The 2022-2023 Russia-Ukraine War and Cyberspace Threats

Lika Lagvilava

Researcher, Caucasus International University (Tbilisi, Georgia)
E-mail: lika.lagvilava@ciu.edu.ge
https://orcid.org/0009-0000-0120-0408

Lagvilava, Lika (2023) The 2022-2023 Russia-Ukraine War and Cyberspace Threats. *Future Human Image*, Volume 19, 41-50. https://doi.org/10.29202/fhi/19/6

In the 21st century, following the process of globalization, the importance of the Internet is increasing, continuous remote communication is carried out, electronic purchases are made, payments are made in electronic form, and official and unofficial correspondence is exchanged between actors and institutions both within the country and abroad. Remote services are developing both in the private and public sectors. Therefore, Internet users, service recipients, legal entities, public agencies, and, in general, any citizen who communicates electronically in public space using remote services are under threats from cyberspace. However, it should also be noted that with the rise in popularity of the Internet, a new era of technological challenges are making the threats from cyberspace become apparent. Addressing these threats requires a comprehensive and multi-layered approach, including robust cybersecurity practices, regular updates and patching of software, user education and awareness, cooperation between governments and private sectors, and the development of international norms and agreements to prevent and respond to cyber threats. The technological progress of the world is so comprehensive that we face its consequences in all fields, including wars between states. No one is surprised anymore that today wars are taking place simultaneously in two dimensions – physical and digital worlds. Such is the daily life of two-sided military battalions of the twenty-first century, which became the focus of people's attention after the start of the Russia-Ukraine war. The presented article discusses cyber attacks carried out by Russia on the territory of Ukraine as a result of the Russian-Ukrainian war. The aim of the paper is to show how important the issue of cyber security is in modern wars and what policies states should implement to neutralize threats from cyberspace.

Keywords: cyber security, cyber threats, cyber war, technologies, Russia-Ukraine war.

Received: 9 June 2023 / Accepted: 2 July 2023 / Published: 5 August 2023

Introduction

Cyber security is a key part of national security and its protection is one of the main duties of each state so that the state can follow the security norms and not be harmed. Cyber security is an element of national security and e-governance, without which the state cannot function.

As research and practice in the field reveal, and Braman, Vaseashta and Susmann say, cyber security has become the most dangerous phenomenon. Many people, private companies and government institutions are affected every day. Billions of dollars are spent on defense" (Braman et al., 2014).

"The leading countries in the world have a national cyber security strategy, which is a determining factor of state policy. The national security strategy aims to identify, prevent, and minimize existing threats" (Shmit, 2015). In this context, cooperation with partner states and appropriate organizations is of the utmost importance for countries. It is essential to study the current situation, as well as to analyze plans, in-depth research, and to present them from a practical point of view.

Cyber security concerns all areas: economicization, democratization, international relations, water supply, national security, etc. In the case of an adequate scientific approach, the consequences of cyber threats will not be as devastating as they are in today's reality.

The use of computer systems and the Internet has a special place in the work of many countries and organizations, therefore, their work interruption or any kind of damage seriously affects any process that the abovementioned organization, company or state structure carries out. Cyber security is also of great importance in shaping modern warfare. Using the example of the current Russia-Ukraine war, we can confidently talk about the importance of threats from cyberspace.

Russian-led group Cyber Berkut

"They start a war when they want to, but end it when they can" (Niccolò Machiavelli). These very words correspond to the current Russia-Ukraine war, which has been in the world's attention since the moment it began, both due to the importance of the potential consequences of the conflict, as well as from a general information point of view.

If we look back a little earlier, we can see that the flagship of Russian-led cyber activities – the group Cyber Berkut – is engaged in cyber support of Russian military operations and strategic tasks. The group engages in propaganda attacks along with technical ones. Since 2014, Cyberberkut has been involved in cyberespionage or DDoS attacks against government sites of NATO, Ukraine, and Germany. From their side, the focus is on the online publication of the documents obtained through hacking, and the goal is to discredit the governments, demoralize the opposing party, reduce trust in the electoral bodies, and intimidate. For all this, Russia uses an army of paid commentators known as "trolls". This group is a state-sponsored organization that itself operates under the Kremlin's directives, distributes pro-government content, and engages in pro-Kremlin online discussions. Their main starting point, the task, is to fight against "Western influence" and the media that is negative towards Russia. "Trolls" are responsible for spreading false content (Timberg & Romm, 2020).

The content is a mixture of true and false information, in which reality, true information is very little, and false information is the main component. The goal itself is to confuse, demoralize and influence the target audience. The target audience is the own population,

certain groups of the population of other countries, the political elite of the country and the target countries (Timberg & Romm, 2020).

Propaganda is spread through a variety of means and includes both radio and television channels, social media, optimized search engines, bribed journalists in foreign media and many other means.

The digital dimension of the ongoing conflict in Ukraine

Cyberattacks were used as tools for espionage, disruption, and potentially even to gain a strategic advantage in the ongoing conflict. These attacks encompassed a range of tactics, including hacking, phishing, and distributed denial of service (DDoS) attacks. Some notable incidents included:

1. NotPetya: In 2017, a massive cyberattack known as NotPetya, which was widely attributed to Russian actors, affected various organizations around the world. While it initially seemed like a ransomware attack, it later became apparent that its primary purpose was to cause widespread disruption.
2. Ukrainian Power Grid Attacks: There were reports of multiple cyberattacks targeting Ukraine's power grid infrastructure. These incidents raised concerns about the potential for cyberattacks to have real world, physical consequences.
3. Espionage and Disinformation: Cyber operations were also used for espionage and spreading disinformation. Hackers targeted government institutions, military organizations, and media outlets to gather sensitive information and influence public opinion.
4. Cyber Espionage and Attribution Challenges: Attribution in the cyber realm is often complex, and while there were strong indications of Russian involvement in many of these attacks, definitively attributing them to a specific group or nation can be challenging.

To jump straight to the present, on the eve of the military attack on Ukraine on February 24, 2022, Russia launched a large-scale cyberattack targeting the government, military, and private companies. That included significant Distributed Denial of Service (DDoS) attacks, as well as the emergence of a new destructive malware called "Hermetic Wiper" by ESET cybersecurity researchers.

"Russia's appalling attacks on Ukraine are not limited to their barbaric land invasion, but also involve sickening attempts to attack their cyber infrastructure that provides vital services, from banking to energy supplies, to innocent Ukrainian people," Sunak, the British Prime Minister said (Dalvinder, 2023).

As this crisis continues to unfold, there are also cyber risks beyond the physical conflict zone for private companies and governments – entities operating in Russia or Ukraine could be directly targeted or harmed (Hermetic Wiper, 2022).

What is interesting about the digital dimension of the ongoing conflict in Ukraine is that the developments seem to confirm what cybersecurity researchers have been saying for years about the use of cyber tools to enhance state power. As cybersecurity expert Jason Blessing has said, there was no such thing as a Russian "cyber blitzkrieg", and it's unlikely there will be one, at least according to the prevailing thinking on cyber conflict (BLESSING, 2022). That is because cyber tools are simply not a good tool for escalation control or battlefield impact.

Yes, the war and Russia's response to global sanctions are likely to dictate a new phase of digital insecurity in international affairs as Moscow seeks to relieve pressure on its sanctioned economy and express displeasure with Western support for Ukraine. As scholars quickly demonstrated, the strategic utility of using cyber tactics in Ukraine to support the invasion itself simply did not exist. Cyber tools provide only temporary victories and are, therefore, not very good for direct coercion. An expected quick victory on the Russian side immediately took sophisticated cyber weapons off the table with the "do not break what you buy" logic.

Grouping – Anonymous and busted myth

It should be noted that there were cyber-attacks from Russia even before the war. As for the war period, the websites of the Ministry of Foreign Affairs of Ukraine, the Ministry of Defense and the banking and financial sector were broken. Since then, the cyber-attack on the government sector has continued. However, it turned out here that in addition to shattering the myth of military strength, another myth of Russia was shattered in this war, which it was the strongest state in cyberspace as well. After the appearance of Anonymous, this myth no longer exists.

In the first days of the Russia-Ukraine war, Anonymous got involved and carried out counter-cyber-attacks against Russia, both on the government, military, banking sector, other large companies, gas and oil extraction sector. These attacks caused serious damage to Russia (Burt, 2022).

The members of the Anonymous group claim to be a free, decentralized organization that unites hacktivists from different countries under one idea. This group became known after attacking government, religious and large corporate websites. In the attack, Anonymous mainly used a distributed denial-of-service or DDoS attack.

Anonymous was created in 2003, as the creators of the group say, Anonymous is not a hacker group. They do not consider themselves to be cybercriminals, and they believe that every person who shares the ideas of Anonymous can call himself Anonymous. The mask became their symbol according to the scenario of the Wachowski brothers in the British thriller "V for Vendetta" released in 2006 (Tidy, 2022).

Anonymous is a loosely organized Internet group of hackers and political activists, which collectively began its activities in 2003. Anonymous community members communicate and collaborate through social networking services and encrypted Internet chat rooms.

Anonymous has a coherent structure, representing decentralized communities interested in engaging in mutual goals. These targets have historically ranged from political statements to pranks and hacks, sometimes with retaliatory actions taken against the group – or those to whom members of a given operation feel kinship.

In 2013, information spread on the Internet, according to which Anonymous Masons offered cooperation, to which only a humiliating response was received from them. This information was soon followed by a response from Anonymous, who claimed that agreeing to this proposal was in direct conflict with the ideas of Anonymous, which underpins the entire group. Based on these ideas, Anonymous got involved in the Russia-Ukraine war of 2022 (Tidy, 2022).

A hacking group has declared a cyber war on Russia and claimed responsibility for hacking the Russian Defense Ministry database and allegedly hacking multiple state TV channels to air pro-Ukraine content.

Hacktivist groups have claimed responsibility for shutting down government, corporate and news websites. Anonymous claimed to have successfully infiltrated Russian state

television to show citizens footage of Putin's invasion of Ukraine. The group also hacked and released e-mails and files from Roskomnadzor, the government agency responsible for censoring Russian media.

The hacker group has gained over 500,000 followers on its Twitter account through these moves.

92 out of 100 Russian databases analyzed were hacked and the file names were changed to "Glory to Ukraine", "Putin, stop this war", "Stop the war", "No war", "HackedByUkraine" and other pro-Ukraine messages (Tidy, 2022).

Most of the files discussed in the databases have been deleted. Hacktivists used a script similar to "MeowBot" that deletes the contents of files and changes their names. One such database was the Commonwealth of Independent States (CIS), which consists of 11 republics and is used to coordinate finance, trade, lawmaking, and security information among member states. Hundreds of files in the database were renamed "Putin! Stop_this_war". E-mails were also distributed (Tidy, 2022).

While Anonymous waging cyberwarfare may seem like a noble cause, future hackers may engage in criminal activity without government authority (Hermetic Wiper, 2022). However, the noteworthy fact is that Anonymous has gained many followers and received thousands of supportive messages and likes on their social media.

As for the myth, in this war, another myth of Russia was shattered, that it was the strongest state in cyberspace as well. Let us start with how this myth was created. Russia carried out its first cyber-attack on Estonia in 2007, when Estonia protested the topic of May 9 and started talking about taking the monument of Soviet troops. This position of Estonia was protested by the Russian-speaking population of the same country. It was then that Russia launched a large-scale cyber-attack on Estonia.

The second large-scale cyber-attack was carried out on Georgia in 2008, which was already a cyber war and not only a large-scale attack. Another proof that Russia was planning to attack Georgia is that the cyber-attacks started in January 2008. Before the war, he had permanent cyber-attacks and was looking for Georgia's weak spots. At that time, cyber security did not exist in Georgia at all. It must be said that during the August 2008 war, parallel to the military attacks, cyber-attacks were also carried out. 80 percent of websites across the country were damaged. After the August war, strategic partners, America and Estonia, have helped Georgia a lot in terms of strengthening cyber security. The restoration of the cyberinfrastructure started with their help.

In 2008, another large-scale cyber-attack was carried out on Lithuania. Then – in Latvia and at the Prague office of "Radio Liberty". However, we cannot really compare the scale of the attack to the one carried out on Georgia.

Since Russia launched a full-scale war in Ukraine, part of the military campaign has moved into cyberspace.

At the start of the war, experts believed that "hacktivists" could play an important role in this conflict, but the actual scale of hacker activity is staggering: hacker groups play an important role on both sides of the cyber war.

Officially, Ukraine protects itself from cyberattacks with the help of Western military cybercrime specialists and private cyber security companies, for which multi-million funds have been allocated. However, unofficial cooperation between vengeful hackers and military officials is also increasingly visible.

Since the beginning of the military invasion, Russia has mainly carried out targeted cyber-attacks on Ukrainian military infrastructure. However, the Killnet group has also carried out attacks on Ukrainian medical facilities and the country's allies.

Russian propaganda in cyber attacks

Russian propaganda is undoubtedly one of the main pillars of the Putin regime, as it prepares public opinion in the Russian Federation as well as abroad and shapes it in accordance with Russia's aggressive goals. From today's perspective, many people probably no longer doubt that the propagandists of Putin's regime, due to the spreading and strengthening of the relevant narratives, are fully complicit in the unprecedented crime and aggression that Putin's regime is committing in Ukraine (Burt, 2022). Russian propaganda and disinformation campaigns have been a prominent aspect of cyberattacks and information warfare on the global stage. The Russian government and associated entities have been accused of using cyberspace as a tool to manipulate narratives, spread false information, and achieve strategic goals. Some key points to understand about Russian propaganda in cyber-attacks include:

- *Disinformation Campaigns*: Russian actors, often linked to state-sponsored groups, have been implicated in orchestrating disinformation campaigns through social media platforms and websites. These campaigns aim to shape public opinion, create confusion, and undermine trust in democratic institutions and processes in other countries.
- *Election Interference*: Russia has been accused of meddling in foreign elections by disseminating fake news, fabricated stories, and divisive content to sow discord and influence voter sentiment in target countries.
- *Troll Farms and Bot Networks:* Russian operatives are believed to operate "troll farms" and automated bot networks that amplify and spread propaganda on social media platforms, making it appear as if there is genuine grassroots support for certain narratives.
- *Cyber Espionage:* Russian state-sponsored groups have been implicated in cyber espionage campaigns targeting various sectors, including government agencies, defense contractors, critical infrastructure, and political organizations, with the aim of gathering intelligence and potentially advancing political objectives.
- *Hybrid Warfare:* Russia is known for its use of hybrid warfare, which combines conventional military tactics, cyber operations, and disinformation to achieve strategic goals. Cyberattacks are often used in conjunction with other forms of influence and aggression.
- *Attribution Challenges:* While there is often strong evidence pointing to Russian involvement in cyber-attacks and disinformation campaigns, attribution can be complex and challenging due to the use of proxies, false flags, and advanced techniques to hide the origin of attacks.
- *International Impact:* Russian propaganda and cyber operations have had significant international implications, leading to strained diplomatic relations, increased distrust, and heightened tensions between Russia and other nations.
- *Countermeasures:* Countries and organizations have responded to Russian propaganda and cyber threats by investing in cybersecurity, strengthening defenses, promoting media literacy, and imposing sanctions on individuals and entities involved in disinformation campaigns.

Let us delve deeper into the tactics and examples of Russian propaganda in cyber-attacks:

- *Weaponizing Leaked Information:* Russian actors have been known to hack and leak sensitive information, often with the intention of influencing public opinion or embarrassing political opponents. Notable instances include the hacking of the Democratic National Committee (DNC) during the 2016 US presidential election, which resulted in the release of confidential e-mails that were widely covered by media and had a significant impact on the political discourse.
- *Fanning Cultural and Ethnic Divides:* Russian disinformation campaigns frequently exploit existing cultural, ethnic, and social divisions within target countries to amplify tensions and create internal conflicts. This approach aims to weaken societies from within and distract from external challenges.
- *Promoting Alternative Narratives:* Russian propaganda often promotes alternative narratives that challenge the mainstream consensus on geopolitical events or conflicts. By disseminating contradictory information, they aim to confuse audiences and undermine the credibility of official sources.
- *Manipulating Historical Narratives:* Russia has been accused of revising historical events to suit its political agenda. These efforts can include downplaying or denying historical atrocities, such as the Holocaust, to shape public perceptions and advance diplomatic goals.
- *Exploiting Social Movements:* Russian actors have been known to exploit social and political movements, such as protests and demonstrations, to amplify their reach and manipulate public sentiment. By disseminating misleading or inflammatory content, they seek to exacerbate social tensions and destabilize societies.
- *Fake News Outlets:* Russian-sponsored media outlets and websites have been established to spread propaganda and false information under the guise of legitimate journalism. These outlets often present biased or fabricated stories that align with Russia's strategic interests.
- *Phishing and Hacking for Propaganda:* Russian hackers have used phishing attacks to compromise e-mail accounts and spread propaganda. By gaining access to influential individuals' accounts, they can disseminate false information to a wider audience and lend credibility to their narratives.
- *Targeting of International Organizations:* Russian disinformation efforts have also extended to international organizations, such as the United Nations, with the aim of shaping decisions and policies in ways that align with Russian interests.
- *Crisis Exploitation:* Russia has been known to take advantage of crisis situations, such as natural disasters or global health emergencies, to disseminate misleading information and exploit public fear and uncertainty.
- *Weaponizing Stolen Documents:* Russian actors steal sensitive documents and strategically release them to achieve specific goals, such as undermining international agreements or discrediting opponents. For example, the release of e-mails from the World Anti-Doping Agency (WADA) in 2016 aimed to discredit anti-doping efforts and portray Russia as a victim.
- *Cultural and Linguistic Manipulation*: Russian propaganda tailors its messaging to specific cultural and linguistic contexts to make it more persuasive and relatable. For example, Russian disinformation campaigns may create content that resonates

with local sentiments during times of political upheaval, such as the annexation of Crimea.

- *Exploiting Crisis Situations*: Russian actors take advantage of global crises, such as the COVID-19 pandemic, to spread disinformation and sow confusion. For example, disseminating misleading information about the origin and spread of the coronavirus to advance geopolitical interests.
- *Geopolitical Manipulation*: Russian propaganda exploits international conflicts and crises to promote narratives that align with Russian foreign policy goals. For example, during the Syrian conflict, Russian media presented Russia's military involvement as a counterterrorism effort while downplaying civilian casualties.
- *Promotion of Extremist Content*: Russian actors disseminate content that supports extremist groups or ideologies, contributing to social unrest and destabilization. For example, Amplification of far-right and far-left content in the United States to deepen societal divisions.
- *Targeting Dissidents and Critics:* Russian propaganda cyber-attacks may target critics of the government, human rights activists, and journalists to silence dissenting voices. For example, hacking and leaking sensitive information about opposition figures to discredit them.
- *Economic Warfare:* Russian propaganda may spread rumors or false information about economic instability in target countries to undermine confidence and disrupt financial markets. For example, Spreading rumors about financial crises in Europe to create uncertainty and weaken economies.
- *Conspiracy Theories and Pseudoscience:* Russian propaganda campaigns may exploit conspiracy theories and pseudoscientific claims to create confusion and manipulate public perceptions. For example, Promoting conspiracy theories related to the downing of Malaysia Airlines Flight MH17 over Ukraine to deflect blame.
- *Online Comment Manipulation*: Russian actors use fake accounts to flood comment sections of news articles, blogs, and forums with propaganda and disinformation to shape online discussions. For example, manipulating online discussions on social media platforms during geopolitical events like the Ukraine crisis.

These examples illustrate the diverse tactics employed by Russian propaganda in cyber-attacks. It is crucial to remain vigilant, critically evaluate information sources, and work collectively to counter disinformation and protect the integrity of digital spaces. As the landscape of cyber threats continues to evolve, efforts to mitigate the impact of propaganda cyber-attacks must also adapt and grow.

It is important to note that while Russia has been a prominent actor in using propaganda in cyber-attacks, other nations and actors also engage in similar activities. Addressing this issue requires a coordinated global effort involving governments, tech companies, civil society, and the media to counter disinformation, promote digital literacy, and defend against cyber threats.

Addressing the multifaceted challenges posed by Russian propaganda in cyber-attacks requires a comprehensive approach that involves strengthening cybersecurity, enhancing digital literacy, promoting media integrity, fostering international cooperation, and holding those responsible for disinformation and cyber operations accountable. As the tactics and strategies employed by state-sponsored actors continue to evolve, it remains crucial for governments, technology companies, and civil society to remain vigilant and work together to safeguard the integrity of information and the security of cyberspace.

Conclusion

The Russia-Ukraine war has a significant cyber dimension, with both sides engaging in cyber attacks and cyber espionage. The conflict began in 2014 when Russia annexed Crimea, and since then, there have been numerous incidents of cyber activity. This issue was further exacerbated by the Russia-Ukraine war that began in November 2022, during which Russia intensified its cyber-attacks and actively used cyberspace in the process of waging war.

Russian state-sponsored hacking groups such as Cozy Bear and Fancy Bear have been accused of targeting Ukrainian government agencies and critical infrastructure such as power grids. These groups are also believed to have carried out attacks on Ukrainian media outlets and political parties.

In response, Ukraine has developed its own cyber security capabilities and has been active in countering Russian cyber attacks. Ukrainian security services have identified and disrupted numerous Russian hacking operations, including the NotPetya malware attack, which caused significant damage to Ukrainian businesses and government agencies in 2017.

The conflict has also used disinformation and propaganda on social media platforms, with both sides trying to shape public opinion and undermine the legitimacy of the other's actions.

Overall, the cyber dimension of the Russia-Ukraine war highlights the importance of cyber security in modern conflicts and the potential of cyber attacks to cause significant damage to critical infrastructure and national security.

🕮 References

Alperovitch, D. (2022) *How Russia Has Turned Ukraine Into a Cyber-Battlefield*. Available online: https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield

Blessing, J. (2022) *Where is Russia's cyber blitzkrieg?* Available online: https://thehill.com/opinion/cybersecurity/597272-where-is-russias-cyber-blitzkrieg/?rl=1

Braman, E., Vaseashta, A., and Susmann, P. (2014) *Cyber Security and Resiliency Policy Framework.* Available online: https://www.researchgate.net/publication/266077764_Cyber_Security_and_Resiliency_Policy_Framework

Burt, T. (2022) *The hybrid war in Ukraine*. Available online: https://blogs.microsoft.com/on the-issues/2022/04/27/hybrid-war-Ukraine-Russia-cyberattacks/

Chapple, M. (2013) *Cyberwarfare Information Operations in a Connected World*.

Collier, K. (2022) *Ukraine foiled Russian cyberattack that tried to shut down energy grid*. Available online: https://www.nbcnews.com/tech/security/ukraine-says-russian-cyberattack-sought-shut-energy-grid-rcna24026

Coe, T. (2015) *Where does the word cyber come from*? Available online: https://blog.oup.com

Dalvinder, K. (2023) *UK government to invest £25m in Ukraine's cyber defences.* Available online: https://nationaltechnology.co.uk/UK_Government_To_Invest_25m_In_Ukraines_Cyber_Defences.php

Hermetic Wiper (2022) *New data-wiping malware hits Ukraine*. Available online: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

Martin, C. (2022) *Cyber Realism in a Time of War*. Available online: https://www.lawfareblog.com/cyber-realism-time-war

Shmit, M. (2015) *Cyber War: The Next Frontier for NATO Paperback.* Available online: https://www.amazon.com/Cyber-War-Next-Frontier-NATO/dp/1522943846

Tidy, J. (2022) *Anonymous: How hackers are trying to undermine Putin*. Available online: https://www.bbc.com/news/technology-60784526

Timberg, C., and Romm, T. (2022) *Hackers are seizing on coronavirus fears to steal data, researchers and US regulators warn*. Available online: https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/