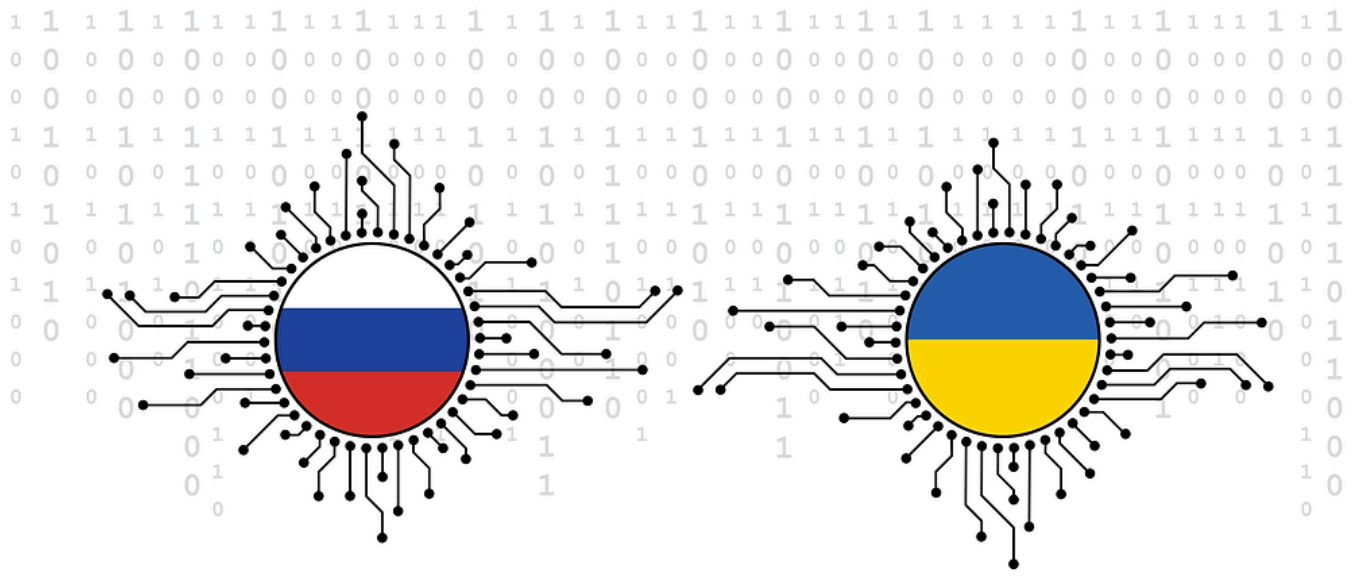
The Cyberwar Between Russia and Ukraine: Impacts and Implications

diplomania.wixsite.com/website/post/the-cyberwar-between-russia-and-ukraine-impacts-and-implications

Diplomania August 17, 2024



By: Sakkcham Singh Parmaar

The author is a second-year B.A.LL.B (HONS.) student at the Jindal Global Law School, O.P. Jindal Global University. He can be reached at 23jgls-sakkcham@jgu.edu.in.

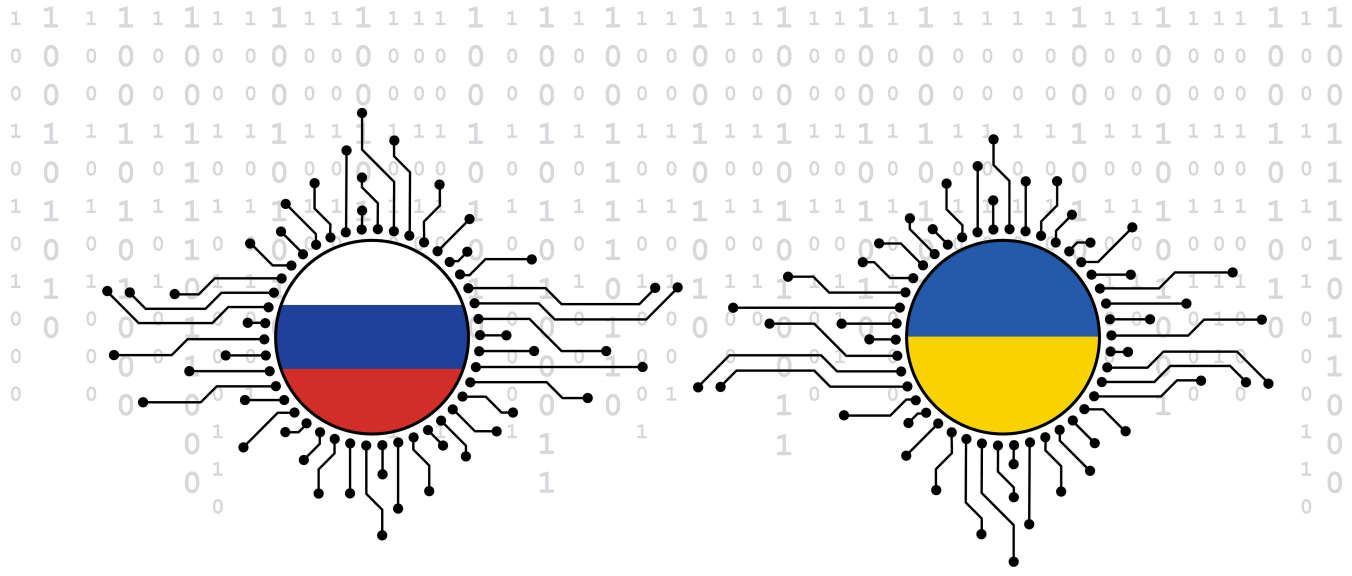


Image Source: Shutterstock

Abstract

Today's cyberwar between Russia and Ukraine implies a change in modern warfare since the need for digital fields has become as crucial as those of the physical world. In this study, we explore the intricacies of this cyber war by assessing its historical background, key cyber strikes and their far-reaching effects on infrastructure, economy, poverty etc. in Ukraine. The attackers' modus operandi, tools they used, reasons for their actions, etc, are depicted via such events as the 2017 NotPetya malware outbreak and the 2015 Ukrainian power grid attack within the Russian cyber operations framework. Moreover, Ukraine's defence mechanisms, owing to support from international bodies like the EU and NATO, especially during the 2014 crisis, are looked into, and their success rate is evaluated.

Introduction to Cyber Operations in the Russia-Ukraine Conflict

Digital fields are imaginary landscapes invented through interconnected computer systems that serve as places of information exchange and manipulation. In modern battlefields, these digital zones have turned into important fronts just like physical areas of combat. The need for securing digital properties and abilities to ensure national security is thus emphasized by using cyberspace for military as well as governmental activities (Sheldon, 2010). The war between Russia and Ukraine, especially after the large-scale invasion in February 2022, indicates a huge change in today's way of waging wars, revealing how important it is for cyber operations to be supported by traditional military strategies. This new era of warfare demonstrates the role that cyber-attacks have played in international conflicts and their impact on both state and non-state actors. It has moved from previous cyber encounters like the 2015 power grid attacks or the NotPetya malware assault in 2017, which laid the groundwork for the level and size of cyber activities taking place present day.

Such events have shown that cyber-attacks can interfere with vital systems and have far-reaching consequences beyond the immediate targets. The attack on Ukraine's electrical grid in 2015 highlighted the exposure of basic utilities to online threats while the NotPetya outbreak displayed global implications and financial repercussions from such strikes. This ongoing war has made these trends worse, as a result of which currently cyberspace operations are becoming increasingly significant in strategy making. In the ongoing Russia-Ukraine war, DDoS Attacks on Ukrainian Government Websites (2022) and Ongoing Cyber Espionage and Disruption (2021-2022) are the best examples that show the significance of cyberspace operations.

It is a common idea that infrastructure and the economy have experienced considerable effects from cyber-attacks. There have been serious interruptions in how power grids work and in the communication networks due to cyber-attacks that hit those important systems. These damages can be summarized as, expenses incurred due to direct loss of lives from these attacks, more money spent to upgrade on cyber safety and significant uncertainty towards investment as well as business continuity (McLaughlin, 2023). For example, during the cyber assault on Ukrainian power grids, failures in critical infrastructure might have affected essential services such as hospitals, which could indirectly lead to loss of lives during critical situations (McLaughlin, 2023).

Therefore, Ukraine has improved its cyber-defence systems with massive worldwide backing from the EU, NATO and other organizations. In particular, this includes enhancing their security systems, upgrading their threat detection mechanisms as well as promoting cross-country partnerships through providing training on computer forensics. However, even with these changes, the global response raises complex issues, such as determining who is responsible for cyber-attacks, how existing international law applies to cyber warfare, and how we should address the ethical concerns related to the impact on civilian resources.

Historical Context of Cyber Warfare in Ukraine

The conflict between Ukraine and Russia has decidedly been influenced by cyber warfare, especially after Russia annexed Crimea in the year 2014. These cyber-attacks are directed at different parts of Ukraine's infrastructure such as government agencies, military networks and vital services like energy and communication. They are one of the strategies loosely associated with Russia's intention to make Ukraine unsteady and gain control over that area.

Early Incidents (2014-2015): During the rising tensions in Ukraine and Russia around 2014, there were several cyber-attacks directed against Ukraine. One of the first and most prominent was the "Snake" virus, which penetrated government networks in that country and allowed hackers to obtain confidential data. The sequence was followed by a string of attacks on Ukraine's media meant for propagandistic purposes and interrupting telecommunication systems (Phys.org, 2014).

Black Energy and Power Grid Attack (2015): In December 2015, one of the most well-known attacks took place when a hacking incident thought to be led by Russian hackers was directed towards the power system of Ukraine. The invasion was called Black Energy wherein electricity

blackouts affected almost 250,000 people. This is an example of one of the first situations where an intrusion physically hits an important subsystem using cyber (International cyber law: interactive toolkit, 2023).

Ongoing Cyber Conflict (2018-Present): Whether state-sponsored or non-state actors, Ukraine continues to face diverse cyber threats. Just in 2017, there were numerous phishing emails sent to military and government officials; escalated election disruptions; and constant efforts aimed at penetrating the important sectors of the economy. Despite Western nations' support in its pursuit of better cybersecurity, the country has not been able to completely shrug off this threat which is a continuous struggle (Willett, 2022).

Major Cyber Attacks Against Ukraine

Several cyber-attacks have characterized this conflict, especially the one that targeted Viasat's KA-SAT satellite a few hours before the invasion took place in February 2022. This led to widespread internet blackouts in Ukraine and other European countries, interrupting military communication seriously (Matamis, 2024). Besides these prominent attacks, Russia has used various methods including data wipers meant to erase vital information, phishing campaigns for information gathering and propaganda deceiving people's opinion. The effects of cyber operations on Ukraine's state have been deep and multifaceted. They have caused considerable disruption in government services, vital infrastructure and public morale. For example, large segments of destructive Russian cyber operations focusing on Ukraine's critical infrastructure that impacted energy, health care and emergency services occurred between February and October 2024 (*The Evolution of Cyber Operations in Armed Conflict - Digital Front Lines*, 2023).

Since the current war, Ukraine has been subjected to many distributed denial-of-service (DDoS) attacks. Inundated by unnecessary traffic, these assaults make it impossible for the affected servers to perform their normal duties. Before the invasion, in January 2022, there were DDoS attacks on Ukrainian governmental bodies that caused breakdowns in their provision of services and circulated rumours regarding essential banking services' operations. This exemplifies that such cyber movements are meant not only to disturb but also to cause alarm among members of society (Pandit, 2022).

The hack caused internet disruptions throughout Ukraine and affected some European nations leading to failure in thousands of terminals. This case revealed how computer attacks on fragile crucial systems could impact widely more than they seem at first sight (Office for Budget Responsibility, 2022). Due to the escalation of cyber menace, Ukraine's government has green-

lighted a new plan for cyber security. The objective is to strengthen the nation's capacity to safeguard its information technology from intruders. In this context, it highlights creating an effective and powerful cyber security mechanism to deter those who attack nations through the internet; enhance their abilities against these attacks; and improve collaboration among different networks that operate in terms of keeping such kind of defence in every country (*National Security and Defense Council of Ukraine*, n.d.). Ukraine has realised the importance of investing in fortifying electronic security for the industries that are usually hackers' targets, especially energy and telecommunication. Thus, such measures may include building systems to lessen the effect of cyber dangers on them (WordPress, n.d.).

Ukraine's Defense Efforts Against Cyber Threats

Due to the overwhelming cyber operations, Ukraine has greatly changed its techniques to defend itself from cyber threats. To tackle these issues, Ukraine has partnered with international technology enterprises and governments that offer essential supplies and assistance in improving their cyber security efforts (*Cyber Conflict in the Russia-Ukraine War*, n.d.). The establishment of CERT-UA (the Computer Emergency Response Team) is part of this particular strategy which enables prompt recognition and neutralizing of cyber threats (*Cyber Conflict in the Russia-Ukraine War*, n.d.). In addition, Ukraine's launching of a worldwide IT Army has attracted international notice and endorsement; however, it poses ethical challenges regarding how combatants should behave during wars (Matamis, 2024).

Global Reactions to Cyber Warfare

The global terrain has reacted to the cyber war between Russia and Ukraine by recognizing that all nations must work together to create collective cybersecurity strategies. Across the globe, government institutions and corporations alike have transformed their approach towards cybersecurity by sharing intelligence information and effective tactics to mitigate such threats. In particular, NATO and the EU have asserted the need for these bodies to cooperate within this arena to avert unison efforts against wicked cyber actions (Matamis, 2024). Moreover, there are deliberations on guidelines and principles that regulate how states act in cyberspace; thus, linking military action with international law (Matamis, 2024).

The European Union, through various measures aimed at improving cybersecurity among its member states and allies, has actively condemned malicious cyber campaigns in Russia. One of these actions was an agreement between the EU Agency for Cybersecurity (ENISA) and

Ukraine to bolster Ukrainian capability in defending against cyber threats and sharing best practices within the region. In light of the war, this treaty reflects the EU's commitment towards building a cooperative cybersecurity approach (*BIPR*, n.d.).

To prevent escalation, NATO has highlighted the importance of cybersecurity as one of its core responsibilities. Given extensive cyber incidents, a paper was produced to explore the use of Article 5 for collective defence (Liu, 2022). The establishment of a cybersecurity reserve is among the recent endeavours that show NATO's commitment to coordinating defensive measures among its member states and ensuring rapid response against cyber threats (*NATO's Chief Information Officer on What Ukraine Did Right in Its Cyberwar With Russia*, n.d.).

Conclusion

The lessons learned from the cyber war between Russia and Ukraine underscore the necessity of enhancing cyber resilience in contemporary warfare. Because cyber-attacks have demonstrated their capability to cause massive disruptions, countries need to develop strong responses that go beyond traditional cybersecurity measures. It implies that this resilience entails an ongoing process of improving the detection of threats, quick recovery mechanisms, and holistic strategies targeted towards plugging possible loopholes in crucial infrastructures (U.S. Department of Defense, n.d.). Thus, as conflicts such as the one observed in Ukraine change, so ought approaches to cyber resilience whereby nations build capacities to mitigate against and recover from any cyber threats quickly and easily (Vakulov, 2023).

The conflict between Russia and Ukraine is a clear demonstration of how significant cyber operations can transform modern-day warfare. The digitally-based assaults targeted at these two countries represent a new dimension in warfare that complements conventional arms. Such attacks have serious effects on their economies, infrastructure and society as a whole. It is, hence, essential to be mindful of our critical systems' weaknesses against cyber threats while building strong defence standards.

Cyberwar defence strategies should also adjust with time as warfare technology changes. We must take proactive steps towards safeguarding ourselves against possible cyber threats by building a security framework that will be able to respond when our nation is under attack in a digitally inclined world.

Bibliography

BIPR. (n.d.). BIPR. https://bipr.jhu.edu/BlogArticles/36-Support-for-Ukraines-Cybersecurity-Will-Increase-.cfm

Cyber conflict in the Russia-Ukraine war. (n.d.). Carnegie Endowment for International Peace. https://carnegieendowment.org/programs/technology-and-international-affairs/cyber-conflict-in-the-russia-ukraine-war?lang=en

Office for Budget Responsibility. (2022, July 7). *Cyber-attacks during the Russian invasion of Ukraine - Office for Budget Responsibility*. https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/

Liu, S. (2022, August 7). *Cyberattacks and the Russian war in Ukraine: the role of NATO and risks of escalation - Georgetown Journal of International Affairs*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/

U.S. Department of Defense. (n.d.). *Defense official calls cyber resilience critical to protecting systems*. https://www.defense.gov/News/News-Stories/Article/Article/2422375/defense-official-calls-cyber-resilience-critical-to-protecting-systems-continui/

Galbreath, J. (2022). EDITORIAL CYBER SECURITY AND DEFENCE CHALLENGES. *CONTEMPORARY MILITARY CHALLENGES*, *24*(2), 11–13. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.00

Maloney, S. (n.d.). *A quick recap on NotPetya – an unofficial guide*. https://www.cybereason.com/blog/blog-a-quick-recap-on-notpetya.

Matamis, J. (2024). False alarms: Reflecting on the role of cyber operations in the Russia-Ukraine war. *Stimson Center*.

McLaughlin, J. (2023, March 3). Russia bombards Ukraine with cyberattacks, but the impact appears limited. *NPR*. https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited#:~:text=For%20Ukrainians%2C%20including%20those%20working%20in%20cybersecurity%2C%20the%20war%20didn%27t%20start%20in%20February%202022.%20It%20began%20in%202014%20when%20Russia%20invaded%20Crimea.%20Russia%20used%20cyberattacks%20to%20successfully%20take%20down%20Ukraine%27s%20power%20grid%20in%202015%20and%202016%2C%20then,of%20dollars.

NATO's chief information officer on what Ukraine did right in its cyberwar with Russia. (n.d.). https://therecord.media/nato-cio-ukraine-war-cyberdefense-russia

National Security and Defense Council of Ukraine. (n.d.). National Security and Defense Council of Ukraine. https://www.rnbo.gov.ua/en/Diialnist/4976.html

Vakulov, A. (2023, April 10). The cybersecurity consequences of the Russia-Ukraine war. *Security Info Watch*. https://www.securityinfowatch.com/cybersecurity/article/53056808/the-cybersecurity-consequences-of-the-russia-ukraine-war

The evolution of cyber operations in armed conflict - digital front lines. (2023, May 25).

The views expressed in this article are those of the author (s). They do not reflect the views or opinions of Diplomania or its members.