Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1064-1079
ISSN – E 2958-8731 P 2958-8723

Russia - Ukraine Cyber Warfare and Its Impacts on Poland's National Security

Fiza Zeeshan[1]

Abstract

This research analyses the Russia-Ukraine conflict in the cyber domain and its boarder impact on Poland national security. It explains that how the nature of cyber warfare represents the impacts on Russian cyberattacks on Ukraine's infrastructure have the influence on Poland national security. The study highlights that Poland facing cybersecurity threats due to its geostrategic location and key ally of NATO and EU, which makes Poland target of the Russian cyber threats. Key challenges faced by the Poland involves misinformation campaigns, and attacks on their infrastructure. By examining the documents and reports, this research demonstrates that how Poland counters the Russian cyber threats by investing and enhancing their cyber defense co-operations with different institutes and in improving the cybersecurity. These recommendations aimed to suggest Poland better respond to the cyber threats through enhancing Poland's role in European cyber security and improving their cyber resilience. The Russia-Ukraine cyber warfare involves numbers of cyberattacks, 2017 NotPetya wiper worm, the 2022, and in between 2015-16 attacks on energy grids. Primarily, thee operations targeted the Ukrainian infrastructure but particularly on Poland's national security. In context of rising global cyber warfare in order to counter the state- sponsored cyber threats they need for adaptive cyber defense policy, collective security agreements and stronger international regulations. The Russia-Ukraine cyber warfare highlights to stay safe from the cyber conflicts international co-operation is necessary, critical infrastructure is a key to protect digital sovereignty and need for strong national cyber plans.

Keywords: NotPetya Cyberattacks, Ukraine power grid Attack, EU-NATO Cyber Cooperation, Polish Ministry of Defense, Digital Infrastructure Protection, ENISA Threat Landscape, Hybrid warfare, Poland Strategic Posture

[1] Department of International Relations, University of Management and Technology, Lahore – Pakistan

Introduction

The cyber conflict between Russia and Ukraine has become a major part of warfare in 21st century and it combines and includes all the cyber factors which state can use for manipulation, disruption and contesting sovereign body. Many countries are engaging themselves in a cyber operation for preparing themselves or carrying out warfare. According to (Rid, 2020), "Cyber has become multi-faceted warfare and now has vast and grave consequences to the security of the nation". The conflict between Russia and Ukraine had already seen impacts on the other regions especially in Europe countries like Poland, German, and the Baltic states. This conflict includes both aspects of traditional military and cyber warfare, which not only destabilize Ukraine but also its neighbouring countries like Poland. The study aims to show the conflict between Russia and Ukraine and how it affects the Poland's government institutions, boarder security and regional stability. The Russia-Ukraine conflict is the first conflict where cyberattacks played such a major rule. According to Kaplan, "In this conflict I have identified four different types of cyber operations disruption, destruction, intelligence and influence.

The tensions between the Russia and Ukraine starts in 1991 when Ukraine declared independence from Soviet Union. At first Russia accepted Ukraine independence but tension starts when Ukraine wanted to join NATO. In 2014 things worsened when Russia sent its military towards Ukraine and capture its territory Crimea. This was the major conflict which move towards the cyberattacks and more military actions between these two countries. Cyberwarfare has been a part of Russia Ukraine conflict since Revolution of Dignity in 2013 and 2014. Russia cyberattacks on Ukrainian businesses and the government systems. Although develops cyber tools like Uroburos malware since 2005 which was used for spying and attacking the systems. According to data from the Centre for Strategic and International Studies (CSIS), Ukraine experienced 27 major attacks between 2014 and 2022.

First operation by Russia in 2013 ARMAGEDDON where hackers tries to steal the data od Ukrainian government and military offices during protest. Second operation was in 2014 SNAKE when Russian hackers secretly access Ukrainian government computers by sending a computer virus. On June 2014 Russian hackers tries their best to mess with computer counts the votes during elections to cause confusion or change the results. On December 2014 hackers used virus called black energy which causes power outrage in parts On June 2017 Petya virus attack on Ukraine's computer system which affects the businesses worldwide. On January 2022 day after

US-RUSSIA negotiations about Ukraine's possible NATO membership failed, Russian hackers attacked Ukraine government websites making them go offline. Russian troops entered eastern Ukraine in February 2022 several Ukraine's government and banking websites were attacked and they shut down. Russia tried to attack Starlink (satellite) but the Starlink(satellite) defended itself by updating its software and makes the Russian cyberattack unsuccessful. The economic and infrastructural damage from these attacks was estimated to be in the hundreds of millions of dollars (ENISA,2020).

In response, Ukrainian hackers also launched multiple cyberattacks against Russia. Their aim was to expose Russian propaganda, collect their sensitive data and fight against the Russian cyber aggression. Ukrainian hacking operation Prikormka (Groundbait) on 2016 where the hackers secretly collected the data Russian military and political activities by accessing their computers. Second operation was on May 2016 where Ukrainian hackers successfully hacked 9 websites of Russia which are belongs to Donetsk People's Republic, Russian Propaganda sites of anti-Ukrainian and Russian private military company websites of Ukraine like Kyiv, Ivano-Frankivsk and Chernivtsi, second Ukraine power grid hack on December 2016. Attacked in 2016 on Ukraine's state treasury which government payments (ENISA,2023).

On June 2016 Channel One hack where the Ukrainian hackers known as Ukrainian Cyber Hybrid warfare theory explains that how Russia uses a mix strategy tools to weaken its enemies without starting a full-scale war. In the case of Russia-Ukraine conflict cyberattacks are not the separate tactics they are the part of strategy to destabilize Ukraine, and block support from the other countries. Russia cyber operations includes the spreading misinformation, access to the data government and military systems. Countries which support Ukraine like Poland also targeted by Russia.The attacks on Poland computer system, Prestige attack on transport and supply networks just to stop and weaken the public support for Ukraine. This theory shows that how cyberattacks are the part of larger strategy, their aim was not to win the but weaken the support of other country.

Poland as a key ally of NATO and a strong supporter of Ukraine faced cyberattacks although it is not directly fighting the war it shows that how smartly Russia use cyberattacks to destabilized both Ukraine and its allies (Borucka,2021).

The study aims to explore as a hybrid warfare strategy how Russia used the tactics which only affects the Ukraine but also impacts its boarder regional countries like Poland. This theory shows that how the modern conflict merge traditional military force with cyberattacks and weaken the other state with declaring any open war (Hoffman,2007). The well- known cyberattacks on 2015-2016 on electricity outrage and in 2017 NotPetya malware in Ukrainian institutions identified as a serious national security threat. These cyberattacks are not only limited to Ukraine but the Ukraine supporter Poland also faced the Russian hybrid attacks which means Alliance hacked the Russian major state-run TV channel (CHANNEL ONE). On October 2016 where the Ukrainian hackers leaked approximately 2,300 emails and the documents from the office Vladislav Surkov (a close aide to Russian President Vladmir Putin) which exposed that Russian had been plaining its actions since September 2013 to December 2014 to take over the Russian territories and stir up the unrest in Ukrainian regions.

On February 2022 Ukraine formed its IT Army which especially focused on the cyberwarfare against Russia right after Russia began its full-scale invasion in 2022. It was started by Mykhailo Fedorov, Ukraine's Vice minister and minister of Digital Transformation, their aim was to target the Russian government and business websites. The goal of Ukrainian cyber responses was to disrupt Russian system and defend Ukraine online. These attacks demonstrate that how cyberwarfare has become a prominent feature of Russia Ukraine war.

Poland as a close ally and a member of NATO also affected by this conflict and face increased cyberattacks, disinformation campaigns and pressure on its boarder security. After Russia invaded Ukraine in 2022 the attacks on Poland gets worse because Poland became a key supporter of Ukraine by sending them military and humanitarian aids and pushing strong sanctions against Russia. In the first quarter 2022 Poland experienced more cyberattacks than in 2021).

The cyberattack by Russia on Poland's computer system and Prestige attack in November 2022 on transport and supply networks in Ukraine and Poland. Other Russian groups like Killnet attacked on the Polish Senate websites which was the major attack happened right after when Poland's Senate declared Russia a terrorist state. In March 2022, a cyber incident caused signal failure which shutdown 80% Poland's train network for a day. To tackle these attacks Poland took early steps which s strengthen its cyber defense. Poland raised its cyber defenses from threat level to CHARLIE CRP which help to prepare themselves for government systems and possible attacks. Only 29% of Russian cyberattacks on Poland are being successful because of Poland's early efforts. Like Ukraine, Poland showed that how important it is to work with the private tech companies like Microsoft which helps to defend themselves against cyber threats. So far, Poland had done a great job to protecting itself but they must prepare themselves for bigger cyberattacks.

Theoretical Framework

Russia-Ukraine Cyber Conflict and its Impacts on Poland's national security and the Hybrid Warfare Theory

Hybrid warfare theory explains that how Russia uses a mix strategy tools to weaken its enemies without starting a full-scale war. In the case of Russia-Ukraine conflict cyberattacks are not the separate tactics they are the part of strategy to destabilize Ukraine, and block support from the other countries. Russia cyber operations includes the spreading misinformation, access to the data government and military systems. Countries which support Ukraine like Poland also targeted by Russia. The attacks on Poland computer system, Prestige attack on transport and supply networks just to stop and weaken the public support for Ukraine. This theory shows that how cyberattacks are the part of larger strategy, their aim was not to win the but weaken the support of other country. Poland as a key ally of NATO and a strong supporter of Ukraine faced cyberattacks although it is not directly fighting the war it shows that how smartly Russia use cyberattacks to destabilized both Ukraine and its allies.

The study aims to explore as a hybrid warfare strategy how Russia used the tactics which only affects the Ukraine but also impacts its boarder regional countries like Poland. This theory shows that how the modern conflict merge traditional military force with cyberattacks and weaken the other state with declaring any open war. The well- known cyberattacks on 2015-2016 on electricity outrage and in 2017 NotPetya malware in Ukrainian institutions identified as a serious national security threat. These cyberattacks are not only limited to Ukraine but the Ukraine supporter Poland also faced the Russian hybrid attacks which means that cyberattacks are deeply interconnected with each other and directly impacting the security of neighbouring nations like Poland.

From the perspective of hybrid warfare theory demonstrates that how modern conflict are not only limited to the only military battle but thy also includes cyberattacks, misinformation, political manipulation and economic instability. Russia use of cyber tools in disrupting or hacking the Ukraine government system not only aims to weakening the Ukraine internally but it using cyber tactics to gain influence without directly confronting NATO.

Poland due to its strategic location, member of NATO and as a frontline supporter of Ukraine had increasingly found itself as part of Russia's strategy. Russia also escalates cyberoperation against Poland's government agencies and tries to undermine its role as a key supplier and logistics hub for Ukraine which shows that how hybrid warfare not only aims to defeat the single territory but to destabilized an entire region. Poland is involved into the conflict due to its alliances and regional infrastructure which makes it strategic target within Russia boarder hybrid warfare campaign (Deibert, 2019).

The consequences of cyber operations not only affect the internal structure and the boarder environment of Ukraine but also impacts its neighbouring country Poland. The cyberattacks on Ukraine damage the faith of public in government institutions, misinformation leads to internal and external conflict and social tensions in Ukraine. Economic impacts of Russian cyberattacks targeted the energy and finance sectors which leads towards the disruptions economic instability in Ukraine. Russia uses the conventional and nonconventional tactics which destabilize the Ukraine. Although Ukraine responds this to by strengthening ties with NATO and US and making agencies like SSSCIP by which their cyber defense posture is improved. Hybrid conflict theory shows that Poland is not a direct party who is fighting directly, its share infrastructure, alliances, geopolitical positioning pushing it towards the conflict. Ukraine response to Russia cyberwarfare strengthening its defense which deepens the co-operation with NATO and US and making agencies like State Service of Special Communication Information Protection which made the cyber defense system of Ukraine strong.

By applying hybrid warfare theory to the Russia Ukraine cyber conflict, it becomes clear that Russia's strategy of using cyber operation, political manipulation and misinformation destabilized the Ukraine without declaring any open war. Unlike traditional warfare hybrid theory emerged military war and cyberwar which to weakening the opposite state and its allies. Russia cyberattacks on Ukraine such

Power grid in 2015-2016 and NotPetya malware in 2017 marks a instability and weakening the Ukrainian sovereignty and resilience. The hybrid threat also impacts the Ukrainian boarders and have significant impacts on Poland. Poland is not directly fighting in the conflict but it pulled up into conflict due to its strategic infrastructure, alliance and geopolitical alignment.

Understanding the conflict through the lens of hybrid warfare gives the aspects of multi-layered approach where Russia use cyberattacks, misinformation and political manipulation. The conflict not only destabilized the Ukrainian territory but also has its impacts on neighbouring countries like Poland. This highlights the importance of cyber and strategic defense efforts across the region.

Effects on Poland's Cybersecurity Policy and Strategic Posture

- **Theory Application**

In 2014, after the Annexation in Crimea Russia-Ukraine cyber conflict represents in the case of hybrid warfare. Russia used cyberattacks, misinformation, political manipulation to destabilize Ukraine without any direct conventional war. Their tactics also have several impacts on the Ukrainian neighbouring countries, especially in Poland which NATO frontline member and a strategic actor in Eastern Europe.

Discussion

In 2014, attacks on Ukrainian infrastructure by Russia includes attacks on Black Energy malware in 2015 and later NotPetya in 2017. Cyber operations could easily spill over the national boarders recognized by the Polish Policy makers. Their attacks not only destroyed the Ukrainian institution but also affected the financial and logistics institutes in Poland.

- **ENISA Report, 2018**

It describes that NotPetya attack although targets the Ukrainian multination companies which branches with Poland such as Maersk and FedEx causing disruption in Poland's shipping and banking sectors. In response to these threats, Poland introduces different national policy changes.

❖ **National Cyber Security strategy (2017-2022)**

In response to these threats, Poland introduces different national policy changes which focuses on co-ordination with different institution in order to build a network response or increasing the cyber defense capabilities.

❖ National Cybersecurity System act (2018)

It implements the cybersecurity protocols on the energy grid health services and banks, national security teams CSIRTs which co-ordinates threat detection and respond them back and also the mechanism for public and private co-operations are established.

❖ **Creation of Cyber Defense Forces (2022)**

It was a military cyber unit under the polish minister designed to counter act the foreign cyber threats from Russian group like APT28 (Fancy Bear) and Sandworm. Poland strategic position in cybersecurity become more important.

❖ **NATO Engagement**

Poland joined NATO Cyber Defense Pledge and starts participating in different NATO led cyber defense exercises like Locked Shields and Cyber Coalitions. In Estonia contributed in Co-operative Cyber Defense Centre of Excellence (CCDCOE).

❖ **EU Co-operation**

Aimed to defend their allies from major cyber threats, to strengthen in regional adaptability co-ordinate with ENISA and integrated with EU Cybersecurity Act in 2019.

❖ **Empirical Data**

According to ENISA THREAT LANDSCAPE REPORT, 2018-2023.In 2014, Russian cyberattacks starts in Ukraine and increase the threats in Poland's Polish agency. In 2015, Black Energy malware in Ukrainian energy grid and warns similar threats in Poland. In 2017, NotPetya malware from Ukraine which disrupt Poland banking and transports. In 2018, Poland enable National Cyber Security System Act which impacts Poland Cybersecurity sector. In 2020-2022 Russian misinformation and full-scale invasion on of Ukraine, Poland enhances and strengthen their military operation and regional responses with NATO and EU.

Poland contribution to regional and international efforts to counter cyber threats

❖ Theory Application

The theory explains that how modern warfare and conventional military war emerges with each other by using different cyber tactics to destabilize each other. In this cyber dispute Russia used Cyber tools against Ukraine which not only affect the Ukrainian infrastructure but also its neighbouring countries especially in Poland. It also explains the Poland's defense system and co-operation campaigns against Russian cyberattacks.

Discussion

❖ NATO Co-operative Cyber Defense Centre of Excellence (CCDCOE)

After the attacks Poland has been the active member in joining and participating in the cyber exercise of military such as Lock Shields and Cyber Coalition where they are allied against the Russian cyber-attacks.

❖ NATO Exercise

Poland hosted the Defender Europe 2022 in the recent years, showing its frontline strategic view by joining the cyber operations and electronic warfare units.

❖ EU NIS Directive Implementation (2014)

To improve their cybersecurity objectives, cross-border co-operation and to standardize or prevent their critical infrastructure Poland adapted the NIS Directive in order to work together Poland and EU countries on the cybersecurity.

❖ Poland Support Ukraine

Poland provides cybersecurity infrastructure to the Ukrainian govt network in the February 2022 invasion described the Polish Ministry of Foreign Affairs(2022). Russian cyberattacks includes disruption in communication lines, DDoS and phishing attacks, Polish cyber units helps to restore and defend themselves against the attacks.

❖ **Education and Training programs**

Ukrainian institutes collaborate with Poland's Universities (Military University Of Technology and Warsaw University of Technology) for the training of cybersecurity.

❖ **Civilian Cyber Units**

Poland respond the cyber threat by empowering the Civilian Volunteer tech Experts by assisting the cyber monitoring and counter the disinformation campaigns of Ukraine.

❖ **Private-Public Partnerships**

Partnership of state agencies with Polish cybersecurity firms which provides support to EU and NATO by malware analysis, intelligence of threats and the further incident response.

❖ **Empirical Data**

Poland is the active contributor in NATOCCDOE exercises in 2022. According to Poland Ministry of Digital Affairs and Polish MFA (2022) Poland developed alliance with NATO-EU defense frameworks and providing the cyber defense aid in in 2022 Ukrainian invasion. Increased resilience in the Polish banks and tech firms and Russia targeted in EU countries reported in Microsoft Digital Report (2022) and ENISA threat Landscape.

Methodology

This study adopts a qualitative research methodology, by focusing on the data analysis of existing secondary data, includes literature, government publication and cybersecurity reports policy briefs and think tanks assessments related to Cyber dispute of Russia-Ukraine and its impact on Poland. This enables a comprehensive understanding on the nature of war and specific challenges and responses by Poland. The data collection was conducted through a review of extensive article reports from organization such as CERT Polska, the ENISA, NATO'S CCDCOE and cybersecurity focused think tanks such as Warsaw institute and Carnegie Europe. This research also incorporates with policy documents and frameworks released by European Commissions, NATO, and polish national authorities. It includes the impact of cyberoperation on policy national infrastructure, role of Poland in NATO and EU in cyber defense initiatives, policy gaps and institutional challenges faced by Poland and regional security implications of cyber conflict for Eastern Europe.

By critically analyzing the literature this research aims to show a understanding on Poland's cybersecurity posture and its strategic responses. This methodological approach highlights the geopolitical conflict of Russia-Ukraine and digital security objectives in the 21st century.

Review of the Literature

A comprehensive literature review for understanding the complex and multifaceted nature of cyber warfare of Russia-Ukraine and its impact on Poland's national security. The conflict between Russia and Ukraine increased the cyber threats, changes the security of Easter Europe and affected Poland directly because it is key ally of NATO and EU and play a key role in regional security. The conflict is not only limited to traditional surveillance. Making a cyberspace an important tool cyber capability has expanded to misinformation and influence information in modern space craft described by Rid (2013). These operations are the tactical moves to achieve political influence not only the targeted territory but also in their regional allies. For instance, Russian cyberattacks or misinformation campaigns on Ukraine had direct impacts on Poland. Poland also faces increased exposure to malware attacks, fake news campaigns from Russian militant groups. The 2016 Presidential Election in Ukraine, Russia hacked their emails and start spreading the false news (Healey, 2019). Similarly, in Central Europe they disrupt the EU unity and manipulating their public opinion. In today's world cybersecurity and cyber threats are the major concerns which not only affect the individual but also causes national and regional stability. The risk of cyberattacks rises when nations starts digitizing their military, economy and civil infrastructure. Joseph Nye (2017) explains that how today's national security extended to the deeply realm, where traditional and non-traditional threats are often identical. Nye also highlights that cyber-powers has blurred the boundaries between state and nonstate actors and transforming their national and economic security. A case study of Russia-Ukraine cyber dispute not only destabilized the country but also the entire region. After the annexation of Crimea in 2014, Russia targets Ukrainian government and launched series of attacks on their media, institutions and cyber infrastructure. Greenberg (2019) describes the devastating attacks such as NotPetya and WannaCry which affects Ukrainian public and private sectors and also its neighbouring countries like Poland. These cyberattacks disrupted the economy, exposed vulnerabilities in critical infrastructure includes power grids and infrastructure. For instance, 2015 and 2016 cyberattacks on Ukrainian power grids which are documented by Lee, Assante, & Conway (2016). The swift integration of cyber operation has left the states close to war zones, like Poland which is extremely vulnerable. As a EU member and frontline NATO, Poland exposed the cyberthreats by making a review of academic and policy-oriented literature which is crucial for the national and regional cybersecurity environment. Studies emphasizes that how Russia deployed their cyber operations strategically to support their military actions in Ukraine but not only targeting the Ukrainian infrastructure as well as its neighbouring supporting countries like Poland. According to the European Union Agency of Cybersecurity (ENISA, 2023), marked the increase in the cyberattacks against the Polish Public institutions, energy grids and the media platforms which are the part of Russian warfare strategy. These findings are documented by CERT Polska (2022) includes the rise of attacks, misinformation campaigns by targeting of the Polish systems.

In analyzing Poland's cybersecurity there are several works which includes The Atlantic Council and Carneige Europe, which defines the role of Poland in strengthening their regional cyber defenses. The discuss how Poland has become a cybersecurity hub in Eastern Europe due to its strategic location or by investing in its infrastructure legal framework and international collaboration. The paper "Cybersecurity in the EU: threats Landscape and Recommendations" highlights Poland's contributions in NATO and EU led cybersecurity initiatives, which includes joint cyber exercises and threat intelligence sharing. The NATO (CCDCOE) also identifies its their warfare tactics by using the cyber tools employed alongside the conventional military conventional military force. However, the challenges remain. Research by the Brooking Institutions (2022) highlights the difficulties in cyberattacks which delayed responses and weakens the deterrence. Similarly, Warsaw Institute (2022) also highlights interagency coordination, public awareness and cybersecurity education in Poland which restrict the country to defend against cyber threats.

Disinformation is also domain of concern

The study "The Russian Information Wain Central Europe" (2022) shows Russian backed media and troll networks are actively influence public opinion in Poland, particularly contentious issue such as Ukrainian refugee support, NATO presence and EU policy alignment. Despite these challenges, literature reveals a strong path for Poland's responses to the cyber threats. Investing more in national cyber infrastructure, aligning with EU cybersecurity rules and participating in the cyber alliances are the ways that country improves its national security posture.

Conclusion

In conclusion, Russia-Ukraine cyber conflict and its impact on Poland's national security in understanding the role of cyber warfare in modern conflicts. The ongoing conflict between these two stated also affected European countries like Poland, it starts from 2014 and intensifies in 2022, that how cyber capabilities combined into boarder military and political strategies. Russia uses cyberattacks includes misinformation campaigns, public institutes and their military systems aiming not only destabilized Ukraine's infrastructure but also have major impacts on its neighbouring countries like Poland and also highlight the cyberspace as a conflict domain. Ukraine evolves in the cyber defense strategy through the support from international actors such as NATO and EU and several private sectors firms by highlighting the importance of cyber warfare and international co-operation. This conflict also demonstrates that cyber operations are not just supplementary tools they are now core component of deterrence and warfare. The conflict between Russia and Ukraine describes the nature of the modern warfare, where the cyberoperations are as important as traditional military strategies. Since 2014 Annexation in Crimea and the full-scale invasion in 2022, Russia deployed several cyberattacks aimed to destroy the Ukrainian infrastructure by spreading misinformation and manipulating the public trust. Their attacks not only targeted the Ukrainian government but also major impacts on financial institutions, energy grids and media. These attacks also affect the Poland national security. In response, to these attacks Ukraine immediately strengthens its cyber defense by co-operating with NATO and EU. Poland key ally of NATO and EU also face threats from Russia to supporting Ukraine. Poland also strengthens its cyber defense strategies and became a leader of regional cyber security by contributing in Eastern Europe stability and working with NATO and EU, which helps Poland to counter the Russian threats.

Despite the huge efforts to strengthen their cyber capabilities, Poland still faces a lot of challenges to overcome when they're dealing with the consequences of cyberwarfare from Russia-Ukraine war. Since Poland has been an excellent partner in NATO cyber defense initiatives or regional alliances. The complexity of Russian cyber aggression includes a vast misinformation campaigns, attacks on infrastructure and partnership in the security measures. Russian cyber operations such as spreading misinformation campaigns on Polish sites and they try to hack infrastructure which cause political mistrust and public anxiety. The study highlights Poland's posture about cyber aggression in any future negotiations includes the collective response from EU and NATO., their ability to respond the challenges are also improved. Poland learns from Ukrainian cyber experiences and their investments in cyber defenses programs helps them to secure cyber space in Eastern Europe which enhances the Poland regional cybersecurity.

References

Betz, D., & Stevens, T. (2011). Cyberspace and the state: Toward a strategy for cyber-power. Routledge.

Binnendijk, H., Marler, T., & Bartels, E. M. (2020). Deterring cyberattacks: How to reduce vulnerability through planning and deterrence. RAND Corporation.

Borucka, A. (2021). Poland's cybersecurity strategy in the context of regional security. Security and Defence Quarterly, 34(2), 1–20.

Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. HarperCollins.

Czarnecki, M. (2023). Poland's response to Russian cyber threats: A case study. European Cybersecurity Journal, 9(1).

Deibert, R. J. (2019). Reset: Reclaiming the internet for civil society. House of Anansi Press.

ENISA. (2021). State of cybersecurity across the EU: Country insights – Poland. European Union Agency for Cybersecurity.

ENISA. (2022). Cybersecurity for critical infrastructure in the EU. European Union Agency for Cybersecurity.

ENISA. (2023). Threat Landscape 2023. European Union Agency for Cybersecurity.

European Commission. (2023). Joint communication on the EU's cybersecurity strategy for the digital decade. https://eur-lex.europa.eu

Giles, K. (2016). Russia's hybrid warfare: A success in propaganda. NATO Defense College.

Healey, J. (2019). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

Jensen, B. M. (2018). Cyber deterrence and the problem of attribution. Strategic Studies Quarterly, 12(4), 14–35.

Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 30(2), 167–214.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber-attacks shape battlefield events? Journal of Conflict Resolution, 63(2), 410–437.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyberattack on the Ukrainian power grid. SANS ICS Report.

Maurer, T. (2018). Cyber norms and the United Nations. Journal of Cybersecurity, 3(1).

Ministry of Digital Affairs of Poland. (2021). National framework for cybersecurity.

Ministry of Digital Transformation of Ukraine. (2022). Cybersecurity strategy of Ukraine.

NATO. (2022). Strategic concept – Enhancing NATO's cyber defense capabilities.

NATO. (2023). Cyber Defence Pledge: Implementation and progress report.

NATO CCDCOE. (2023). Locked Shields exercise: Lessons and findings.

Nye, J. S. (2017). Power in the cyber age: From realism to neorealism. Harvard Kennedy School.

Polish Ministry of National Defence. (2019). Cybersecurity strategy of the Republic of Poland 2019–2024.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Tikk, E., Kaska, K., & Vihul, L. (2010). International cyber incidents: Legal considerations. CCDCOE.

U.S. Department of Homeland Security. (2022). Russia's cyber operations in Ukraine: Lessons learned.

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. Oxford University Press.

Zetter, K. (2020). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Crown.

Article Information:

Received	*6-Mar-2025*
Revised	3-May-2025
Accepted	1-Jun-2025
Published	15-Jun-2025

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**

- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest**: NIL

- **Funding Sources**: NIL

Correspondence:

Fiza Zeeshan

f.zeeshan@gmail.com