

Julian Maj

gen. dyw. prof.dr hab., Rector

WSHIU Academy of Applied Sciences

ORCID: <https://orcid.org/0009-0007-5517-0217>

Magdalena Gorska

Founder

WSHIU Academy of Applied Sciences

ORCID: <https://orcid.org/0000-0002-5208-1637>

Paulina Kolisnichenko

PhD in Economics, Vice Rector for International Cooperation

WSHIU Academy of Applied Sciences

ORCID: <https://orcid.org/0000-0001-6730-1236>

DOI: <https://doi.org/10.30525/978-9934-26-634-8-4>

RETHINKING NATIONAL SECURITY IN EU COUNTRIES AGAINST THE BACKDROP OF A FULL-SCALE ARMED INVASION OF UKRAINE

Summary

The paper reveals the rethinking of national security in the European Union states against the backdrop of the full-scale armed invasion of Ukraine by the Russian Federation after February 2022. It is shown that the war caused a change in the basic ideas about risks in Europe and returned the threat of large-scale interstate aggression to the center of the agenda, which, in turn, increased attention to deterrence, defense readiness, military mobility, and defense-industrial capacity. It is substantiated that national security in the European space is complex and encompasses not only military instruments, but also energy security, cyber defense, countering hybrid threats, protecting critical infrastructure, economic sustainability, and the ability of institutions to ensure the continuity of key state functions. The peculiarities of multi-level governance, where the national responsibility of states is combined with common rules, standards and coordination mechanisms, which are of crucial importance due to the transborder nature of modern threats, are emphasized. The paper emphasizes the interconnectedness of defense decisions with energy policy, sanctions regimes, financial stability and information stability of society. It is summarized that the effectiveness of the new security model depends on the combination of defense capabilities with the stability of society, trust in institutions and the ability to withstand prolonged crises without losing unity and manageability.

Introduction

The full-scale armed invasion of Ukraine by the Russian Federation after February 2022 was a turning point for security perceptions in the European Union countries, as it brought war back as a reality to the European continent and shattered the assumption that large-scale interstate aggression was unlikely. In response, the European Union countries began to rethink national security as a holistic policy, where defense, societal resilience, energy, cybersecurity, and economic dependencies are combined into a single system of risks. Symbolically, as early as March 2022, European Union leaders in Versailles noted the need to strengthen defense capabilities and reduce dependencies, primarily energy ones, and in the same month the Strategic Compass on Security and Defense was adopted, which was an attempt to transform the new reality into concrete political actions. The defence re-thinking block has not only touched on the volume of funding, but also on the very logic of readiness, interoperability and industrial capacity. The war has shown that national security depends on the availability of stocks, the speed of production, the ability to repair and replenish equipment, as well as on coordinated procurement that reduces fragmentation and competition between states. This is why instruments have emerged at the European Union level to accelerate the production of ammunition and stimulate joint procurement, in particular the regulation on support for the production of ammunition and the instrument for strengthening the European defence industry through joint procurement.

In parallel, in 2024, the European Commission presented the European Defence Industrial Strategy and proposed a European Union programme for the defence industry as a bridge from short-term emergency solutions to a longer horizon of industrial readiness. As a result, the security debate has become less abstract, shifting to issues of joint planning, capacity sharing and supply chain resilience. Until 2022, energy risks were often seen as an economic issue, but the war has made it clear that dependence on fossil fuel imports from an aggressor state creates vulnerability to pressure, blackmail and the budgetary fueling of war. That is why the European Commission presented a plan in May 2022 to rapidly reduce dependence on Russian fossil fuels and accelerate the transition to clean energy, and the European Union's governing institutions have set a goal of ending such dependence through energy savings, diversification of supplies and acceleration of the transition. In the national strategies of the European Union states, this has manifested itself as a change in priorities, from protecting prices and market stability to the broader task of ensuring continuity of supply, modernizing networks, increasing efficiency and the physical security of energy facilities.

The full-scale war accelerated the convergence of national security priorities of the European Union countries with the broader architecture of collective defense, and at the same time consolidated the practice of long-term support

for Ukraine as a component of European security. An important event was the accession of Finland on April 4, 2023 and Sweden on March 7, 2024 to the North Atlantic Alliance, which showed how risk assessments in Northern Europe have changed dramatically. At the level of the European Union, one of the instruments was the European Peace Support Facility, through which 6.1 billion euros were mobilized in 2022–2024 to meet the urgent military and defense needs of Ukraine, and according to the analytical materials of the European Parliament, as of April 2025, the European Union and its states had mobilized significant amounts of financial, military and humanitarian support. As a result, national security in the European Union countries began to be interpreted more broadly as the ability of the state and society to withstand prolonged crises, maintain control, maintain defense capabilities, protect critical systems, and reduce strategic dependencies that can be converted into weapons.

Chapter 1. The essence and features of national security in EU countries

National security is a state of security for the state, society and each individual, in which a country is able to maintain its sovereignty, territorial integrity, constitutional order and basic freedoms, as well as maintain the normal functioning of its economy and institutions even when it is under pressure from external or internal threats. It is not only about the army and borders. National security includes political stability, the ability of authorities to make decisions without blackmail and interference, the stability of democratic procedures, the protection of human rights, the security of critical infrastructure, energy reliability, cyber security, combating organized crime, as well as preparedness for emergencies such as large-scale man-made accidents, epidemics or natural disasters. It also covers the information space, because manipulation, disinformation and undermining trust in institutions can achieve the same effect as direct pressure by force, only by other methods. In practical terms, national security means that people can live, study, work, use transportation, healthcare, banking, and communications without the constant risk of system shutdown, panic, or chaos. It is the ability of a state to prevent threats, detect them in time, contain them, mitigate the damage, and recover from them, while maintaining the rule of law and the balance between security and freedom. The importance of national security for the countries of the European Union is particularly growing due to the deep interdependence created by the common market, freedom of movement, integrated supply chains, transnational financial links and shared technological and energy systems. What may appear to be a local problem in one country quickly becomes a common challenge within the Union. If a major port, energy hub, transport corridor or network operators are disrupted, this affects production, logistics, prices, employment and stability in many countries at once. The free

movement of people and goods offers enormous benefits, but at the same time it increases the requirements for coordination in matters of border protection, control of the risks of terrorism, smuggling, human trafficking and illegal trafficking of weapons or drugs. In addition, the countries of the European Union have open economies that depend on foreign trade and the import of resources, so economic shocks, energy crises and attempts at economic pressure can quickly affect public sentiment, budgetary capabilities and political stability. In such a system, national security is no longer just an internal matter of each state, it becomes a condition for the normal functioning of the entire community, so it is beneficial for countries to coordinate approaches, exchange information, conduct joint exercises, strengthen the protection of critical infrastructure, and form mechanisms for mutual assistance. Another reason why national security is critically important for the countries of the European Union is the emergence of hybrid threats, which often do not take the form of traditional warfare, but are capable of destroying states from within. Such threats can combine cyberattacks on banks, hospitals or energy networks, disinformation campaigns, bribery or blackmail of officials, interference in elections, the creation of artificial social conflicts, the use of migration flows as a tool of pressure, sabotage of infrastructure, economic restrictions and targeted violence through proxy groups. The problem is that the response to such methods is more complex than to a direct military attack, because it is necessary to act simultaneously in the legal, diplomatic, financial, technological and information spheres, without destroying its own democratic principles. National security here means the ability of the state not only to punish the guilty, but also to build sustainable institutions that make it impossible for private interests or external influence to seize state decisions. It is also important that in the countries of the European Union, security is directly related to the trust of citizens. When people believe that the state is in control, communicates risks honestly, protects critical systems, and acts within the law, then society is better able to withstand crises, is less susceptible to panic and manipulation, and radical forces are less likely to use fear to undermine democracy. Therefore, national security in the European context is also about societal resilience, media literacy, quality education, independent courts, transparent procedures, and accountability of government. Investment, innovation, scientific programs, industrial modernization, energy transition and digital transformation require predictability, and predictability is born from security. Companies do not build factories and research centers where there is a risk of sudden power outages, logistics blockages, uncontrolled cyberattacks or political destabilization. The state cannot effectively finance education, healthcare and social programs if it is forced to constantly patch up the consequences of crises that could have been prevented. For citizens, security is manifested in simple things, in the stable operation of public services, in the

availability of medical care, in the protection of personal data, in the ability to express oneself freely without fear of violence, in the confidence that the rules are the same for everyone. For the countries of the European Union, national security also strengthens their international subjectivity, because it allows them to protect their own interests and values, support partners, respond to crises near their borders, ensure the safety of sea routes and the stability of trade. In the end, national security is not only about preventing the worst, it is about creating conditions in which a country is able to live a normal life, develop and maintain freedom, and for the countries of the European Union it is also about preserving a common space of trust, cooperation and prosperity, which works only when each link is stable.

National security in the European Union is a comprehensive policy of protecting the state and society from threats that can violate sovereignty, territorial integrity, constitutional order, public order, human rights and freedoms, as well as the stable functioning of critical systems. In theoretical terms, national security is not limited to military defense, although the defense component remains its core. It includes political stability, economic capacity, energy reliability, cyber defense, information security, protection of critical infrastructure, the ability to respond to emergencies and maintain social cohesion during a crisis [1-2]. It is because of this multidimensionality that security is increasingly described as the ability of the state and society to withstand pressure, adapt to change and recover from shocks, while maintaining the manageability and legitimacy of institutions. The peculiarity of national security in the European Union is that it is formed simultaneously at two levels, national and supranational [3-5]. On the one hand, each state retains the sovereign right to determine its own interests, threats, defense priorities and the organization of the security sector. This is directly reflected in the founding treaties, in particular in the provision that national security remains the responsibility of each state separately. On the other hand, the very nature of risks in Europe is cross-border, and therefore national security strategies are practically impossible without coordination, common rules and mechanisms of mutual assistance. States are connected by a common market, common transport and energy networks, interdependence of supply chains, as well as a pan-European information space, where threats spread quickly, and the consequences almost always go beyond the borders of one country.

In security theory itself, an approach is often used according to which threats are grouped according to the main aspects, the military aspect, the political aspect, the economic aspect, the societal aspect and the technological aspect, including cyberspace. For the states of the European Union, this approach is particularly relevant, as it allows us to explain why even without a direct military attack, a country can be in a state of danger, for example, due to sabotage of critical infrastructure, large-scale cyberattack, manipulation of the

information field, disruption of energy supplies, or due to external pressure on strategic enterprises. At the same time, modern theoretical understanding emphasizes that threats are rarely “pure”. They are intertwined. A cyber incident can create economic damage and social panic. An energy shock can affect political stability. Information operations can push towards radicalization and violence. That is why states are increasingly moving from a sectoral logic, where each body is responsible only for its narrow direction, to a comprehensive logic of risk management, where interagency interaction, data exchange, joint scenario plans and uniform response standards become important (Table 1).

National security for a European Union country is the ability of the state, as well as its institutions and society, to maintain sovereignty, territorial integrity, constitutional order and the security of its citizens, even when under pressure from external adversaries, internal crises or technological risks. It encompasses not only the army and borders, but also the work of the police and intelligence services, the protection of critical infrastructure, energy and food security, economic stability, health care, information hygiene, the ability of the state to make decisions quickly in times of crisis and maintain trust in society. An important nuance in the European Union is that national security legally remains primarily the responsibility of each state, the treaties explicitly state that national security is the sole responsibility of the member state. At the same time, countries are so interconnected by the common market, common supply chains, mobility of people, data exchange, financial systems and energy networks that the security of one country actually depends on the stability of others. That is why in the European Union, national security is practically becoming multi-layered. At the national level, it is the constitutional powers of the state and its resources, and at the European Union level, it is agreed rules, common response mechanisms and common tools that strengthen resilience, reduce vulnerabilities and stitch different policies into a single logic. The defence component of national security in the European Union has intensified dramatically in recent years, as war in Europe has once again become a reality, and risk scenarios have expanded from the classic threat of armed aggression to long-range strikes, massive drones, sabotage, maritime incidents and pressure on the defence industry. European Union law provides for a mutual obligation of assistance: if a Member State is the victim of armed aggression on its territory, other States must provide assistance and support by all available means, while emphasizing coherence with obligations within the North Atlantic Alliance. There is also a solidarity logic in responding to terrorist attacks and major disasters, which allows for joint action and the mobilisation of European Union instruments at the request of the affected State.

Table 1

The concept of national security of EU countries

Conceptual dimension	What it means in EU Member States, with emphasis on modern security conditions
National security as a comprehensive state-and-society capacity	In EU countries, national security is increasingly defined as the ability of the state and society to prevent, withstand, and recover from disruptions that threaten sovereignty, constitutional order, territorial integrity, public safety, and the continuity of vital services. This meaning goes beyond military defence and includes resilience of institutions, crisis management, civil protection, and the capability to keep critical systems functioning even under sustained pressure. The benchmark is not “no threats,” but “maintained governability and rapid recovery.”
Multi-level governance combining national responsibility with EU frameworks	Member States retain primary responsibility for national security, yet the practical toolkit is shaped by EU-wide rules and coordination in areas where risks cross borders. This includes common standards for cybersecurity, protection of critical entities, sanctions implementation, and shared situational awareness. The EU level often acts as a force multiplier by harmonising requirements, funding capacity building, and enabling coordinated responses when national measures alone are insufficient due to interconnected markets, networks, and infrastructure
Security as risk management across interdependent sectors	Modern threats are rarely isolated. A cyberattack can cause physical disruption, financial losses, and public panic, while energy shocks can trigger social instability and affect defence readiness. Therefore, EU national security strategies increasingly use a risk management logic that connects defence, energy, economy, transport, health, digital services, and information integrity. The focus is on identifying systemic vulnerabilities, reducing strategic dependencies, building redundancy, and planning continuity so that cascading failures are less likely
Legitimacy, rule of law, and societal cohesion as security resources	EU countries treat legality, public trust, and social cohesion as elements of security, not merely political values. In hybrid conflict conditions, adversaries exploit polarisation, disinformation, and distrust to weaken governance without crossing the threshold of open war. As a result, national security includes protecting democratic processes, ensuring credible public communication, safeguarding rights while responding to threats, and maintaining social solidarity during long crises, because internal fragmentation directly reduces national and collective security effectiveness

Source: formed by the authors

In practice, this is complemented by policy documents and capability development plans, including the Strategic Compass, approved by the Council of the European Union on 21 March 2022 as an action plan to strengthen security and defence by 2030, and the idea of a rapid deployment of a modular force of up to 5,000 troops for crisis situations. In parallel, the European Union is trying to strengthen the defence industrial base through financing and joint procurement. In 2025, additional instruments appeared, including the European

Defence Industrial Programme until 2027, as well as joint lending mechanisms for defence procurement at Union level, which shows the transition from declarations to industrial mobilisation, where production, standardisation and logistics become no less important than the number of units.

The European Union states are characterized by a combination of the traditional approach to security, based on deterrence, defense capabilities and allied guarantees, with a newer approach that emphasizes resilience and continuity of vital functions. Resilience in this context means the ability of a state to ensure the operation of key systems, such as energy supply, communications, transport, water, health care, financial services, even when there is a deliberate attack or a large-scale accident [6-7]. This logic is well consistent with European policies in the field of cybersecurity and the protection of critical entities, where risk management, mandatory continuity planning, preparedness for incidents and recovery from them are key. This leads to an important theoretical conclusion: in modern Europe, national security is increasingly described not as a «state of absence of threats», but as «the ability of the state and society to act under the pressure of threats».

An important element of the European specificity is also the fact that national security in the Member States develops in an environment of institutional solidarity. Solidarity here is not only a political principle, but also a legally enshrined logic of interaction in crises. At the legal level, there is a mechanism of mutual assistance in the event of armed aggression against a Member State, which is enshrined in the provision on mutual assistance within the framework of the Common Security and Defense Policy. A separate solidarity mechanism has been established in the event of a terrorist attack or a natural or man-made disaster, which provides for joint actions by the Union and the Member States. In a theoretical sense, these norms are important because they demonstrate that security in Europe is being built as a shared responsibility, where national institutions remain key performers, but there is a legal and political «framework» for a collective response. Another essential feature of national security in the European Union states is multi-level governance [8-10]. The state forms the strategy, legislation, budgeting and security structures. At the same time, a significant part of the instruments operates through Union rules, through agreed standards, common requirements for sectors, coordination mechanisms, as well as through financial support for joint programs. This is evident in the example of cybersecurity, where a single legal approach to key sectors operates and states are required to develop national strategies and cooperate for cross-border response. This is also evident in the example of increasing the resilience of critical actors, where obligations are established to be prepared for a wide range of threats, including physical and hybrid challenges.

The relationship between the external and internal components of security requires a separate explanation. Thus, in a more traditional logic, national

security was often associated with external threats and border defense. In European practice after the Cold War, an approach was more pronounced, where internal security, in particular countering terrorism, organized crime, illegal arms trade, achieving the resilience of cities and critical infrastructure, is part of broader national security. At the same time, the line between internal and external is increasingly blurred. Hybrid operations by foreign actors can combine cyberattacks, disinformation, economic pressure and incitement of social conflicts, without formally crossing the threshold of open armed aggression. The theoretical conclusion here is that national security becomes an integrated policy, where law enforcement agencies, cyber defense services, energy regulators, diplomacy and defense work in an interconnected logic (Table 2).

Table 2

External and internal components of the EU national security system

Component	Core purpose	Key instruments and typical stress points
1	2	3
External component	Deter and respond to external coercion and armed aggression, protect borders and sovereignty, and manage security crises beyond national territory that could destabilise the European security environment.	Instruments include defence planning, force readiness, intelligence cooperation, interoperability with allies, military mobility, and defence diplomacy. Stress points include stock depletion during prolonged crises, industrial bottlenecks, escalation risks, and dependence on limited suppliers for critical equipment and ammunition.
Internal component	Maintain governability and societal stability by ensuring continuity of essential services, preventing cascading failures, and protecting citizens from hybrid pressure aimed at disrupting daily life and public trust.	Instruments include protection of critical infrastructure, cybersecurity governance, emergency management, continuity planning for energy, transport, health, finance, and digital services, plus counter-disinformation and strategic communication. Stress points include cyberattacks, sabotage, energy disruptions, panic dynamics, and uneven preparedness across sectors and regions.

1	2	3
Integrated component	Link external defence with internal resilience so that shocks in one domain do not collapse the whole system, and so that national and EU-level measures reinforce each other under simultaneous pressure.	Instruments include whole-of-government risk assessments, cross-sector crisis exercises, shared situational awareness, coordination among defence, interior, energy, digital and intelligence bodies, and partnerships with private operators. Stress points include institutional fragmentation, slow coordination, competing priorities, and vulnerabilities created by tightly coupled interdependent systems.

Source: formed by the authors

It can be said that the essence of national security in the European Union states lies in the protection of the state and society through a combination of defense, legal stability, economic capacity and the protection of critical systems. Its feature is multi-level, where national responsibility is combined with supranational rules, solidarity mechanisms and a common strategic vision. In modern Europe, security increasingly means less and less only “the ability to repel an attack”, and increasingly means “the ability to withstand pressure and maintain the functioning of the state and society”, including cyberspace, energy, communication, citizen trust and institutional governance. It is this logic that creates the basis for further analysis of how the full-scale armed invasion of Ukraine by the Russian Federation after February 2022 accelerated changes in the national security strategies of the European Union states, their budgets, resilience policies and defense cooperation.

Chapter 2. EU security in the face of a full-scale war in Ukraine

The full-scale armed invasion of Ukraine by the Russian Federation after February 2022 has dramatically changed the security environment for the states of the European Union, because it has destroyed the assumption of long-term predictability in Europe and has brought the threat of a major conventional war back to the agenda. In a theoretical sense, this has meant a change in the basic model of understanding security, from the idea of gradual integration through economic interdependence to the idea of competition, coercion and force as real instruments of international policy. For the European Union, this has become a challenge not only as a community that builds policy on law and rules, but also as a complex system of interdependencies, where the disruption of stability in the east is rapidly transforming into energy, financial, migration, information and cyber risks. In such conditions, security begins to be interpreted more broadly, as the ability to simultaneously contain a threat, maintain the resilience

of society, protect critical systems and maintain political unity under prolonged pressure. A key feature of the European Union's security in wartime is the combination of national responsibility and common response mechanisms. National security remains the responsibility of states, but many of the instruments that have become decisive after 2022 are shaped at the level of pan-European decisions, through common rules, financing, coordination and sanction regimes. This creates a specific architecture where the European Union is at the same time a platform for policy coordination, a source of resources and a regulatory regulator that pushes member states to increase their preparedness. The military factor has made visible the limitations of this architecture, because defense and the use of force are traditionally more related to national structures and the North Atlantic Alliance. At the same time, the war has accelerated the processes in which the European Union is developing its own instruments in the field of security and defense, trying to be not only an economic actor, but also a participant in the security ecosystem.

It has reinforced the understanding that deterrence requires not only intentions and statements, but also the ability to act quickly, supply resources, ensure mobility and maintain the industrial base. This leads to a dual security logic. The first logic is deterrence through allied guarantees and compatibility with the North Atlantic Alliance. The second logic is the development of European capabilities that reduce dependence on external suppliers and increase autonomy in a crisis situation. Thus, within the framework of the Strategic Compass, the intention is recorded to form a European rapid deployment capability of up to five thousand soldiers and to make it fully operational by 2025. For security theory, this means that the European Union is trying to have a rapid reaction instrument that does not replace the collective defense of the North Atlantic Alliance, but allows it to act in crises where speed and political coherence are required. The significance of this approach is also that it stimulates regular training, common standards and practical interaction, and it is these elements that form real readiness in a complex external environment. A separate problem has become military mobility, which has proven to be a critical condition for effective defense on the eastern flank and for supporting partners. When a war is going on nearby, the speed of movement of forces and equipment, procedural permits, transport capabilities and logistics become factors of a strategic scale. Against this background, the European Union is developing military mobility policies and coordinating them with the North Atlantic Alliance, in particular through action plans in this area (Table 3).

Table 3

The role of EU countries in ensuring the functioning of NATO during active hostilities in Ukraine

Role performed by EU Member States (many of which are NATO Allies)	How this role sustains NATO functioning during wartime conditions near the Alliance's borders
Strengthening deterrence and defence posture on NATO's eastern flank	EU countries contribute forces, readiness units, air policing, and maritime presence, helping NATO maintain credible deterrence and forward defence. This reduces the risk of spillover, reassures exposed Allies, and signals unity, which is central to Alliance cohesion. By hosting forces, enabling exercises, and improving national readiness, EU states help NATO translate political commitments into operational reality under conditions of heightened tension
Enabling logistics, military mobility, and host-nation support	NATO's effectiveness depends on the ability to move troops and equipment quickly across Europe. EU countries provide transport corridors, infrastructure access, reception and staging areas, and legal-administrative facilitation for cross-border movement. In wartime proximity, these functions become strategic, because speed and predictability determine whether reinforcements can arrive before a crisis escalates. Investments in roads, rail, ports, and procedures directly increase NATO's operational tempo and credibility
Building and sustaining defence production, procurement, and stock replenishment	Active hostilities create high demand for ammunition, air defence, spare parts, and replacement systems. EU countries support NATO functioning by expanding industrial output, coordinating procurement, and rebuilding depleted stocks, which ensures that deterrence is not hollowed out by prolonged consumption. Defence industrial capacity acts as a strategic backbone, because NATO's plans assume that Allies can sustain operations over time rather than relying on short-term inventories
Sustaining political cohesion, sanctions implementation, and resilience against hybrid pressure	NATO is a political-military Alliance, so cohesion is a core capability. EU countries reinforce NATO's functioning by maintaining unity on threat assessment, public messaging, and long-term commitments, while also implementing sanctions and countering disinformation and sabotage that aim to fracture solidarity. By strengthening cyber resilience, protecting critical infrastructure, and supporting civil preparedness, EU states reduce the effectiveness of hybrid coercion that could distract Allies and undermine NATO decision-making speed

Source: formed by the authors

One of the central features of the European Union's security in the context of war has been that support for Ukraine has become a practical tool for

reducing risks for the member states themselves. In international security theory, this can be described as a policy of preventing the spread of the conflict and as an investment in stability, because the outcome of the war determines the level of threat to Europe for years to come. That is why the security logic of the European Union includes simultaneously military, financial, technological and political support for Ukraine. War near the borders of the European Union inevitably affects internal security. This is manifested in the increasing burden on border services, in the challenges associated with the reception and integration of people fleeing the war, in attempts to destabilize society through disinformation, polarization and incitement to conflict. Theoretically, this confirms that internal and external security are linked, and national security does not end at the border line. In such an environment, strategic communications, trust in institutions, media literacy, the protection of electoral processes and the ability of authorities to work together with local communities and the private sector are increasingly important. It is also important that resilience cannot be reduced to technical standards. In security theory, resilience includes social capital, the willingness of people to support rules, the ability of a society to withstand prolonged restrictions, and the presence of institutions that act consistently and understandably. In a nutshell, if infrastructure is the body of security, then public trust is its nervous system. This is why, in the context of the war in Ukraine, the security of the European Union is increasingly described in terms of unity, coordination and long-term support, rather than just one-off solutions.

The internal component of national security in the European Union is based on the simple idea that the security of citizens begins with the governance of the space in which people move, work and do business freely. Here, the risks appear less military, but are often no less destructive. These include terrorism, organised crime, illicit trafficking in arms and drugs, human trafficking, financial crime, money laundering, corruption networks, as well as the instrumentalisation of migration and smuggling. Due to the openness of the borders within the Schengen area, the effectiveness of one country depends on the capabilities of its neighbour, which therefore creates the need for common information systems, common inspection standards and joint operations. The European Agency for Law Enforcement Cooperation, known as Europol, received an expanded mandate in 2022, which shows the desire of the European Union countries to strengthen the exchange of data and the coordination of investigations within the framework of common rules. A separate common border architecture operates, where the European Border and Coast Guard Agency, known as Frontex, plays a key role, its mandate is defined by a regulation that sets the framework for support to states at the external borders. At the political level, the European Commission presented the Security Union Strategy for 2020-2025 in 2020, which focuses on combining physical security,

digital security, the protection of citizens and the resilience of societies. All this directly affects the national security of each state, because internal security in conditions of high mobility is a common task, and if one link is weak, the risk quickly spreads throughout the Union through transport, finance, digital services and human connections. Cybersecurity and the protection of critical infrastructure have today become the core of national security for the countries of the European Union, because the modern state actually lives in networks. Energy, banking, hospitals, transport, water, telecommunications, satellite services, public registers, electoral infrastructure and industrial control systems are often connected to the digital environment and can therefore be disrupted without a single shot being fired. In response, the European Union adopted in 2022 Directive 2022/2555 on measures for a high common level of cybersecurity in the Union, as well as Directive 2022/2557 on the resilience of critical entities. The logic of these acts is that countries should have at least the same requirements for risk management, incident reporting, supplier control and verification of the preparedness of sectors that are vital. This was followed by the Cyber Solidarity Regulation, which aims to strengthen common capabilities, including better threat detection and collective support in the event of major attacks. Alongside cyber risks, there is another layer, often referred to in the European Union as hybrid threats, where the adversary combines cyberattacks, disinformation, economic pressure, provocations at the borders and influence on political processes. The Council of the European Union describes this approach as a toolbox for countering hybrid campaigns, which allows for coordinated cross-sectoral responses. Other instruments are also in place in the information sector, including the European Action Plan for Democracy, as well as the Digital Services Regulation, which requires platforms to be more transparent and accountable and is already being implemented in practice, as is evident even from the first major decisions and fines. The massive use of automated content creation and distribution systems, including artificial intelligence-based technologies, creates particular complexity, as they make manipulation cheap, large-scale and fast, and therefore national security increasingly depends on the ability of the state and society to distinguish truth from deliberate influences and to recover quickly from digital attacks.

Conclusions

Thus, the security of the European Union in the context of a full-scale war in Ukraine is a multi-level system that includes defense readiness, support for Ukraine as an element of its own security, sanctions and financial policy, energy independence, cyber resilience, protection of critical actors and social cohesion. The war has shown that threats are interconnected, and therefore the effectiveness of security policy depends on the ability to combine instruments

of different nature, from law and regulations to industry, logistics and communications. It is at this point that the rethinking of national security in the states of the European Union is turning into practice, where preparedness, resilience and strategic unity become the main ones.

National security in the European Union states is a multidimensional policy that encompasses defense, institutional resilience, the ability of the economy to withstand shocks, energy security, cyber security, information security, and the continuity of critical systems. In this sense, security has long ceased to mean only the absence of a threat. It means the ability of the state and society to act under pressure, maintain control, adapt quickly, and recover from crises without destroying the legal basis and the trust of citizens. It is this ability that becomes a key criterion, because modern threats rarely have a single nature and usually spread through interdependent networks, markets, infrastructure, and digital platforms. The European specificity of security is that it is formed simultaneously at the national level and at the level of the European Union, where common rules, standards, and coordination mechanisms operate. Member States retain responsibility for the core elements of security, but modern risks, hybrid attacks, cyber incidents, infrastructure sabotage, energy shocks, migration challenges, information operations and financial fluctuations, often have a cross-border nature and require synchronised action. This makes multi-level governance not a bureaucratic superstructure but a necessary condition for effectiveness, as without coherence of strategies and procedures even strong national systems can remain vulnerable due to weak links in the common space.

References:

1. Valikhnovsky, R. (2010). Approaches to building a humanitarian paradigm of national security. *Bulletin of the National Academy for Public Administration under the President of Ukraine*, no. 1, pp. 243-253.
2. Prav, R. (2021). Ways to improve the efficiency of mechanisms for ensuring the national security of Ukraine in the context of European experience. *Scientific Perspectives*, vol. 9(15). DOI: [https://doi.org/10.52058/2708-7530-2021-9\(15\)-197-206](https://doi.org/10.52058/2708-7530-2021-9(15)-197-206)
3. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning*, vol. 19, no. 1, pp. 277-288.
4. Kryshchanovych, M., Antonova, L., Filippova, V., Dombrovska, S., Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. *International Journal of Safety and Security Engineering*, vol. 12(2), pp. 193-199.
5. Light, S.E. (2014). Valuing national security: Climate change, the military, and society. *UCLA Law Review*, no. 61, pp. 772-1812.

6. Dumchykov, M., Utkina, M., Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering*, vol. 12(4), pp. 481-490.
7. Sotiroski, L. (2024). The impact of climate change on national security. *International Journal of Sustainable Development and Planning*, vol. 19, no. 1, pp. 391-401.
8. Sytnyk, G. (2017). Institutional and civilizational paradigm as the basis of the methodology of public administration in the field of national security. *Scientific Journal of the National Security Academy*, no. 1-2, pp. 10-23.
9. Shtangret, A., Topalova, E., Polovcev, O., Chornenka, O., Musiyovskyi, A. (2021). Practical aspects of the use of anticipative management in the process of ensuring the economic security of an enterprise. *Business: Theory and Practice*, vol. 22(1), pp. 202-210.
10. Alazzam, F.A.F., Shakhathreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. *Ingénierie des Systèmes d'Information*, vol. 28, no. 4, pp. 969-974.