russian mobile phones has yet to be discussed more widely in open sources. The technical details of the methods used to intercept the content of conversations and transmitted information have yet to be discovered. It is known that initially, Russian troops occupying Ukrainian territory destroyed local base stations. However, the lack of mobile telephony caused considerable confusion in the aggressors' ranks, and thus discontinued this practice. Over time, the Ukrainians began publishing intercepted conversations in which soldiers complained about hunger and mess as well as received instructions from their families about what else to steal[35]. Whether the Ukrainians used downgrade attacks or the calls were intercepted in some other way - is unknown. Also the amount and character of intercepted Russian calls is unknown. It does not although change the fact that possessing mobile phones during hostilities is a weak point in Russian aggression and is very well exploited by the defenders.

At the same time, it is worth noting that the Ukrainians often published intercepted material: videos, photos or instant messaging messages found on the mobile phones of fallen Russian soldiers. Whether these were obtained by bypassing biometric security or computer forensics techniques is jet unknown. However, it is known that the scale of the phenomenon is significant and leads to the identification of more and more war crimes. And the shortcomings of PERSEC[36] affect the Russian military's effectiveness and morale.

**Disinformation and propaganda**

How the Russian authorities and media carried out disinformation is expected to be analysed for years. The blatant lies and illogical arguments were repeated en masse shocking foreign audiences. Strangely enough, they seem to have been accepted unreflectively by a large part of Russian society for a long time. The resistant were arrested and beaten, and the passive crowd absorbed information from the public media. Slogans and symbols aided this. "*Fight against fascism*", "*Liberation of Ukraine*", and the famous "Z" - "Russian patriots" gathered around these symbols. Enemies of the nation were punished for spreading disinformation about the Russian armed forces -

[32] Radzewicz Sz., Ukraińcy mają aplikację, przez którą zgłaszają pozycje wojsk rosyjskich. eWróg został użyty już 200 tys. razy Spider's Web 2022 https://spidersweb.pl/2022/03/ewrog-aplikacja-wskazuje-wojska-rosyjskie.html

[33] Druziuk Y., A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops - here's how it works Insider 2022 https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4?IR=T

[34] Ukrainians use phone applications to spot deadly Russian drone attacks The Guardian 2022 https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo

[35] Russian Soldiers Phone Calls https://www.nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html

[36] PERSEC: Personal security, prevention of disclosure of personally identifiable information.

including calling the invasion of Ukraine a 'war' with no 'special operation'[37]. It should be emphasised that this type of propaganda activity was not limited to Russian territory only. The activities of so-called '*useful idiots'*, who significantly increased their activity with the outbreak of war, could very clearly be observed in neighbouring countries[38].

At the time of the attack, Ukraine also launched a massive propaganda campaign on social media. A legend was built around the defence of Snake Island with the famous quote "*Русский военный корабль, иди* нахуй"[39] . The legendary pilot "Spirit of Kyiv" appeared in the public space[40]. The brave Ukrainian tractor drivers gained international fame, which led even Finland to announce the relocation of tractors closer to the border in response to Russian threats[41]. On the other hand, looters in uniform stealing washing machines, fridges and even pots and flip-flops were ridiculed without resistance. Many of these soldiers from one of the world's most powerful armies were later tracked down by getting information from shipping companies about the shippers and packages they were sending to their homes[42].

Propaganda was also carried out more actively - using cyber attacks, i.e. through so-called 'hacktivism'. The first visible activities occurred just before the war when some Ukrainian websites were modified by posting information about Poland's planned attack on Ukraine[43]. However, from the moment the war began, the most visible activities were those of various hacktivist collectives countering the policies of the Russian Federation. Simultaneously with the attack on Ukraine, they launched massive cyber attacks targeting various Russian entities. Administrations, financial institutions, media outlets, key service operators and even private companies - all became targets. On several occasions, hackers took over the TV signal of Russian state-run media outlets publishing factual information about the war[44]. They broke the security of cash

[37] Russia fights back in information war with jail warning, Reuters 2022 https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/

[38] Stodolak S., Zbiór pożytecznych idiotów jest coraz większy. Dlaczego uwierzyli Putinowi? Dziennik Gazeta Prawna 2022 https://www.gazetaprawna.pl/magazyn-na-weekend/artykuly/8413199,pozyteczni-idioci-putina-rosja-stone-kusturica-rourke.html

[39] Battle of Snake Island Русский военный корабль, иди на хуй https://www.youtube.com/watch?v=6_B1m5iNndg

[40] Michalk K., Duch Kijowa - bohater czy miejska legenda?, RMF 2022 https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-duch-kijowa-bohater-czy-miejska-legenda,nId,5884226#crp_state=1

[41] Finowie wyśmiewają ruchy wojsk rosyjskich przy granicy. Wysyłają swój "specjalny sprzęt", Onet 2022 https://wiadomosci.onet.pl/swiat/finowie-wysmiewaja-ruchy-wojsk-rosyjskich-przy-granicy-pokazuja-traktory/zysdn71

[42] Coynash H., Belarusians name Russian soldiers caught on camera sending goods plundered in Ukraine to Russia, Kharkiv Human Rights Protection Group 2022 https://khpg.org/en/1608810358

[43] Konieczny P. Ktoś chciał nas wplątać w cyberkonflikt z Ukrainą https://niebezpiecznik.pl/post/ktos-chcial-nas-wplatac-w-cyberkonflikt-z-ukraina/

[44] Smith A., Anonymous news - live: Russian TV hacked with Ukraine footage in 'biggest op ever seen'. Yahoo News 2022 https://news.yahoo.com/anonymous-news-live-russian-tv-090008311.html

registers by causing information about the war to be printed on receipts[45,46], they broke the security of companies doing business in Crimea by publishing images of them on the Internet[47] and they also published documents stolen from many Russian entities. These actions were gaining a great deal of international support.

Russia's aggression unleashed a spark that caused not only hackers to decide to defend Ukrainians, but many others decided to get involved in some way by responding to the appeal of Ukrainian Minister of Digitalisation Mykhailo Fedorov[48]. Some used their computers to launch DDoS attacks on Russian institutions using dedicated software[49]. Others conducted OSINT activities identifying war criminals. Still, others were involved in the creation and use of 1920.io, through which millions of text messages were sent to random Russian mobile phone numbers obtained through various leaks[50]. These messages were aimed at spreading the true image of the war.

Although the activities of the collectives were not visibly coordinated, the activities carried out certainly involved the time of Russian cyber-security experts. They fostered truthful information about the war in public. However, some of the activities, such as the theft and publication of personal data of Russian soldiers and their associates, the publication of information of essential service operators, internal information from banks or the identification of the business connections of Russian oligarchs, may have had a more significant impact on the fate of the war than it may first appear. The lack of anonymity of Russian soldiers and the melting fortunes of the oligarchs and their families could have impacted the progress of the "armed operation".

Gaining international sympathy for the Ukrainians was crucial. As often seen in other conflicts, the usual apathy of the crowds was overcome by messages from the tormented President Volodymyr Zelensky and memes ridiculing the Russian aggressors. This, among other things, has contributed to the popularity of online fundraisers collecting medicine, uniforms, bulletproof vests and even Bayraktar drones or 'kamikaze' drones such as Warmate circulating ammunition... In the author's opinion,

[45] Kotowski A., GhostSec zhakował drukarki w Rosji. Zdalnie drukują informacje o wojnie na Ukrainie. Komputer Świat 2022 https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/ghostsec-zhakowal-drukarki-w-rosji-zdalnie-drukuja-informacje-o-wojnie-na-ukrainie/hrsft0c

[46] Mazurkiewicz P., „Putin zabija" na rosyjskich paragonach. Anonymous włamali się do drukarek. Rzeczypospolita 2022 https://cyfrowa.rp.pl/bezpieczenstwo/art35915801-putin-zabija-na-rosyjskich-paragonach-anonymous-wlamali-sie-do-drukarek

[47] Hackers play Ukrainian songs https://www.reddit.com/r/UkraineWarVideoReport/comments/ww11u3/hackers_play_ukrainian_songs_and_watch_the/

[48] Szpor G., Gryszczyńska A., Hacking in the (cyber)space. GIS Odyssey Journal 2022 | Vol. 2, no. 1 | 141:152 https://doi.org/10.57599/gisoj.2022.2.1.141 https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e50da523-a3b5-48f8-91e3-6369a2d8edf1

[49] Anshori M. F., Db1000n Software as Ukraine's Military Utility to Counter Russian Invasion in 2022.Jurnal Pertahanan 8(2):198-210. https://doi.org/10.33172/jp.v8i2.1683 https://www.researchgate.net/publication/363158743_Db1000n_Software_as_Ukraine's_Military_Utility_to_Counter_Russian_Invasion_in_2022

[50] Vail E., 'We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship, The Record 2022 https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship

these propaganda activities, songs, memes, social media posts, or involving celebrities allowed the Ukrainians to achieve one of the most important goals. The international community has ceased to be indifferent and has taken a keen interest in the details of the conflict by offering its assistance.

Unsurprisingly, however, the negative effect of these measures has been to raise the security level of Russian entities in cyberspace. Willingly or unwillingly, the systems of the Russian administration or businesses had to be updated. Also, the soldiers' awareness of OPSEC and PERSEC has increased significantly, although this may simultaneously reduce the number of war crimes committed.

At the same time, it is worth emphasising that collectives of hackers worldwide can be helpful. Entrusting them with essential tasks, in the Author's opinion, will not be wise, but in some situations, the mere fact of 'sowing chaos' can have positive effects.

## CONCLUSIONS

Russia's invasion of Ukraine showed what future armed conflicts might look like. This tragic war should be analysed in detail. Cyber attacks do not play a significant role during a conflict from the point of view of offensive action. However, they can create confusion, tying up resources and affecting soldiers' morale.

The great 'cyber-war' that was expected by analysing the destructive activities of Russian hackers evident over many recent years[51,52] did not take place. Analyses are emerging as to why this happened[53,54] and one possible answer touches on the fact that Russia expected a complete victory within a few days and thus did not want to destroy the areas it would later rebuild itself[55,56].

Gaining conclusions from this painful lesson is essential to identify those actions that will help other countries resist an attack or make it as difficult as possible. As Poland has de facto become a NATO frontline country, it should be vital for us to

[51] Baezner M., Robin P., Cyber and Information warfare in the Ukrainian conflict, Center for Security Studies (CSS), ETH Zürich 2018 https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

[52] Mohee A., Cyber war: The hidden side of the Russian-Ukrainian crisis https://doi.org/10.31235/osf.io/2agd3 https://www.researchgate.net/publication/358841316_Cyber_war_The_hidden_side_of_the_Russian-Ukrainian_crisis

[53] Gavrila A., Ukraine's great cyberwar that did not happen. Opinion Paper. IEEE 99/2022 https://www.ieee.es/Galerias/fichero/docs_opinion/2022/dieeeo99_2022_adagav_ucrania_eng.pdf

[54] Maschmeyer L., Cavelty M. D., *op. cit.*

[55] An interview with Andrew Boyd, director of the CIA's Centre for Cyber Intelligence Risky.biz https://risky.biz/andrewboyd/

[56] Dziwisz D., Sajduk B., Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej". Gruszczak A. (red.) THE WAR MUST GO ON. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski. Wydawnictwo Księgarnia Akademicka 2023 43:52 https://doi.org/10.12797/9788381388801.04

identify all effective ways of defending our borders. The ability to conduct effective operations in cyberspace is thus a pivotal competence to be developed[57].

## BIBLIOGRAPHY


1. An interview with Andrew Boyd, director of the CIA's Centre for Cyber Intelligence Risky.biz https://risky.biz/andrewboyd/
2. Ankel S., Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up. Business Insider 2022 https://www.businessinsider.in/tech/news/ukrainian-hackers-created-fake-profiles-of-attractive-women-to-trick-russian-soldiers-into-sharing-their-location-report-says-days-later-the-base-was-blown-up-/articleshow/94009908.cms
3. Anshori M. F., Db1000n Software as Ukraine's Military Utility to Counter Russian Invasion in 2022. Jurnal Pertahanan 8(2) 198:210 https://doi.org/10.33172/jp.v8i2.1683
4. https://www.researchgate.net/publication/363158743_Db1000n_Software_as_Ukraine's_Military_Utility_to_Counter_Russian_Invasion_in_2022
5. Ashley, How the food delivery app helped Russian women find torturers in the police station. News Rebeat 2022 https://newsrebeat.com/world-news/96916.html
6. Augustyniak Sz., Wystawiliśmy bitną cyber-armię. Wywiad z gen. Karolem Molendą, IT Wiz 2023 https://itwiz.pl/wystawilismy-bitna-cyber-armie-wywiad-z-gen-karolem-molenda/
7. Baezner M., Robin P., Cyber and Information warfare in the Ukrainian conflict, Center for Security Studies (CSS), ETH Zürich 2018 https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict
8. Battle of Snake Island Русский военный корабль, иди на хуй https://www.youtube.com/watch?v=6_B1m5iNndg
9. Corera G., Russia hacked Ukrainian satellite communications, officials believe, BBC 2022 https://www.bbc.com/news/technology-60796079
10. Coynash H., Belarusians name Russian soldiers caught on camera sending goods plundered in Ukraine to Russia, Kharkiv Human Rights Protection Group 2022 https://khpg.org/en/1608810358
11. Davis B., Speedo-wearing Russian tourist inadvertently reveals location of Putin’s artillery in Crimea, Evening Standard 2022


[57] Augustyniak Sz., Wystawiliśmy bitną cyber-armię. Wywiad z gen. Karolem Molendą, IT Wiz 2023 https://itwiz.pl/wystawilismy-bitna-cyber-armie-wywiad-z-gen-karolem-molenda/

https://www.standard.co.uk/news/uk/russian-tourist-ukraine-war-putin-target-geolocation-crimea-b1020094.html
12. Destructive malware targeting Ukrainian organisations, Microsoft 2021 https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. Drążkiewicz A., Lekcja dla nas, poznajemy techniki przeciwnika. Gen. Molenda o działaniach Rosji w cyberprzestrzeni. Polskie Radio 24. 2022 https://polskieradio24.pl/130/4437/artykul/3088678,lekcja-dla-nas-poznajemy-techniki-przeciwnika-gen-molenda-o-dzialaniach-rosji-w-cyberprzestrzeni
14. Druziuk Y., A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops — here's how it works Insider 2022 https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4?IR=T
15. Dunhill J., Pentagon Impressed By StarLink's "Eye-Wateringly" Swift Shut Down Of Russian Cyberattack IFLScience 2022 https://www.iflscience.com/pentagon-impressed-by-starinks-eyewateringly-swift-shut-down-of-russian-cyberattack-63401
16. Dziwisz D., Sajduk B., Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej". Gruszczak A. (red.) THE WAR MUST GO ON. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski. Wydawnictwo Księgarnia Akademicka 2023 43:52 https://doi.org/10.12797/9788381388801.04 https://ruj.uj.edu.pl/xmlui/handle/item/309135
17. Finowie wyśmiewają ruchy wojsk rosyjskich przy granicy. Wysyłają swój "specjalny sprzęt", Onet 2022 https://wiadomosci.onet.pl/swiat/finowie-wysmiewaja-ruchy-wojsk-rosyjskich-przy-granicy-pokazuja-traktory/zysdn71
18. Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape. Mandiant 2023 https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
19. Gavrila A., Ukraine's great cyberwar that did not happen. Opinion Paper. IEEE 99/2022 https://www.ieee.es/Galerias/fichero/docs_opinion/2022/dieeeo99_2022_adagav_ucrania_eng.pdf
20. Hackers play Ukrainian songs https://www.reddit.com/r/UkraineWarVideoReport/comments/wwl1u3/hackers_play_ukrainian_songs_and_watch_the/
21. Haertle A., Tysiące terminali internetu satelitarnego poważnie uszkodzonych w dniu ataku na Ukrainę Zaufana Trzecia Strona 2022 https://zaufanatrzeciastrona.pl/post/tysiace-terminali-internetu-satelitarnego-powaznie-uszkodzonych-w-dniu-ataku-na-ukraine/

22. Hart R., Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database. Forbes 2022 https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/
23. Italiano L., Orecchio-Egresitz H., Ukraine and Russia have both weaponised facial recognition — in very different ways. Insider 2022 https://www.businessinsider.com/ukraine-russia-have-both-weaponized-facial-recognition-2022-3?IR=T
24. Khatsenkova S., Ukraine war: Backlash after Elon Musk says he can no longer fund Starlink satellites, Euronews 2022 https://www.euronews.com/2022/10/14/backlash-after-elon-musk-says-he-can-no-longer-fund-starlink-in-ukraine
25. Konieczny P. Ktoś chciał nas wplątać w cyberkonflikt z Ukrainą https://niebezpiecznik.pl/post/ktos-chcial-nas-wplatac-w-cyberkonflikt-z-ukraina/
26. Kotowski A., GhostSec zhakował drukarki w Rosji. Zdalnie drukują informacje o wojnie na Ukrainie. Komputer Świat 2022 https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/ghostsec-zhakowal-drukarki-w-rosji-zdalnie-drukuja-informacje-o-wojnie-na-ukrainie/hrsft0c
27. Kowalska-Sendek M., Ukraina na cybernetycznym froncie, Polska Zbrojna 2022 https://polska-zbrojna.pl/home/articleshow/36629?t=Ukraina-na-cybernetycznym-froncie
28. Krzykowski P. Konsekwencje wojny na Ukrainie w wymiarze żywnościowym, ekonomicznym i energetycznym, Roczniki Nauk Społecznych T.15(50) nr 4, Akademia Sztuki Wojennej 2022 https://ojs.tnkul.pl/index.php/rns/article/view/17785/16759
29. Kuśmierek M., Rosjanie nakradli sprzętu rolniczego za 5 mln dolarów. Wywieźli go do Czeczenii i nie potrafią uruchomić Spider's Web 2922 https://spidersweb.pl/2022/05/rosjanie-nakradli-sprzetu-rolniczego-za-5-mln-dolarow-wywiezli-go-do-czeczenii-i-nie-potrafia-uruchomi.html
30. Macias A., UN report details horrifying Ukrainian accounts of rape, torture and executions by Russian troops CNBC 2022 https://www.cnbc.com/2022/10/28/russia-ukraine-war-un-report-details-accounts-of-rape-torture-and-executions.html
31. Maschmeyer L., Cavelty M. D., Goodbye Cyberwar: Ukraine as Reality Check, Policy Perspectives Vol. 10/3, May 2022 Policy Perspectives Vol. 10/3, May 2022 https://doi.org/10.3929/ethz-b-000549252 https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/2/PP10-3_2022-EN.pdf
32. Mazurkiewicz P., „Putin zabija" na rosyjskich paragonach. Anonymous włamali się do drukarek. Rzeczypospolita 2022

https://cyfrowa.rp.pl/bezpieczenstwo/art35915801-putin-zabija-na-rosyjskich-paragonach-anonymous-wlamali-sie-do-drukarek
33. Michalik K., Duch Kijowa - bohater czy miejska legenda?, RMF 2022 https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-duch-kijowa-bohater-czy-miejska-legenda,nId,5884226#crp_state=1
34. Mohee A., Cyberwar: The hidden side of the Russian-Ukrainian crisis https://doi.org/10.31235/osf.io/2agd3 https://www.researchgate.net/publication/358841316_Cyber_war_The_hidden_side_of_the_Russian-Ukrainian_crisis
35. Olszewski D., Elon Musk udostępnia Starlink na Ukrainie, Computerworld 2022 https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie,436628.html
36. Palczewski Sz. Białoruscy Cyberpartyzanci atakują systemy kolejowe. Utrudniają transport rosyjskich wojsk na Ukrainę, Cybersefence24 2022 https://cyberdefence24.pl/armia-i-sluzby/bialoruscy-cyberpartyzanci-pomagaja-ukrainie-utrudniaja-transport-sil-okupacyjnych-
37. Radzewicz Sz., Ukraińcy mają aplikację, przez którą zgłaszają pozycje wojsk rosyjskich. eWróg został użyty już 200 tys. razy Spider's Web 2022 https://spidersweb.pl/2022/03/ewrog-aplikacja-wskazuje-wojska-rosyjskie.html
38. Roth E., Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment. The Verge 2022 https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere
39. Russia fights back in information war with jail warning, Reuters 2022 https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/
40. Russian Soldiers Phone Calls https://www.nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html
41. Satter R., Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official, Reuters 2022 https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/
42. Smith A., Anonymous news – live: Russian TV hacked with Ukraine footage in 'biggest op ever seen'. Yahoo News 2022 https://news.yahoo.com/anonymous-news-live-russian-tv-090008311.html
43. Stodolak S., Zbiór pożytecznych idiotów jest coraz większy. Dlaczego uwierzyli Putinowi? Dziennik Gazeta Prawna 2022 https://www.gazetaprawna.pl/magazyn-na-weekend/artykuly/8413199,pozyteczni-idioci-putina-rosja-stone-kusturica-rourke.html

44. Stokel-Walker C., Russia and Ukraine are both weaponising mobile phones to track troops, New Scientist 2022 https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/
45. Štrucl D., Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare. Contemporary Military Challenges 2022(2):103-123 2022. https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.2.6 https://www.researchgate.net/publication/361569176_russian_aggression_on_ukraine_cyber_operations_and_the_influence_of_cyberspace_on_modern_warfare
46. Szpor G., Gryszczyńska A., Hacking in the (cyber)space. GIS Odyssey Journal 2022 | Vol. 2, no. 1 | 141:152 https://doi.org/10.57599/gisoj.2022.2.1.141 https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e50da523-a3b5-48f8-91e3-6369a2d8edf1
47. Ukraine 2022 na cyfrowym froncie. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzenie, 2023 https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf
48. Ukraine hits Russian Wagner mercenary HQ in east, BBC 2022 https://www.bbc.com/news/world-europe-62547403
49. Ukrainians use phone app to spot deadly Russian drone attacks The Guardian 2022 https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo
50. Vail E., ‘We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship, The Record 2022 https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship
51. Vasilyeva N., Beatings and psychological torture: The fate that awaits Russian dissidents like Marina Ovsyannikova, The Telegraph 2022 https://www.telegraph.co.uk/world-news/2022/03/15/beatings-psychological-torture-fate-awaits-russian-dissidents/
52. Vicens A., A year of cyberwar' with Russia: An inside look from a top Ukrainian cybersecurity official Cyberscoop 2023 https://cyberscoop.com/victor-zhora-ukraine-russia-cyber-war-one-year/