Journal of Climate and Community Development
A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal
E-ISSN: 3006-7855 P-ISSN: 3006-7847

Militarization Development in Cybersecurity and Shift in Poland's Security Strategy After Russia-Ukraine War

Mussa Iqbal [1] **Rami Bashir** [2] **Umme- e- Rubab** [3]

[1] M.Phil. Scholar, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

[2] M.Phil. Scholar, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Email: romebux02@gmail.com

[3] M.Phil. Scholar, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Email: rubab.naqvi7676@gmail.com

Corresponding Author: mussaiqbalgill@gmail.com

Vol. *4,* ***Issue*** *1, 2025*

Article Information

Received:

2025-03-13

Revised:

2025-05-17

Accepted:

2025-06-15

ABSTRACT

The article focuses on how Russian-Ukraine War change concept of security in Europe. the study also elaborates the larger framework of national security, how war on Ukraine security concern of Europe and especially for Poland which share a boarder with Ukraine and military and cyber security development in reaction to counter Russia.the effects of this War on the dynamics of European security cannot be undermined. This research offers a thorough analysis Poland's policy and strategy shift in security, with a Lens of balance of power theory to maintain balance of power, which this battle has altered in the region. It explores emphasis of how nations, such as Poland prioritized defense measures and fostered regional cooperation in response to tackle security concerns and a powerful enemy. It also takes into account that, beside alliance with NATO, which was as external balance of power measure and remains trustful, Poland shifts its strategy to internal balance of power approach by build its own military capabilities in conventional, cyber security and cyberspace.

Keywords: *Military Modernization, Cyber Security, Cyber Space, Security Shift, Security Strategy.*

Citation: APA

Iqbal, M., Bashir, R & Rubab, U. (2025). Militarization Development in Cybersecurity and Shift in Poland's Security Strategy After Russia-Ukraine War, Journal of Climate and Community Development, 4(1), 237-243.

Introduction

On 24 February2022 Russia initiate a full-scale war on Ukraine, which raise economic and security concern of Europe and especially for Poland which share a boarder with Ukraine.the effects of this War on the dynamics of European security cannot be undermined. The Russian escalation disrupts equilibrium of power and raised security concern in all over the Europe. This change in power balance and make a situation of anarchy. The anarchic order is defined as absence of an effective regional institution to maintain balance of power. Anarchy is characterized with power struggle and arms modernization in state for their security. Same is happening after Russian invasion in Ukraine, which create an insecurity in Europe and they focused on security and arms development. Poland which is on eastern border of Europe holds the first place in this pursuit. Poland insecurity is logical. Before Ukraine - Russia war Ukraine was serving as buffer space between Russia and Poland but now a powerful Russia is on the border of Poland.

Although Poland is member of NATO and abrupt adoption of NATO standards by member states started to pick up momentum not seen in past. But NATO alliance is not reliving Poland security dilemma created by perceived threat of Russian military capabilities of a state constitute.

There are two main reasons of this security dilemma. 1st the dominance of Russia in war despite of massive support of NATO and America. 2nd trump administration concerns about alliance, theirs funding and motive to withdraw from alliances. These reasons shake the believe in NATO. to gain balance of power against the Russia Poland started its military built-up and modernization. to achieve these strategic and security goals Poland increase its spending on defence. Poland makes many agreements to purchase military equipment and also adopt strategies to strength the field of cyber security Which is future battlefield. Cyber Security Summit and Expo held in Vienna in February 2024 reveled, from Check Point Research findings, that Poland has emerged as the foremost nation globally in terms of cyber-attacks. The Polish Cyberspace Defense Forces reported that in February 2024, Poland experienced over 1,000 cyber-attacks on different organizations in each week, making it the most targeted country worldwide. The surge in cyber-attacks became particularly pronounced in 2022. following the Russian invasion of Ukraine in February of that year. At that time, Poland was already among the most frequently attacked nations, and the frequency of these incidents has continued to rise since then. A significant number of Polish enterprises remain inadequately prepared for cyber threats. A study conducted by AON revealed that fewer than 43 percent of businesses in Poland have established a post-incident response plan or conducted a formal risk assessment regarding cyber-attacks. Investment in cyber defense within Poland has been on the rise in recent years, with the industry experiencing a 14 percent growth in value during 2023, as reported by the Polish publication Rzeczpospolita. Poland showed notable developments in cyber security solutions public and private sectors. U.S. companies that specialize in advanced cyber security technologies may find significant opportunities with Polish government and private sector entities aiming to enhance their cyber security frameworks and preparedness. and next war in Europe will be hybrid war instead of conventional war.

Literature Review

On 24 February 2022 Russia initiated a full-scale war on Ukraine which raise economic and security concern of Europe and especially for Poland which share a boarder with Ukraine.the effects of this War on the dynamics of European security cannot be undermined (Burant, 1993).

The Russian escalation disrupts equilibrium of power and raised security concern in all over the Europe. also altered the power balance and make a situation of anarchy.

The anarchic order is defined as absence of an effective regional institution to maintain balance of power. Anarchy initiates arms race and modernization, as in Poland after Russian invasion in Ukraine, which on eastern border of Europe (Liu, 2016). In an anarchic environment, the growth of one's capabilities unsecure other, result in vacuum which states try to fill by acquiring arms to preserve balance of power (Kivimäki, 2012).

Despite all support of NATO, Russia seems unbeatable in Ukraine, which makes Europe more

worried about its security and forced to think to redefine its security architecture. adoption of NATO standards stated to pick up momentum not seen in past to gain balance of power against the Russia (Mukarzel, 2023). 2022 invasion was also a wakeup call and all of NATO's structures are being modified to better align the defense alliance with the new reality and to maintain balance of power. threats on its boarder make it realize to change it security strategy. It is also unknown what will happen in future. God know, West might be divided and NATO might be dissolved. so, he makes a shift in its security policy by taking a step of internal balance of power. He started to build its own military power and making it more advance to tackle a situation in both military and non-military expressions.

The Ukraine war also make it realize that the current crisis is a longer-term in order to be ready for this, Poland needs to increase its investments in the military security strategy (Kamiński, 2023). to achieve these strategic goals Poland, increase its spending on defence.

Table 1: *Yearly Defense Budget of Poland.*

Year	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Approximate Defense Spending $ billion	10.36	10.67	10.30	9.8*	9.5	10.1	12.5	12.5	13.3	14.0	24.0

The above table depicts the drastic increase in Poland's spending on defense in 2021 and 2022 the defense spending was 13.3 and 14 billion USD which drastically rose to 24 billion USD in 2023 (over 50%) (Dorn, 2024).

Such huge spending in military buildup shows Poland's strategy to gain enough power to create balance of power and capability to counter Russia (Mix, 2023). To gain this goal Poland ordered 1000 Korean K-2 and Abraham tanks to build up its armor, which will arrive in 2026 (Jang, 2023). Poland signed another order of K-9 self-propelled gun-howitzers in 2022 to strengthen its defense capability (Muzyka, 2020). As it indigenous gun howitzer K9PL will be in lines after 2026. Furthermore, Poland is adding up to 400 new Rosomak APCs units in its line nest year (Śledź, 2024). The Russian Ukraine war also eliminates another thing that a well-defended position has no value without air superiority. Keeping this in mind Poland going to extend its air strike and defense capabilities with multi layered anti air infrastructure (Lubiejewski, 2023). patriot batteries, CAMM systems, PSR-A Pilica and up to 3000 Piorun MAND PADS also acquired to strengthen the air and missile defense system (Grobelny, 2023).

Another important step in modernization and strength building is effectiveness is rocket-artillery systems. Poland increased it from 40Km to 300Km of range. The eye-catching thing is a deal of nearly 500 HIMARS Rockets with aims to become the foremost artillery force in Europe. It will enable Poland to effectively hit enemy troops and logistics. As long-range strike capability, Poland is also interested to acquire a close-range missile inventory or air support cover.

In September of 2022 Poland also order 96 AH-64E Apache attack helicopters equipped with longbow radar from American to achieve a superior Strick range that will enable Poland to damage Russian armor and surly will help to hold Russia's mobility (Gill, 2024). The war in Ukraine also gave a practical experience. That smaller units, like drones, are more affordable and efficient in short range missions as compare to helicopters. keeping this in view Poland prioritized the introduction of drones of all classes in the future such investments would offer better value for the money. And if we talk about combat aircrafts Poland has already sign a deal with Korea to buy 32 F5 As and 48 FA50 (Bogusz, 2024).

The Ukraine war scenario also illuminate that Russia views NATO as a strategic alliance that could be undermine through a variety of non-military means like, political corruption, disinformation campaigns in EU nations, pressure from migrants and economic instability. the Ukrainian conflict revealed Russian strategy of using cyber-attacks to week enemy before on ground attack. keeping this in mind Poland also developing it cybersecurity and cyber space

capabilities (Karpiuk, 2023). As the conflict evolved, the Russian military adapted its cyber-attacks to meet the demands of wartime conditions. Both cyber and conventional weapons were utilized in assaults on nuclear power facilities, government networks, and various agencies. The report "Microsoft A Year of Russian Hybrid Warfare in Ukraine," published in March 2023, outlines the evolution of Russian destructive cyber-attacks. Cyber threats have adapted to the growing destructive and intelligence capabilities of Ukraine and its allies' civilian and military assets. Cyber operations were categorized into three phases: Phase 1 (January-March 2022) aimed at securing victory in Ukraine, Phase 2 (March-September 2022) focused on destructive attacks targeting the logistics and transportation sectors, and Phase 3 (September onward). The escalation of military and cyber operations aims to undermine the resolve of Ukrainian society. In Phase 3, Russian cyber threat actors executed attacks utilizing wiper malware targeting energy and water infrastructure, alongside intelligence operations directed at NATO organizations.

Cyberspace is the future battlefield. It consists of all the world's computer networks and everything they connect and control via cable, fiber optic, or wireless connections. In addition to the Internet, cyberspace includes many other computer networks, including those not connected with Internet.

Enemy can hack or destroy these networks, steal all the data or planting instructions to transfer money, blow up oil refineries, launch missles, these all threats are linked which would result in the financial system collapsing, the supply chain disruption, space satellites being lost from orbit, and air traffic disruption (Humayun, 2020). Poland is taking many measures in cyber security field to create a comprehensive system to protection against digital threats. Before the Russian invasion on February 24, 2022, Ukraine experienced a cyber-attack just hours prior, on February 23. This attack employed a cyber-weapon known as "Foxblade" and targeted 19 government entities along with critical infrastructure in Ukraine. This indicates that Russian employed cyber strategy in invasion that included three distinct, occasionally coordinated actions: destructive cyber-attacks on Ukraine, network infiltration and espionage beyond Ukraine's borders, and cyber influence operations aimed at a global audience (Lin, 2022). Russian key elements of the tactics employed in the cyber-attack on Ukraine, the first element involved targeted phishing and other methods designed to breach computer networks, manipulating users to acquire sensitive information and login credentials. The second element pertained to the deployment of "wiper" malware, which obliterates data on hard drives, making recovery impossible. The third element involved disseminating malicious software to additional computers within the network, such as those in the Ministry, to broaden the attack's reach and facilitate further infiltration. State-sponsored hackers from Russia engaged in aggressive maneuvers to secure dominance in cyberspace. Additionally, Moscow undertook information operations to influence the narrative surrounding the conflict. The invasion of Ukraine has prompted shifts in the Eastern European cybercriminal landscape, potentially leading to long-lasting implications for the scale and coordination of cybercrime on a global scale

Poland in year 2024 systematically enhanced and developed the national cybersecurity outline. The foundation of cybersecurity will relies on initiatives that bolster the resilience of information systems in all sectors, as well as ability to effectively prevent incidents. It is notable about 40% of public administration units adopted cloud computing services that in 2023, a notable increase from approximately 31% in 2019. To maintain this upward trajectory Cybersecurity Standards are essential.

After Russia-Ukraine conflict, Poland created a clear legal foundation for handling cyber risks across critical infrastructure, public administration, and private sector operators, Poland security strategy adopt a dynamic shift and add cybersecurity as integral part of its security strategy. For detecting, disclosing, and addressing cyberattacks, cybersecurity authorities are made. CSIRT NASK, and sectoral CSIRTs for energy, finance, and healthcare. After Russia-Ukraine conflict, Poland created a clear legal foundation for handling cyber risks across critical infrastructure, public administration, and private sector operators, Poland security strategy adopt a dynamic shift and add cybersecurity as integral

part of its security strategy. For detecting, disclosing, and addressing cyberattacks, cybersecurity authorities are made like, Governmental Computer Security Incident Response Team (CSIRT GOV), the national-level CSIRT NASK, and sectoral CSIRTs for energy, finance, and healthcare (Siemieniak, 2024).

Poland has taken significant measures to improve data protection., Polish companies and government agencies have adhered to the fundamental principles of data minimization, user permission, and breach notification, A key regulatory function is played by the Office of Protection of Personal Data (UODO), which oversees the GDPR's implementation, imposes administrative penalties, and informs the public about their rights regarding personal data (Żurawski, 2025). Government organization, army and corporations have implemented advanced security measures including firewalls, endpoint detection, and intrusion prevention systems (Dorobisz, 2024).

Poland needs to adopt more adaptive, intelligence-driven cybersecurity frameworks to engage Emerging technologies which would give a new shape to cybersecurity (Kolisnichenko, 2025).

Research Methodology

In this study, we employed a systematic literature review method and network analysis using VOS viewer to identify the leading research topics in the context of hybrid warfare, both in general and with a focus on Poland and Ukraine. Subjective data obtained from peer review articles, Research generals and websites. Theory of balance of power and its variant internal balance of power applied to explain the phenomena of military advancement in Poland in reaction of Ukraine Russia war.

A systematic literature review was selected as the research method to discover research topics and their interrelationships in the field of hybrid warfare. The systematic review was chosen because it involves rigorous procedures for searching and selecting articles for review, providing a methodological basis for synthesizing research topics effectively (Snyder, 2019). Exploring the existing literature on the relationships within the thematic area of hybrid warfare was based on the identification of available studies using keywords.

Conclusions

The Russian escalation disrupts equilibrium of power and raised security concern in all over the Europe. This change in power balance and make a situation of anarchy, which initiates arms modernization, in Poland to preserve security, which is called balance of power. Poland started to invest heavily in military and cyber security field. During the CPX Cyber Security Summit and Expo held in Vienna in February 2024, findings from Check Point Research indicated that Poland has emerged as the foremost nation globally in terms of cyber-attacks. The Polish Cyberspace Defense Forces reported that in February 2024, Poland experienced over 1,000 cyber-attacks on organizations each week, making it the most targeted country worldwide. The surge in cyber-attacks became particularly pronounced in 2022, After Russia-Ukraine conflict, Poland created a clear legal foundation for handling cyber risks across critical infrastructure, public administration, and private sector operators, Poland security strategy adopt a dynamic shift and add cybersecurity as integral part of its security strategy. For detecting, disclosing, and addressing cyberattacks, cybersecurity authorities are made like CSIRT, NASK, and sectoral CSIRTs for energy, finance, and healthcare. After Russia-Ukraine conflict, Poland created a clear legal foundation for handling cyber risks across critical infrastructure, public administration, and private sector operators, Poland security strategy adopt a dynamic shift and add cybersecurity as integral part of its security strategy. For detecting, disclosing, and addressing cyberattacks, cybersecurity authorities are made like, Governmental Computer Security Incident Response Team (CSIRT GOV), the national-level CSIRT NASK, and sectoral CSIRTs for energy, finance, and healthcare.

Poland has taken significant measures to improve data protection., Polish companies and government agencies have adhered to the fundamental principles of data minimization, user permission, and breach notification, A key regulatory function is played by the Office of Protection of Personal Data (UODO), which oversees the GDPR's implementation, imposes administrative penalties, and informs the public about their rights regarding personal data. Government organization, army and corporations

have implemented advanced security measures including firewalls, endpoint detection, and intrusion prevention systems. Poland to adopt more adaptive, intelligence-driven cybersecurity frameworks to engage threats. which give a new shape to cybersecurity. Investment in cyber defense within Poland has been on the rise in recent years, with the industry experiencing a 14 percent growth in value during 2023, as reported by the Polish publication Rzeczpospolita. Poland has made great strides in creating a strategic, institutional, and legal basis for data protection and cybersecurity. The nation must, however, keep enhancing its cyber resilience through public involvement, workforce development, legislative adaptation, and international collaboration as digital technologies advance and cyber threats become more complex. Poland can guarantee the long-term trust of its citizens and partners in the digital sphere, as well as the protection of its data and infrastructure, by integrating cybersecurity as a fundamental element of its digital future.

Conflict of Interest

The authors showed no conflict of interest.

Funding

Funding

The authors did not mention any funding for this research.

References

Bogusz, D. (2024). Polish Air Force.

Burant, S. R. (1993). International relations in a regional context: Poland and its eastern Neighbours—Lithuania, Belarus, Ukraine. *Europe-Asia Studies, 45*(3), 395-418.

Dorn, F. P. (2024). European Defence Spending in 2024 and Beyond: How to Provide Security in an Econo-mically Challenging Environment. *Institute-Leibniz Institute for Economic Research at the University of Munich*.

Dorobisz, J. (2024). Analysis of trends and risks in the field of network security based on statistical data. *GIS Odyssey Journal*, 147-163.

Gill, B. L. (2024). Geopolitics, Military Modernisation and the Future of the Indo-Pacific. *Taylor & Francis.*

Grobelny, Z. K. (2023). Defense and deterrence as the foundation of the a2/ad system in smart city air defense. *Safety & Defense*, 14-23.

Humayun, M. N. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 3171-3189.

Jang, W. J. (2023). The Rise of Korea's Defense Industry in the New Global Security Paradigm. *Korea Institute for Industrial Economics and Trade*, 23-37.

Kamiński, M. A. (2023). Poland's Threat Assessment. *Prism, 0*(2), 130-147.

Karpiuk, M. M. (2023). The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity. . *Polish Political Science Yearbook*, 155-163.

Kivimäki, T. (. (2012). Southeast Asia and conflict prevention. *The Pacific Review*, *25*(4), 403-427.

Kolisnichenko, P. (2025). Poland's Digital Leap: Progress, Challenges and Opportunities. Digital Transformation and IT Implementation. *Driving Sustainable Development Across Nations*, 153-182.

Lin, H. (2022). Russian cyber operations in the invasion of Ukraine. *The Cyber Defense Review*, 31-46.

Liu, X. (2016). Anarchy in the East: Eurocentrism, China-centred geopolitics and uneven and combined development. *International Politics*, 53, 574-595.

Lubiejewski, S. (2023). Conclusions from the use of aviation in the first half of the first year of the Ukrainian-Russian war. *Security and Defence Quarterly*, *42*(2), 68-10.

Mix, D. E. (2023). Poland: Background and Us Relations. *Current Politics & Economics of Europe*, 34.

Mukarzel, R. (2023). The Russo-Ukrainian war and its transformative impact on European security dynamics: shifting power, emerging challenges, and future implications. *Doctoral dissertation, Notre Dame University-Louaize).*

Muzyka, K. (2020). Russian Forces in the Western Military District. *Center for Naval Analyses (CNA).*

Siemieniak, M. (2024). Analysis of the use in Polish industry of modern technology resources as tools for building smart structures. *Zeszyty Naukowe Politechniki Poznańskiej*.

Śledź, P. (2024). The restructuring process of the Polish defence industry in the twenty-first century: doing more of the same while expecting different results. *Defense & Security Analysis*, 1-20.

Żurawski, S. C. (2025). Effectiveness of information security incident management systems: identifying practices, challenges and development perspectives.