Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1182-1199
ISSN – E 2958-8731 P 2958-8723

The Impact of Descriptive Technologies in the Russia-Ukraine War on Poland's National Security

Javeria Nazir[1]

Abstract

The Russia-Ukraine war has ushered in an era where descriptive technologies play a central role in shaping military outcomes and national security policies. This paper examines how technologies such as satellite surveillance, AI-driven analytics, and cyber intelligence are influencing the dynamics of the conflict and, by extension, Poland's security posture. Using neorealism as the theoretical lens, the study analyzes Poland's strategic adaptations, including military modernization and increased investment in open-source intelligence (OSINT). Through qualitative analysis of policy reports, OSINT platforms, and case studies, the paper highlights how Poland is leveraging technology to reinforce its defenses amid a volatile geopolitical landscape.

Keywords: Descriptive technologies, Russia-Ukraine war, Poland, national security, neorealism, OSINT, cyber intelligence, satellite surveillance

Introduction

The Russia-Ukraine war, escalating dramatically since 2022, has significantly altered the European security landscape. Descriptive technologies—including satellite imagery, cyber tools, and artificial intelligence—have transformed traditional warfare (Maxar Technologies, 2022; ENISA, 2023). For Poland, a NATO frontline state bordering Ukraine and Belarus, these developments necessitate a comprehensive reassessment of national defense strategies. This paper explores Poland's technological and strategic responses to the war, analyzed through the lens of neorealist theory (Waltz, 1979).

[1] Department of Political Science, University of Management and Technology, Lahore – Pakistan

The recent conflict in Ukraine has provided a striking example of how descriptive technologies might revolutionize modern combat. The terrain of military operations has been drastically changed by these technologies, which include but are not limited to drone surveillance, satellite reconnaissance, and advanced data analysis. This change has had a major impact on the war's dynamics by enabling real-time intelligence gathering, greater target identification, and increased situational awareness. The use of these cutting-edge instruments has made war more complex, faster, and blurred the lines between what is considered to be the traditional battlefield. The ramifications of this technical advancement are very important for Poland. Poland's national protection is inextricably connected to the direction of the struggle because it's miles an immediate neighbor. the need for strong shielding talents, state-of-the-art intelligence collection, and the capacity to react speedy to converting threats has accelerated because of the growing usage of descriptive technologies. It has also emphasized the importance of statistics protection, cybersecurity, and the potential to thwart disinformation efforts. Poland now has to modify its countrywide security plans to the needs of a quick evolving geopolitical panorama and a technologically state-of-the-art international.

Neorealism as a Theoretical Framework

Neorealism, as articulated by Kenneth Waltz, posits that the anarchic nature of international politics compels states to pursue power and security through self-help mechanisms. Poland's security behavior in response to the Russia-Ukraine war aligns with this framework, as the nation prioritizes technological autonomy, deterrence, and alliance-building (Waltz, 1979).

Review of the Literature

- **Neorealism and International Security**

In step with neorealism, governments positioned strength and security first in chaotic global structures so that you can live on. in step with Kenneth Waltz's concept, structural boundaries—just like the allocation of talents amongst states—have a greater have an effect on conduct than internal variables. Neorealists contend that maintaining sovereignty calls for technological superiority, army might, and deterrent. The battle among Russia and Ukraine serves as an example of neorealism in motion, as Poland and different NATO international locations toughen their defenses in reaction to Russia's attempts to regain local manage. The conflict

validates neorealist presumptions through displaying how one nation's efforts to enhance protection (consisting of Ukraine's Western orientation) can lead to responses from other states (which include Russia's aggression). (Ministry of National Defence, 2023).

- **Technological Advancements in Modern Warfare**

With its capability to offer remote targeting, predictive analytics, and actual-time situational awareness, descriptive technology has completely modified fight. Documenting conflict crimes and exposing military moves have both benefited significantly from satellite tv for pc pix. Proactive reactions are made possible by way of AI-pushed systems that examine trends in fight advances and navy logistics. electronic struggle and cyber spying intrude with adversary communications and command structures. these trends clear up the fog of battle and provide events with extra technological prowess the strategic side (Maxar Technologies, 2022; Sentinel Hub, 2023). Those abilities have helped stage the gambling area in Ukraine against a Russian pressure this is numerically superior. This technological exchange highlights the necessity for Poland to make investments in similar skills that allows you to beat back aggression and guard its sovereignty. (ENISA, 2023)

- **Poland's Security Posture in the NATO Context**

Since 2014, Poland, a NATO member on the eastern border of the alliance, has dramatically raised its defense budget and modernized its armed forces. This trajectory was accelerated by the Russian invasion of Ukraine. Poland's military strategy places a strong emphasis on alliance interoperability, hybrid threat countermeasures, and territorial defense. Poland has hosted multinational combat groups, improved cyber resilience, and updated surveillance systems with NATO's assistance. (NATO, 2022). Descriptive technologies and OSINT are becoming more and more important in national security planning. However, there are still obstacles in the way of completely integrating these technologies into a coherent strategy framework. Poland's emphasis on alliance-building, deterrence, and self-help as logical reactions to a changing regional power structure is explained by neorealism.

Methodology

So as to investigate the consequences of descriptive technologies when it comes to the struggle between Russia and Ukraine and Poland's national security response, this observe uses a qualitative method that includes case studies and coverage

evaluation. The method, which makes a specialty of kingdom behavior and technology model in anarchic global systems, is based on interpretive analysis motivated with the aid of neorealist idea.

- **Qualitative Analysis (Case Studies, Policy Reports)**

The study makes use of recorded examples of technology use in the struggle between Russia and Ukraine, such as satellite tracking showing force concentrations and AI-powered analytics for missile concentrated on. Case studies of Poland's defense procurement choices, the introduction of its cyber coverage, and NATO joint physical games also are protected. Comparative analysis will display how Poland perceives and responds to nearby risks.

Data Sources (Government Reports, OSINT Platforms, NATO Documents)

- **Primary data sources include:**

- Polish Ministry of Defense white papers (Ministry of National Defence, 2023)
- NATO strategic documents (NATO, 2022)
- OSINT platforms (e.g., Bellingcat, 2022; Sentinel Hub, 2023)
- Cybersecurity reports from ENISA and CERT Polska (ENISA, 2023)

In line with neorealist notions of strength balance and hazard reduction, those records resources provide empirical aid for assessing the methods wherein descriptive generation and intelligence impact Poland's strategic selections.

Findings and Discussion

Satellite Intelligence (Maxar, SpaceX): Satellite statistics has been essential in confirming the effects of missile strikes, tracking convoy moves, and revealing Russian army buildups. The Ukrainian army changed into capable of make tactical decisions that had been aggressive with conventional intelligence thanks to near real-time geospatial awareness supplied by way of business organizations such as Maxar technologies and Starlink (SpaceX).

AI for Predictive Analytics: By examining beyond combat data, logistical styles, and communication alerts, machine gaining knowledge of algorithms were used to predict Russian offensives. by way of working with Western defense tech agencies,

Ukraine was capable of acquire predictive competencies that progressed the distribution of limited defense resources and enabled proactive civilian evacuations.

Poland's Takeaways: Poland has learned loads from Ukraine's technologically advanced defense. thru collaboration with the European space business enterprise (ESA), Warsaw is growing investments in satellite surveillance abilities and intends to improve the mixing of artificial intelligence (AI) into its protection systems. similarly, to presenting strategic deterrence, these technologies provide Poland intelligence collection autonomy, lowering its need on allies during important escalation periods.

In step with neorealist concept, Poland's emphasis on obtaining these technologies is a mirrored image of its desire for relative advantages and its understanding of the anarchic nature of world politics, wherein a kingdom's capacity to live on rests on its ability to protect itself militarily.

The warfare among Russia and Ukraine has introduced to light how open-supply intelligence (OSINT) can revolutionize contemporary battle. Intelligence accumulated from publically handy sources, or OSINT, has become a crucial device for each state and non-state actor. Russian troop movements, military logistics, and warfare crimes had been continuously found out by way of structures like Bellingcat, war Intelligence team, and mainstream media. according to neorealism, the full-size use of OSINT is indicative of a structural change in which governments goal to optimize their comparative benefit by means of utilizing all to be had approach to guarantee security and strategic vision.

NATO and associated agencies have used OSINT to follow Russian army motion near the Suwałki hole, a narrow land hall between Poland and Lithuania that is flanked with the aid of Russian ally Belarus. this is one of the maximum terrific examples of OSINT's usefulness. for the reason that it could function a chokepoint for NATO forces inside the case of Russian assault, the Suwałki hole is strategically giant. Russian deployments and logistic routes that would have generally stayed inside the purview of labeled intelligence have been determined with the aid of OSINT investigations the usage of satellite pix, TikTok videos, and Telegram chats. NATO quickly shared those effects and utilized them to create backup plans and run conflict video games in case of a Japanese front war of words.

Poland has acknowledged the strategic necessity of setting up its personal OSINT capabilities as a front-line NATO kingdom that borders Belarus and Ukraine. The Polish authorities has started out to growth the variety of cyber units in the internal security company (Agencja Bezpieczeństwa Wewnętrznego, ABW) and the armed forces. To reap and validate intelligence on cross-border military threats, those devices collaborate with partners inside the public and personal sectors, such as it corporations, academic establishments, and OSINT agencies. The Polish military' partnership with industrial satellite tv for pc companies to establish geospatial intelligence networks to perceive anomalous movement along its eastern border is one noteworthy initiative.

This strategy is an example of neorealist reasoning: Poland needs to construct self-sufficient talents to assure situational consciousness and short response in anarchic structures in which it can't completely rely on NATO partners for spark off assistance. (NATO, 2022). OSINT isn't simplest a helping tool; it's far an essential part of Poland's large protection strategy, which enables deterrence by using making opposed operations more apparent and, thus, riskier for enemies. (Bellingcat, 2022; Sentinel Hub, 2023)

However, the use of OSINT isn't without its difficulties. The unfold of false information is one great hassle. a good way to propagate false narratives, Russian operatives have weaponized social media and exploited open-supply platforms, producing noise which could crush analysts and skew situational reviews. as an instance, fake documents and motion pictures of army actions had been used to deceive NATO and polish choice-makers and incite fear. This demonstrates how tough actual-time verification may be, especially when adversaries are actively waging records struggle.

Furthermore, reliability isn't always continually similar to data velocity. OSINT makes it possible for statistics to unfold quickly, however delays in verification might lead to strategic mistakes. that allows you to make sure a extra correct operational photograph, the Polish Ministry of countrywide defense has replied via investing in information fusion structures that combine OSINT with human intelligence (HUMINT) and classified signals intelligence (SIGINT). these hybrid structures reduce reliance on anybody intelligence source and assist restrict the risks associated with misleading records.

Poland's increasing dependence on OSINT represents a reassessment of its strategic stance from a neorealist viewpoint. Poland is building a self-help mechanism based totally on independent statement and intelligence competencies in preference to waiting for allied confirmation or relying just on NATO command institutions. This evolution is steady with structural realism's awareness on power balance and state survival. Poland affords itself as an improved and proactive participant inside the worldwide device by using improving its potential to apprehend and examine Russian army movements on its very own.

All things considered, OSINT has grown to be an important issue of Poland's safety framework. Its strategic software in monitoring Russian threats, mainly inside the place of the Suwałki gap, illustrates the benefits and downsides of open-source strategies. Poland's ability to expand and institutionalize OSINT can be vital to maintaining national security and wearing out its responsibilities in the NATO alliance because the nature of conflict adjustments.

In what ways has Poland’s adoption of emerging defense technologies (e.g., drone warfare, electronic countermeasures, and NATO-backed cyber defenses) been accelerated by the Russia-Ukraine conflict, and what vulnerabilities remain?

The Russia-Ukraine war has acted as a strategic catalyst for Poland, pushing it to accelerate its military modernization with an emphasis on emerging defense technologies. This response is consistent with neorealism’s assertion that states act rationally to ensure their survival in an anarchic international system. Poland's strategic decisions are shaped by a recognition that power must be actively accumulated, especially when proximate threats like Russia exhibit revisionist behavior. The adoption of drone warfare, electronic countermeasures, and NATO-backed cyber defenses is not just a tactical response, but a structural imperative driven by the shifting balance of power in Eastern Europe.

- **Drone Warfare: Poland’s Strategic Leap**

Unmanned aerial vehicles, or UAVs, have come to be a key thing of conflict within the twenty-first century. Drones can function pressure multipliers, imparting low-fee, high-effect options for direct assaults, artillery recognizing, and reconnaissance, as proven through the Russia-Ukraine warfare. Poland can research from Ukraine's a hit use of Turkish Bayraktar TB2 drones to break Russian air defense structures and armored formations.

Poland has quickly taken movement to achieve comparable abilities in retaliation. Poland agreed to shop for 24 Turkish Bayraktar TB2 drones in 2021, prior to the full-scale invasion of Ukraine. those drones are presently being integrated into regular military devices and Poland's Territorial defense Forces. at the equal time, Poland is growing its personal drone zone, specifically with reference to WB Electronics' Warmate soaring guns. these devices can serve as disposable precision strike structures and provide independent target monitoring.

In line with neorealist principle, Poland's purchase of UAVs is a try and bridge capability gaps with Russia so one can make stronger deterrence and gain greater army autonomy. Drones are a scalable and asymmetric method to Russian numerical dominance in a risky location.

- **Electronic Warfare: Countering Russian GPS Spoofing and Communications**

Russian navy doctrine has been characterized by means of electronic war (EW), especially in Ukraine in which radio interference, GPS jamming, and spoofing had been significantly used. these techniques are searching for to impair situational consciousness, intrude with command-and-control structures, and reduce the efficiency of precision weapons provided with the aid of the West.

Poland has made the creation of counter-digital measures a pinnacle precedence considering the fact that it is properly aware of how inclined it is to such techniques. with the intention to shield drone operations, jam enemy alerts, and defend against cyber-physical attacks, the Polish military have commenced implementing electronic countermeasure devices. those consist of radar-based devices and mobile EW units which could pick out and forestall Russian interference tries.

those investments exhibit the neorealist reasoning for adjusting to the abilities of combatants. with the aid of making an investment in disruptive and defensive era, Poland hopes to maintain its own operational integrity and improve its deterrent posture because it receives geared up for the possible replication of Russian hybrid strategies on its territory.

- **Cyber Defenses: NATO Integration and Infrastructure Vulnerabilities**

Cybersecurity has turn out to be one of the maximum vital fronts inside the persevering with war between NATO and Russia. everything from electrical

infrastructure to authorities' websites has been the goal of hackers in Ukraine, causing vast disruption and confusion. these moves are low-price, debatable gentle struggle operations, the exact kind which could get beyond traditional army deterrents.

Poland has advanced its stance in phrases of cyber defense in collaboration with NATO. The Ministry of countrywide defense has shaped cyber instructions, and Estonia is a member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). purple-teaming physical games, threat intelligence change, and joint exercises have become not unusual components of Poland's cyber readiness program.

There are nonetheless weaknesses, despite the fact that, specifically in essential national infrastructure (CNI), which incorporates banking establishments, transportation networks, and strength structures. considering that a lot of these industries are still adjusting to NATO cybersecurity policies, nation and non-state actors may be capable of take gain of any vulnerabilities that could exist. furthermore, the floor region for viable cyber-attacks grows as Poland digitizes its army command systems.

Neorealism places this difficulty in angle: Poland is strengthening its digital borders as an herbal reaction to the ongoing chance posed by means of an competitive and technologically superior neighbor, not due to the fact it's miles idealistically aligned with Western beliefs. in addition to being a strategic requirement, the state's incorporation into NATO's cyber structure serves as a method of sharing defense charges even as retaining middle sovereignty.

Poland has demonstrated a clean strategic calculation based totally on neorealist principles via its fast deployment of recent protection technology, together with drones, digital warfare systems, and cyber competencies. The warfare between Russia and Ukraine has offered a strong motivation to innovate in addition to sensible evidence of new chance modalities. Poland has made sizable strides; however, the USA's safety scenario continues to be risky. digital war and cyber resilience gaps imply areas that need ongoing investment and strategic interest. Poland's technical modernization is a natural and important step toward maintaining its sovereignty in an international device driven by means of power politics and survival imperatives.

❖ **Neorealist Analysis – Poland's Security in an Anarchic System**

A powerful framework for comprehending how states negotiate a precarious worldwide order is furnished via the application of neorealism, also known as structural realism, to Poland's safety posture during the Russia-Ukraine war. Neorealists like Kenneth Waltz contend that states have to depend on self-help to live on in view that anarchy—the shortage of a government—defines the global device. in step with this paradigm, protection is a 0-sum sport. other states ought to react while one state seizes control or threat being strategically disadvantaged. Poland's logical moves in a device characterized by way of ongoing lack of confidence encompass growing its military, making an investment in descriptive technology, and strengthening its ties with NATO.

❖ **Self-Help and Poland's Military Expansion**

One of the clearest illustrations of Poland's neorealist posture is its decision to dramatically increase defense spending. In 2023, Poland raised its military budget to over 4% of GDP—one of the highest in NATO. This expansion includes the procurement of advanced weapons systems, including U.S.-made Abrams tanks, F-35 fighter jets, South Korean K2 tanks and K9 howitzers, and long-range HIMARS rocket systems. These acquisitions underscore a strategic imperative: to reduce dependence on allies and build sufficient military capability to deter or defend against Russian aggression autonomously if needed.

This move is an instance of a traditional balancing approach from a neorealist attitude. The moves of Russia in Georgia (2008), Crimea (2014), and Ukraine (2022) have led Poland to view Russia as a revisionist electricity that is prepared to redraw borders via armed force. Poland has a sturdy strategic way of life of prudence and readiness due to its near proximity and beyond experiences with both German and Russian invasions. States in anarchic structures invest in their very own survival rather than anticipating others to do so. Poland's army buildup is therefore a high example of putting a balance in response to perceived foreign threats.

❖ **Technology as a Tool of Relative Power**

Descriptive technologies—satellite reconnaissance, cyber intelligence, AI analytics, and electronic warfare systems—have become force multipliers in contemporary warfare. Neorealism posits that states seek relative power, and advanced technology is a decisive tool in altering power asymmetries. Poland's integration of emerging technologies is therefore not about achieving technological parity with global

powers like the U.S. or China, but about achieving regional superiority or, at minimum, credible deterrence against Russia.

Using AI-pushed analytics for real-time battlefield predictions in Ukraine has illustrated how era can modify the rate and best of decision-making. Poland has drawn clean instructions from this and is currently working with eu companions, consisting of the ecu area organisation (ESA), to broaden its personal satellite tv for pc and geospatial intelligence programs. in addition, the purchase and indigenous improvement of drones (e.g., Warmate loitering munitions) replicate efforts to advantage tactical and strategic blessings in a capability hybrid conflict situation.

Neorealism does now not inherently emphasize the technological dimensions of strength; but, inside the present-day context, technology becomes a way to build up abilities—the currency of security in an anarchic international. consequently, Poland's emphasis on excessive-tech defenses aligns with the common sense of maximizing relative advantage over a peer competitor.

- **NATO and the Limits of Collective Security**

Regardless of Poland's dedication to NATO, neorealism despite the fact that doubts alliances as lengthy-term commitments. in step with this paradigm, alliances are short-term, convenient unions which are vulnerable to modifications in the pursuits of the USA. Poland recognizes the capability for delayed reactions, conflicting dreams, or political department inside the alliance, despite NATO's Article 5's provision for collective protection—specially for the reason that sure Western ecu nations might be hesitant to provoke a navy warfare with Russia.

Poland's measures so demonstrate a two-pronged method: strengthening country wide abilities and furthering NATO integration. This encompass supporting NATO's jap flank army infrastructure, taking component in superior presence missions within the Baltics, and hosting main NATO physical games like Defender Europe. to be able to be able to act on its own inside the event that collective techniques fail, Poland is concurrently making an investment in home production strains, country wide cyber defense facilities, and intelligence structures.

This illustrates the neorealist attention that whilst community safety mechanisms reduce the want for self-assist, they do now not completely eliminate it. Poland have to keep its personal preparedness and resilience towards hybrid threats that would

no longer elicit a conventional NATO response, while NATO offers a framework for deterrence.

- **Hybrid Warfare and Future Threats**

The sizable use of hybrid war—a mixture of conventional navy pressure, cyberattacks, disinformation operations, monetary strain, and sabotage—has been one of the distinguishing characteristics of the conflict among Russia and Ukraine. elements of this have already passed off in Poland: tries to destabilize the Japanese border thru armed migration, cyber-attacks into government networks, and fake-flag media narratives meant to erode public confidence.

Technological agility and version are crucial on this placing. In response, Poland has expanded collaboration with NATO's Cyber speedy response groups, broadened cybersecurity collaborations between the private and non-private sectors, and simulated hybrid assault situations inside the banking, transportation, and strength sectors. although, there are nevertheless weaknesses in essential infrastructure, mainly in the telecommunications and electricity grid, wherein complete compatibility with NATO structures continues to be being labored out.

The hybrid hazard helps the idea that governments can't outsource their safety, in line with neorealist concept. in particular vulnerable to asymmetrical attacks are the cyber and information sectors, as a result Poland's defenses must constantly enhance to keep up with Russian abilities.

Conclusion and Recommendations

Poland has reexamined its national security doctrine in mild of the Russia-Ukraine conflict, which has been both a strategic shock and an enlightening revel in. this is mainly genuine when considering new technology and alliance dynamics. according to neorealist concept, Poland's safety features, which range from cyber resilience to army modernization, are encouraged by using the structural realities of anarchic global law, in which states need to put survival, autonomy, and power first, in place of by ideological affinities or institutional idealism.

Three principal areas were examined in this examine: how Poland's strategic mastering and the warfare had been inspired by descriptive technology; how OSINT and real-time records accumulating advanced countrywide readiness; and how the

nearby security disaster sparked the deployment of latest military technologies. the main conclusion is unmistakable: Poland is performing in a neorealist manner by means of increasing its abilties, decreasing its reliance on different countries, and being ready for ongoing instability on NATO's eastern border.

- **Strategic Implications for Poland**

In the warfare in Ukraine, the software of sophisticated descriptive technology—which include satellite tv for pc photography, cyber tracking, and AI-pushed analytics—has confirmed crucial. information dominance is becoming just as essential as kinetic pressure, as visible by using Ukraine's capability to use each navy and commercial technology to reveal, are expecting, and counter Russian offensives.

Those lessons were grasped via Poland. It makes a legitimate try to trap as much as its enemies in phrases of era via boosting its spending in area-based surveillance, domestic drone production, and AI-pushed chance analytics. Poland's structural necessity to increase independence and reduce its susceptibility to technological imbalances that Russia may want to take advantage of is meditated in these developments.

Moreover, traditional intelligence frameworks have modified because of OSINT and real-time facts gathering. Poland and NATO allies can now watch Russian troop actions with extraordinary element due to the fact to open-source software, commercial satellite tv for pc records, and social media verification. Crowd-sourced, transparent records have been delivered to standard intelligence by way of corporations consisting of Bellingcat and industrial intelligence offerings. In reaction, Poland has increased the size of its OSINT and cyber divisions; but, problems with information verification and resistance to misinformation nevertheless exist.

Poland is getting equipped for a multifaceted conflict surroundings that consists of kinetic, cyber, and facts warfare, as visible via the acceleration of emerging defense generation, including drones, jammer gadgets, and cyber protection systems. however, there are still weaknesses, particularly inside the regions of key infrastructure, home protection production, and political resistance to hybrid threats.

❖ **Neorealist Takeaways**

From a neorealist perspective, Poland's strategic behavior aligns with the central pillars of structural realism:

- Self-help remains fundamental. Poland is taking steps to strengthen its very own deterrent capability in spite of NATO assurances, acknowledging that alliances can put off but no longer get rid of threats.
- Relative power matters. Poland's investments are supposed to obtain nearby strategic sufficiency with regards to Russia, no longer to reap parity with the world's superpowers.
- Technological capability is now integral to national power. Controlling the statistics, communications, and technological realms is simply as important in cutting-edge battle as having tanks and airplanes.
- The international system remains anarchic and uncertain. Poland needs to get equipped for gray-area conflict, hybrid threats, and evolving alliance priorities that would in no way call for classic struggle responses.

Policy Recommendations

To secure its sovereignty and bolster its position in a volatile region, Poland must adopt the following policy measures:

❖ **Develop Domestic Defense Technology Ecosystems**

Poland ought to hold investing in its very own defense industry to lessen its reliance on foreign navy generation. This includes:

- Growing home drone tasks, including the Warmate collection.
- Setting up country wide AI-protection research institutes with an emphasis on self-reliant structures, logistical forecasting, and battlefield analytics.
- The use of streamlined procurement and subsidies to encourage non-public-public collaborations in protection studies and improvement.
- Poland's impact in principal and eastern Europe grows because of this, which also improves self-sufficiency and lets in Poland to export protecting competencies.

❖ **Fortify Against Hybrid Threats**

One of the maximum forthcomings and realistic threats to Poland is hybrid battle, which mixes political manipulation, cyberattacks, sabotage, and disinformation. Thus, Poland must:

- Expand cybersecurity cooperation with NATO and EU's cyber command initiatives.
- Establish an interagency hybrid threat response unit that includes intelligence, defense, infrastructure, and civil society actors.
- Invest in election security and media literacy programs to defend against external manipulation of public opinion.
- Resilience in the face of hybrid threats will be a critical component of strategic stability.

❖ **Institutionalize NATO-EU Tech-Sharing for Eastern Flank Defense**

Poland should play a leading role in pushing for NATO-EU defense tech integration, especially on the Eastern Flank. Priorities should include:

- Joint procurement and interoperability of reconnaissance drones and satellite systems.
- Real-time OSINT and SIGINT data fusion centers focused on Russia and Belarus.
- Coordinated exercises involving electronic warfare and disinformation response.
- Such cooperation enhances collective deterrence and reduces the asymmetries between Western and Eastern NATO members.

❖ **Expand Resilient Infrastructure Capabilities**

Poland has to very well take a look at how vulnerable its essential country wide infrastructure (CNI) is to kinetic, cyber, and EMP attacks. Future investments should include:

- Hardened energy grids with redundancy systems.
- Protected military command and control facilities.
- Cross-border infrastructure projects with NATO allies that serve dual-use civilian and military logistics.

- The foundation of both public stability and military persistence in instances of disaster is resilient infrastructure.

Similarly, to being a local conflict, the Russia-Ukraine warfare serves as an example of the way alliances, era, and hybrid threats are reshaping traditional ideas of power and sovereignty. The stakes are existential for Poland, that's located on the NATO border. Its acts are justified, vital, and protective from a neorealist attitude. Poland's safety method must stay bendy, technologically superior, and structurally unbiased in a world wherein the international order is precarious and enemies are still emboldened.

Poland's security calculations have also been influenced by the increasing reliance on real-time intelligence and OSINT platforms, which have been brought to light by the efforts of groups like Bellingcat and NATO's intelligence-sharing programs. Disinformation tactics and troop movements close to Poland's borders have been exposed thanks in large part to OSINT. Poland has responded by increasing the size of its cyber teams and working with both public and commercial entities to improve situational awareness. The proliferation of open data, however, presents additional hazards, especially with regard to false information and the accuracy of intelligence, which emphasizes the necessity of strong verification procedures.

Finally, Poland's protection improvement has been expedited via the conflict, specially within the areas of cyber defenses, digital countermeasures, and drone warfare. collectively with NATO-aligned cyber capabilities, the purchase of structures which include the Turkish Bayraktar TB2 and the introduction of indigenous systems together with the Warmate show the urgent want to fill capability gaps. however, troubles nonetheless exist: Poland nonetheless depends in large part on overseas defense technologies, and its critical infrastructure continues to be liable to hybrid and cyberattacks.

Those traits are defined by neorealism. Poland's actions are inspired by a realistic evaluation of material energy, national hobby, and the constraints of anarchic structures instead of by way of an idealistic self-belief in norms or institutions. Poland still has a fundamental need for unbiased navy readiness even as NATO gives a framework for collective protection. with a view to counterbalance Russian electricity, Poland has boosted its defense budget (aiming for 4% of GDP), accelerated its navy, and invested in generation.

Thus, Poland needed to re-evaluate its vulnerabilities and adopt a more proactive, technologically integrated protective posture due to the manner that descriptive technologies have changed the nature of the conflict between Russia and Ukraine. consistent with the file, Poland's direction is an example of a neorealist technique to systemic lack of confidence: growth capability, reduce reliance, and get equipped for escalation in continuously unstable surroundings. There are still strategic weaknesses, although, in particular in the regions of cybersecurity, protective important infrastructure, and growing home defenses. Resolving those can be essential for the stableness of NATO's jap flank in addition to for Poland's national security

References

Bellingcat. (2022). OSINT tracking of Russian military operations. Retrieved from https://www.bellingcat.com

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

Maxar Technologies. (2022). Satellite imagery for Ukraine conflict. Retrieved from https://www.maxar.com

Ministry of National Defence, Poland. (2023). National Security Strategy. Warsaw: Government of Poland.

NATO. (2022). Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization. Retrieved from https://www.nato.int

Schwarzer, R., & Jerusalem, M. (1995). Generalized Self-Efficacy Scale. In Weinman, Wright & Johnston (Eds.), Measures in health psychology.

Sentinel Hub. (2023). Satellite Tracking Data. Retrieved from https://www.sentinel-hub.com

Waltz, K. (1979). Theory of International Politics. McGraw-Hill.

Article Information:

Received	*26-Feb-2025*
Revised	2-May-2025
Accepted	22-May-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:

Javeria Nazir

Javerianazir2@gmail.com