Assessment of threats to Ukraine's national security through the prism of the Kingdom of the Netherlands' experience

Ivan Tkach [1 A]; Yana Martynenko [2 B]; Andrii Zdorovylo [3 B]; Tetiana Cherneha [4 B]

[1] Dr. Sc., Full Professor, e-mail: tim68@ukr.net, ORCID: https://orcid.org/0000-0001-5547-6303
[2] e-mail: martunenko05199662@gmail.com
[3] e-mail: andmaister88@gmail.com
[4] recipient, e-mail: chtetiana888@gmail.com, ORCID: https://orcid.org/0009-0000-5534-6664

[A] National Defence University of Ukraine, Ukraine
[B] Ministry of Defence of Ukraine, Ukraine

Received: February 21, 2025 | Revised: March 01, 2025 | Accepted: March 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.1.2

Abstract

The current state of threats to Ukraine's national security has been analyzed through the lens of the experience of the Kingdom of the Netherlands. Common and distinct aspects of hybrid threats have been studied, including cybercrime, disinformation, and espionage. An analysis of key provisions of national and international approaches to protecting critical infrastructure and the information space has been conducted. Conclusions have been drawn regarding the feasibility of adapting effective practices from the Netherlands to the realities of Ukraine.

Key words: national security, hybrid threats, cyber defense, disinformation, critical infrastructure, Ukraine, Netherlands.

Introduction

Modern global security challenges, especially in the context of Russia's military aggression against Ukraine, demonstrate the need for a deep analysis of threats to national security and the development of effective counter-strategies. The Russian Federation employs a wide range of methods, including military actions, cyberattacks, disinformation, and economic pressure, posing a threat not only to Ukraine's security but also to the stability of Europe.

One example of effective security risk management is the Kingdom of the Netherlands, which has a developed system for protecting against hybrid threats. This country has faced cyber threats, information attacks, and espionage multiple times, particularly from Russia and China. In this context, the experience of the Netherlands could be valuable in strengthening Ukraine's national security system.

Ukraine's national security remains under constant threat from aggressive actions by the Russian Federation. Since 2014, Ukraine has faced not only direct military attacks, but also numerous cyber operations aimed at undermining its infrastructure and destabilizing society. These challenges are compounded by information attacks, economic blackmail through energy dependence, and attempts by Russia to sow division in international support for Ukraine.

Despite its geographical distance from the conflict region, the Netherlands also feels the impact of Russian threats. Hybrid aggression, which includes espionage, disinformation, and sabotage of critical infrastructure, poses significant risks to the country's stability. The challenge lies in identifying common threats for both Ukraine and the Netherlands and adapting effective approaches from the latter to the realities of Ukraine.

Result and Discussion

1. Threats to Ukraine's National Security

Ukraine's national security has been under constant pressure from the Russian Federation in recent years. The hybrid methods of influence actively used against Ukraine include cybercrime, disinformation, economic blackmail, and military aggression. These threats are complex in nature and affect various areas of national security.

Cyberattacks on Critical Infrastructure: Russian cyberattacks are one of the main challenges for Ukraine. They aim to undermine the functioning of the energy, transportation, and communication infrastructure. Since 2015, Ukraine has experienced a series of large-scale attacks on energy networks, resulting in power outages for hundreds of thousands of citizens. Attacks such as the BlackEnergy operation demonstrate Russia's ability to use cyber weapons to achieve its geopolitical goals. The use of wiper malware, targeted at destroying data and creating chaos in government and the economy, is particularly concerning.

Disinformation and Information Warfare: Russia actively conducts an information war against Ukraine, focusing its efforts on discrediting the Ukrainian government, spreading fake news, and creating social division. Disinformation campaigns have several directions:

- Influencing internal stability by creating tensions between regions and social groups;
- Discrediting Ukraine on the international stage to reduce the level of support from partners;
- Using social media to spread propaganda, fake news, and sow distrust in state institutions.

Energy Blackmail: Ukraine's energy dependence on Russian gas has become one of the tools for political pressure. Russia has repeatedly reduced gas supplies or raised prices, creating economic challenges and undermining the stability of the state. The energy crisis caused by supply restrictions had not only economic but also social consequences, which Russia has used to strengthen its influence.

2. Threats to the National Security of the Netherlands

Despite the absence of direct military conflict, the Netherlands also faces numerous threats, many of which are similar to those encountered by Ukraine. Although the scale of these threats is smaller, they pose serious challenges to the democratic rule of law, economic security, and critical infrastructure.

Espionage and Sabotage: Russian intelligence services are actively operating in the Netherlands, using diplomatic missions as a cover to gather information about NATO, the EU, and international organizations such as the Organization for the Prohibition of Chemical Weapons. The AIVD report for 2024 emphasizes that Russian espionage activities target the political, economic, and military spheres, as well as scientific developments.

Cyber Threats: The Netherlands is an important digital hub in Europe, making it an attractive target for cybercriminals. Russian hackers frequently attack government institutions, private companies, and international organizations located in the country. Cyberattacks aimed not only at information theft but also at undermining trust in state institutions.

Sabotage of Critical Infrastructure: The Netherlands also faces risks of physical sabotage, particularly concerning wind power plants, underwater cables, and gas pipelines. These facilities are strategically important for the country's energy security, and their vulnerability to attacks increases the risks of destabilization.

3. The Netherlands' Experience in Countering Hybrid Threats

The Netherlands demonstrates an effective approach to countering hybrid threats, particularly through the work of AIVD and MIVD. The country actively invests in cybersecurity, the development of monitoring technologies, and international cooperation.

Cybersecurity: The Netherlands has established the National Cyber Security Centre (NCSC), which ensures monitoring and coordination of measures against cyber threats. This approach has significantly reduced the number of successful attacks on government systems and improved the level of cybersecurity in the private sector.

Countering Disinformation: The Dutch government conducts an active information campaign aimed at increasing the media literacy of the population. Engaging media, social platforms, and non-governmental organizations allows for effective combat against the spread of fake news.

International Cooperation: Close collaboration with NATO and the EU helps the Netherlands access cutting-edge technologies and intelligence data, as well as participate in joint exercises and training.

4. Recommendations for Ukraine Based on the Experience of the Netherlands

Ukraine can significantly strengthen its national security system by adapting the practices of the Netherlands. Specifically:

- **Development of Cyber Defense**: Establishing a national cybersecurity center based on the NCSC model will enhance monitoring and operational response to cyber threats.
- **Countering Disinformation**: Implementing educational campaigns on media literacy and collaborating with international partners will help reduce the impact of information warfare.

International Cooperation: Expanding Ukraine's participation in NATO programs, particularly in the context of implementing the provisions of the 2022 Strategic Concept, will contribute to strengthening the national security and defense capability of the country.

Conclusions

The analysis of threats to Ukraine's national security through the experience of the Kingdom of the Netherlands demonstrates that hybrid threats have become a major challenge in the modern world, especially in the context of the escalation of military conflict in Ukraine. These threats are multifaceted, encompassing cybercrime, disinformation, sabotage of critical infrastructure, economic pressure, and espionage.

For Ukraine, the threats from Russia are unprecedented in scale and intensity. Cyberattacks on energy infrastructure, the spread of propaganda, and attempts to undermine trust in Ukrainian state institutions are aimed at reducing the country's defense capability and its political stability. Simultaneously, the Netherlands, despite the absence of direct military conflict, also faces similar challenges that undermine its democratic system and economic security.

The experience of the Netherlands in countering hybrid threats is highly relevant for Ukraine. Effective measures, such as the establishment of the NCSC, fighting disinformation through educational and informational campaigns, and close cooperation with international partners, demonstrate the possibility of reducing the impact of hybrid threats even in difficult conditions. At the same time, Ukraine should take into account the specifics of its own situation, particularly the high level of military threat and direct conflict with Russia.

Ukraine can and should utilize the experience of the Netherlands to develop its national security strategy. This includes:

- Improving the cyber defense system by expanding monitoring and response infrastructure for cyber threats;
- Integrating educational programs to enhance media literacy and counter propaganda;
- Strengthening cooperation with international organizations, such as NATO and the EU, to gain access to modern technologies and information sharing.

Thus, a comprehensive approach to developing a national security system, based on the adaptation of successful practices from the Netherlands, can significantly enhance Ukraine's

defense capability, increase its resilience to hybrid threats, and ensure long-term stability.

Prospects for Further Research

Despite the substantial analysis conducted, this topic remains multifaceted and requires further exploration. Future research should focus on the following directions:

- Developing practical solutions in the field of cybersecurity. In-depth studies are needed to create integrated monitoring and response platforms for cyber threats, drawing on the best practices of the Netherlands;
- Researching the impact of information warfare on public opinion. Understanding the mechanisms of disinformation spread and developing methods for its neutralization are critically important for enhancing the resilience of Ukrainian society against information attacks;
- Analyzing energy security in the context of the conflict. Special emphasis should be placed on strategies for diversifying energy supplies and reducing dependence on Russian energy resources;
- International cooperation in the field of security. Further research may examine the mechanisms of Ukraine's integration into NATO's collective security system and assess the impact of this integration on national security;
- Socio-economic aspects of hybrid threats. Researching the economic impact of cyberattacks, energy blackmail, and disinformation will help evaluate the real scale of challenges and develop effective tools to address them;
- Modeling potential scenarios for the development of hybrid threats. This will not only allow anticipating potential challenges but also facilitate the early development of response mechanisms.

Success in countering hybrid threats largely depends on the depth of understanding of their nature and an interdisciplinary approach to addressing these issues. Further research should serve as the foundation for developing a national security strategy that is resilient to the challenges of the modern world.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

AIVD Annual Plan Letter 2025 Available from : https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024Z21726&did=2024D51230.

24/2 – The Russian attack on Ukraine: a turning point in history від 17.03.2023. Available from : https://english.aivd.nl/publications/publications/2023/03/17/24-2---the-russian-attack-on-ukraine-a-turning-point-in-history.

Plan AIVD on 2025 рік. Available from : https://www.aivd.nl/actueel/nieuws/2024/12/19/aivd-2025-wordt-een-onrustig-jaar.

Military and Hybrid Threat Assessment 2024. Available from : https://www.rijksoverheid.nl/documenten/rapporten/2024/12/06/tk-bijlage-1-dreigingsbeeld-hybride-en-militaire-dreigingen-na-cdinev.

NATO Strategic Concept 2022: Collective Defence and Emerging Threats. Available from : https://www.nato.int/cps/uk/natohq/topics_210907.htm?selectedLocale=en.