

The Strategic Logic of Total Defense in the Age of Artificial Intelligence: Algorithmic Resilience

Veljko BLAGOJEVIĆ¹, Aleksandar PAVIĆ²

Abstract: The paper explores the impact of artificial intelligence on the transformation of the concept of total defense in the contemporary security environment. Starting from the understanding of total defense as a comprehensive system of societal and institutional resilience, the paper analyzes artificial intelligence as a structural factor that reshapes the organization of defense, decision-making processes, and state action. Through a comparative analysis of the experiences of the Baltic and Scandinavian countries, key models for integrating algorithmic systems into national mechanisms of deterrence, crisis management and warfare are identified. The inclusion of artificial intelligence as a structural factor in the concept of total defense transforms its organizational architecture, shifting the focus from the traditional civil–military concept to an integrated system of societal resistance and resistance management of the entire society. Based on these findings, the paper proposals are formulated for a strategic approach to Serbia’s concept of total defense and its transformation into a modern model that integrates political, economic, military, informational and technological capacities into a unique architecture of algorithmic resilience. The aim of the paper is to show how artificial intelligence is becoming the foundation of a new strategic logic of total defense, in which algorithms serves as a catalyst for resilience and deterrence in an era of complex security threats. At the same time, the paper highlights the potential risk of using artificial intelligence in the absence of an adequate legal framework, with emphasizing the need to strengthen social cohesion in terms of trust in institutions, resilience to information warfare and active public engagement in the modern concept of total defense.

Keywords: total defense 2.0, artificial intelligence, strategic logic, algorithmic resilience, national security

¹ Senior Research Associate, Institute for International Politics and Economy, Belgrade, Serbia. E-mail: veljko@diplomacy.bg.ac.rs, ORCID: <https://orcid.org/0000-0001-6981-0560>.

² PhD candidate, University of Defense – Military Academy, Belgrade, Serbia. E-mail: aleksandar.pavic@mod.gov.rs, ORCID: <https://orcid.org/0009-0005-6737-0094>.

Introduction

In an era in which the boundaries between peace and war, civil and military, physical and cyberspace are increasingly blurred, the concept of state defense must reconsider its theoretical and operational foundations. Contemporary threats, including hybrid operations, non-state actors, cyberattacks and disinformation campaigns indicate that the traditional model of military defense is no longer adequate. In a broader theoretical context, this question is linked to the Copenhagen School's concept of societal security, which emphasizes the importance of protecting the vital functions of society, as well as with paradigms of multidomain warfare that emphasize the integration of all instruments of national power.

As emphasized in the Brookings Institution recently published study, modern enemies can paralyze the functioning of the state not by firing a single missile, but by "killing the system from within", through infrastructure disruption, information entropy and cyber operations (Noyes and Humpal 2025). In this context, there is a need for a concept that encompasses society as a whole and mobilizes all available resources a model that will make the state not only resilient, but also adaptive in times of crisis.

The concept of total defense, which traditionally referred to the mobilization of civilian and military capabilities in times of war, has regained prominence. As described by Grigalashvili (2023), the modern concept of total defense is based on two fundamental principles: resistance and resilience. Research conducted by Jordan (2024, 315) shows that the Baltic states, under pressure from developments in their immediate security environment, have once again adopted a comprehensive approach to defense in which society itself constitutes a key element of resistance.

These examples demonstrate that the concept of total defense is not only a traditional concept inherited by small and medium-sized countries, but has also attracted scholarly attention in major powers, including the United States of America (USA). The reaffirmation of the total defense model in response to modern challenges and threats to national security requires, in addition to traditional instruments, the application of advanced technologies. However, as technologies are evolving faster than institutions can adapt their regulatory framework, we are entering an era in which the application of artificial intelligence is no longer merely an option but a strategic necessity. Jacob Simpson et al. (2021) as early as 2021 observed that artificial intelligence could transform command-and-control and information systems. However, if

implemented without thorough prior analysis, such systems may themselves become sources of critical vulnerabilities. Therefore, the integration of artificial intelligence in the concept of total defense requires a new strategic logic that not only technological, but also organizational and, to some extent, cultural.

Based on the foregoing, this paper hypothesizes that incorporating artificial intelligence as a structural component of total defense transforms its organizational architecture by shifting the focus from the traditional civil-military concept to an integrated system for managing societal resilience through data, algorithms and predictive analytics. The paper aims to analyze that process using the comparative analysis, present examples of best practice and propose a model for Serbia.

Methodologically, the paper relies on a comparative analysis of selected models of total defense of several states, as well on a content analysis of strategic documents, academic articles and research institute reports, in order to identify potential organizational and technological models for the application of artificial intelligence. The paper also formulates recommendations of the Republic of Serbia's total defense concept, particularly with regard to institutional organization, technology, human resources, and the legal framework.

In addition to the Introduction and Conclusion, the paper consists of four substantive sections. The first section discusses the theoretical framework and modern approaches to the concept of total defense. The second section introduces the modern concept of total defense, the so-called. 2.0. The third section examines artificial intelligence as a transformative factor in development of concept. The final section proposes a model for Serbia, and concludes with recommendations for further research.

Theoretical framework of the concept of total defense

The concept of total defense has evolved through different historical and political phases, but its essence has remained unchanged. The evolution from mass mobilization during two World Wars, through the Cold War to modern doctrines of resilience and comprehensive digital defense reflects significant changes in the global strategic environment. Contemporary security threats have led to a conceptual shift, in which total defense is no longer based solely on territorial defense but on the long-term resilience of society as a whole (Buzan and Waever 2003; Linkov and Trump 2019). State defense is not exclusively a military responsibility but a systemic undertaking involving society as a whole.

Although traditionally associated with smaller states facing existential threats, total defense has attracted renewed attention in academic and strategic debates, particularly following the Russian annexation of Crimea in 2014, the escalation of the conflict in Ukraine, and the rapid development of digital technologies, cyber threats, and artificial intelligence. This concept implies that state defense is based on the integration of society, state institutions, the economy and military capacities into a unified national security system.

The origins of total defense can be traced to the nineteenth-century models of mass mobilization, particularly in Prussia, while its modern form emerged during the Cold War, especially in the Scandinavian countries. Sweden and Finland developed the so-called “Total Defense” (*totalförsvar*) system, which integrates military and civilian resources into a comprehensive model of national preparedness for crises, war, and occupation. As Sundelius and Eldeblad (2023) point out, total defense entails the structural integration of civil and military capacities in order to ensure the continuity of state functions. In the post-Cold War period, the concept evolved, as states such as Estonia and Israel incorporated cyber resilience, social cohesion, and strategic communications, thereby broadening its conceptual scope. The total defense concepts adopted by the Baltic States deserve special attention in the context of adaptation to the modern security environment. The Baltic States have adopted a comprehensive approach to national defense. Latvia has placed greater emphasis on public education, whereas Lithuania has prioritized the development of international cooperation. Estonia has been the most successful in implementing a comprehensive approach to defense (Jordan 2024). Estonia has adopted the so-called distributed resilience, which integrates the information and communication sector with civil society (Tikk, Kaska and Vih 2010).

Contemporary literature emphasizes that total defense is best understood through two complementary concepts: institutional coordination (*whole-of-government*) and societal mobilization (*whole-of-society*). Among other countries, the Baltic States integrate all societal subsystems – political, economic, informational and security – into a common architecture of resistance (Jordan 2024, 315). Small security systems cannot compensate for strategic weaknesses through the quantity of their weaponry, but by synthesizing their resources into a functional defense system. This is the fundamental principle on which total defense is founded in the modern strategic environment.

The dominant theoretical approaches to the concept of total defense are based on engagement of both government institutions and society as a whole. The concept thus plays a key role in the credibility of national defense and deterrence. These approaches are also grounded in the theory of military

strategy. In modern doctrines, total defense has become closely associated with the concepts of resistance and resilience (Grigalashvili 2023, 240). Holling's concept of adaptive cyclicity shows that complex systems can survive by absorbing disturbances, reorganizing their structure, and maintaining their functionality (Walker et al. 2004). In the field of security studies, this theory has evolved through approaches that define resilience as *the ability of a system to prepare, react, recover and adapt* (Linkov, Trump and Hynes 2019). Resilience is not only a physical or infrastructural category but also psychological and cultural one. Society must be capable of withstanding the stresses of crisis without collapsing the value structure and the will to resist.

On the other hand, Lawrence Freedman's (2013) work places total defense within the broader framework of *the deterrence strategy in conditions of limited resources*. Total defense enables smaller states to raise the cost of aggression to a potential aggressor through societal mobilization, resistance to occupation, and a long-term defensive strategy. In the context of the strategic concepts of small states, their greatest asset is a predictable organizational architecture that enables rapid response and minimizes initial damage.

Furthermore, contemporary literature increasingly interprets total defense through the lens of complexity theory. Modern threats have a multi-domain structure, which means that they do not follow the linear logic of classical warfare. Buzan and Waever (2003) argue that security is "structurally dispersed" across different sectors: military, political, economic, social and cyber space. In such a system, national defense becomes networked, and all subsystems of the state are interdependent. The failure of a single domain can trigger systemic effects, particularly in the case of digital threats, which evolve more rapidly than traditional institutional response capacities. This implies that total defense in the twenty-first century is no longer a traditional model of mobilization but a dynamic system of adaptive response.

Finally, when the role of artificial intelligence is considered in the context of the theoretical concept of total defense, as a transformative factor, it introduces a new dimension of this concept. While earlier theoretical approaches regard the state as the primary bearer of resistance, the age of artificial intelligence shifts the center of gravity toward technological infrastructure as an equally strategic factor. Artificial intelligence is transforming the very foundations of command and control by introducing predictive capabilities, autonomous detection and algorithmic decision-making. However, the same authors warn that the uncritical introduction of artificial intelligence creates new vulnerabilities, including algorithmic bias, cyber dependency and structural exposure to unreliable data. In this sense, the paper argues that artificial

intelligence should be understood as a structural factor of total defense rather than as a tool added to existing models. The integration of artificial intelligence moves the concept toward “algorithmic resilience” defined as the system’s ability to predict, absorb and adapt risks through dynamic data analysis. The integration of artificial intelligence in the traditional concept of total defense elevates the concept to a new level and may well provide the foundation for what the authors define as “total defense 2.0”.

The strategic logic of the “total defense 2.0” concept

Strategic logic in the modern security environment represents an intellectual framework that connects political objectives, available resources and the dynamics of the operational environment into a coherent system of action. It rests on the premise that a strategy cannot be a series of isolated decisions but must possess an internal rationality and “grammar” that explains why a certain approach is effective under conditions of complex, hybrid, and technologically mediated threats. As Colin S. Gray (1999) points out, strategy is sustainable only when there is a clear logical causal relationship between politics, military power and its employment. Similarly, Freedman (2013) emphasizes that contemporary strategy functions as a “narrative logic” that integrates the goals, methods, and perceptions of different actors. In an era of rapid technological change and advances in artificial intelligence, strategic logic becomes even more important because it enables complex data, multidomain realities, and uncertainty to be translated into a sustainable and adaptive model of action.

The concept of total defense, which lost some of its prominence after the end of the Cold War, regained relevance again during the second decade of the twenty-first century. As some theorists have noted, old recipes are being applied to new threats. For example, following the end of the Cold War, Sweden abandoned the further development of its total defense model and instead focused on strengthening emergency management and capabilities for expeditionary military operations, an approach that was typical for most European countries. The renewed interest in the previous model was prompted by changes in the regional security environment following Russian aggressive policy. Accordingly, in 2019, Sweden carried out an analysis and put forward proposals in a document entitled *Resilience - the concept of total defense and the development of civil defense 2021–2025*. This document represents the first phase in the revitalization of the concept of total defense, i.e. its new version

2.0 as discussed in the Warsaw Institute (2018) report *Swedish Total Defense*. The document places particular emphasis on strengthening resilience against hybrid threats. The document’s central objective is to strengthen society’s ability to function independently during the first twelve weeks of a crisis or potential war. The proposed measures envisage the mobilization of all citizens and the transition to a wartime condition of living, organization and work. The concept is based on the premise that every citizen has an individual role and responsibility, with everyday activities adapted to support the functioning of society during crisis or wartime. *Table 1* below indicates the classification and evolution of the strategic approach to Sweden’s total defense concept (Angstrom and Ljungkvist 2024, 517).

Table 1. Swedish total defense strategies, 1948–2022

		Command and control	
		<i>decentralized</i>	<i>centralized</i>
Civil-military roles	<i>Separate</i>	„Cell“ (1948–1972)	„Stovepipe“(1972–1993)
	<i>Blurred</i>	„Fort“(2014–2022)	„Cluster“(1994–2014)

Source: Authors; according to: Angstrom and Ljungkvist 2024, 517

The evolution of the leadership and command model, as presented in Table 1, in correlation with the relationship between civilian and military roles, indicates a gradual transformation of security management from institutional segmentation to functional integration. The early “cell” model (1948–1972), based on decentralized command and clearly separated civil-military responsibilities, ensured a high degree of systemic resilience, albeit at the cost of limited strategic coherence. In contrast, the “stovepipe” model (1972–1993) introduced centralized management while preserving institutional duality, contributing to more effective control but also to the emergence of functional “silos” and weak intersectoral coordination. The post-Cold War period was characterized by the “cluster” model (1994–2014), which integrated civilian and military roles within a centralized system, enabling greater coordination of policies and operations while simultaneously increasing dependence on the decision-making center. Finally, the “fortress” model (2014–2022) reflects adaptation to hybrid threats and a multidomain environment, combining integrated civil-military capabilities with decentralized command, thereby

strengthening operational flexibility and systemic resilience, while poses challenges to preserve unified strategic governance.

Immediately after Sweden's measures, a new study examined the concept of total defense 2.0 in the context of the Baltic region. In addition to various measures aimed to improve the concept, particular emphasis is placed on the development of scientific and technological communities, the economy and the defense industry. The concept emphasizes investment in technologies as part of overall defense and societal resilience capabilities, including increased production of critical products, drones, artificial intelligence, robust cyber capabilities and cost-effective space technologies. The extent to which the Nordic states coordinate and share the benefits of these technologies with their Baltic partners will directly enhance regional resilience and the overall effectiveness of total defense (Saxi, Sundelius and Swaney 2020, 13).

In 2022, Jones and Love (2022) introduced the concept of "Resilience and Resistance 2.0", arguing that it serves as a catalyst for enhancing societal resilience and resistance against invasion and potential occupation by revisionist forces. Drawing on the experiences of the initial phase of the conflict in Ukraine, Jones and Love highlighted the need for continuous assessment and refinement of total defense measures. The authors emphasize the importance of mobilizing society as a whole under government leadership. The development of an appropriate institutional framework in peacetime provides the foundation for successful implementation of the concept in wartime. All government programs must be legitimate and clearly understood by both the public and state institutions. At the same time, they must convey a credible deterrent message to the potential enemy (Jones and Love 2022). The above approach represents an enhanced concept of total defense that emerged in response to the crisis. However, if properly implemented, the concept can enhance a nation's resilience and deter aggression.

Annelies van Vark's (2025) examines the conceptual difference among the North Atlantic Treaty Organization (NATO) member states regarding the concept of total defense. With NATO Secretary General Mark Rutte's proposal to increase military spending to 3.5% of GDP, with an additional 1.5% allocated to strengthening societal resilience and infrastructure, the Alliance signals a renewed commitment to defending not only its territory but also the democratic values of its member societies. This dual emphasis on military capabilities and general societal preparedness is reminiscent of the "total defense" model long practiced in the Nordic countries (Van Vark 2025). This revitalized model of financing societal resilience, and thereby strengthening the Alliance's capacity to respond to emerging security challenges, demonstrates that the concept of total defense continues to evolve in response to the changing global security environment. In

this way, the concept of total defense continues to evolve, demonstrating that military power itself is not enough to defend the state and that national defense must be a responsibility shared by society as a whole. The revitalized concept should ensure that societies, states and allies act in a synchronized, structural and functional manner in response to a potential enemy.

It can be concluded that the concept of “total defense 2.0” represents the natural evolution of the classic concept of total defense, adapted to the modern multidimensional security environment. Whereas the traditional concept of total defense primarily integrates military and civilian resources to counter direct aggression, version 2.0 extends this approach by incorporating emerging technologies and a multidomain perspective. These emerging technologies are primarily reflected in the application of artificial intelligence, cyber security, and advanced weapons systems and military equipment. At the same time, the societal resilience requires the development of systemic capacities that enable both civil and public institutions to function under a wide range of pressures, including disruptions affecting essential services, healthcare, critical infrastructure, and public awareness. A particular challenge is posed by hybrid threats that combine cyber and cognitive operations, economic coercion and geopolitical manipulation – dimensions that were not systematically addressed by the classic total defense.

Finally, a multidomain approach, based on the integration of emerging operational domains such as space and cyber space, enables coordination across the physical, information and digital space, resulting in a more dynamic and flexible defense posture. Total Defense 2.0 is not merely a military or civilian strategy; rather, it represents a holistic model of state and societal resilience, in which technology and intellectual capital become key enablers of crisis prevention and response.

Three-level transformation and total defense 2.0 in the age of artificial intelligence

The new challenges facing the concept of total defense in an era of advanced technologies, multidomain engagement of forces and assets, asymmetric threats and hybrid warfare require an equally comprehensive and integrated response. The traditional concept of total defense, which relied primarily on the military component, with the civilian sector serving in a supporting role, is no longer sufficient to address modern security challenges. For this reason, this paper adopts the concept of total defense 2.0 as a necessary response. The integration

of artificial intelligence into the security system represents not merely a technological advancement but a profound transformation of the concept of total defense. This transformation encompasses changes at three interrelated levels: structural, functional, and social. Although these three levels are already embedded in Northern European models of total defense, it is only with the advent of artificial intelligence that they acquire a coherent systemic dynamic, integrating defense and security institutions, national infrastructure, critical resources and the society into a unified architecture of algorithmic resilience.

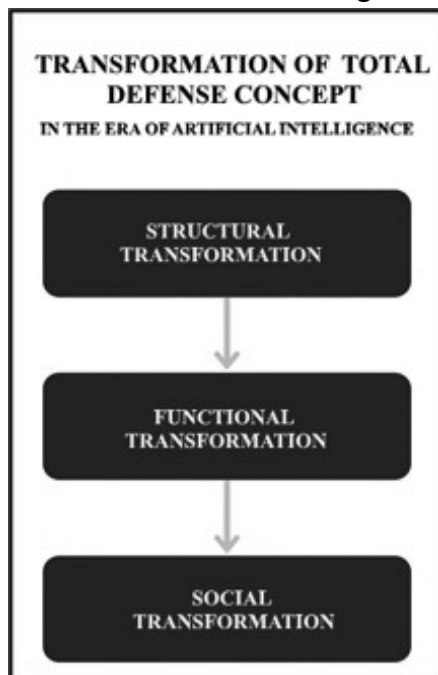
The transformation of the concept across these three levels is intended to ensure the algorithmic resilience of the nation, state, or an alliance, thereby establishing a new approach to implementing the concept. Algorithmic resilience refers to the ability of the state, its institutions and society to leverage artificial intelligence, big data analysis, and automated processes to anticipate, absorb, adapt to and recover from complex multidomain threats. In era of exponential technological advancement, resilience is no longer merely an organizational or infrastructural category, but also an algorithmic capability that enables systems to learn, analyze and respond proactively to emerging crisis. Research on crisis response and artificial intelligence demonstrates that algorithmic models can significantly enhance early risk detection and raise levels of systemic resilience (Ilcic, Fuentes and Lawler 2025), while advances in generative artificial intelligence for cyber security are increasingly viewed as a key factor in the protecting critical infrastructure and maintaining social stability (Radanliev, Santos and Ani 2025).

Within the Total Defense 2.0 framework, algorithmic resilience serves as an integrative mechanism that links the military, civilian, cyber and cognitive domains into a unified national security system. It enables hybrid threats to be detected before they escalate, allows institutions to automatically stabilize under pressure, and supports decision-makers by providing predictive models and cognitive analytics. In this way, algorithmic resilience transforms Total Defense 2.0 from a reactive defense model to a proactive, dynamic and adaptive system capable of operating in real time.

As illustrated in *Figure 1*, the transformation should be understood as a sequence of clearly defined stages. The first stage involves structural changes at the societal, state and the alliance levels. This first level provides the basis for further development and lays the foundation for an enhanced concept of total defense. Once an optimal system structure has been established, the next stage is functional transformation. New and more advanced functions should ensure the more effective use of available resources and optimize responses at all levels, from the individual to the society as a whole. The capabilities offered by

technologies such as artificial intelligence are essential to this process. Finally, the third level represents the society, which understands, knows and accepts the new developments in security.

Figure 1. The transformation of the concept of total defense in the era of artificial intelligence



Source: Illustration by the authors

Every state constitutes a complex system, regardless of whether it is a small, medium-sized state or a great power. The structure of a such system is inherently complex. However, a sound institutional structure does not necessarily guarantee the effective functioning of the system. This means that the functional level must constitute a natural extension of a well-structured state, supported by a clear allocation of responsibilities and resources. The last level related to society is perhaps the most sensitive. Without public acceptance and understanding of the functions of state structures, there is no cohesion in the system. This represents one of the most important challenges in implementing the concept of total defense. A lack of understanding roles of individuals, groups of people, a legal entities, large state systems and other relevant actors is the

main source of inconsistency in the process of planning, organization, and realization of the concept of total defense. One potential source of cohesion is the broad application of artificial intelligence resources across the three levels of transformation examined in this paper. It is precisely the structural, functional, and social transformation of the total defense concept that is necessary in order to introduce artificial intelligence into the concept.

Artificial intelligence can be understood as a structural transformer, which should provide a new defense management logic but also contribute to the actualization, optimization, and activation of the predict-prevent-respond paradigm. In essence, the power of the algorithm should become a central part of the command -and- control infrastructure. Such an upgrade of the concept, in addition to numerous advantages, also leads to the already traditional risks and limitations associated with the artificial intelligence. These are malicious activities of rival systems (*adversary attacks*), manipulation of data (*data poisoning*), automation of decisions, and ethical risks. This paper places particular emphasis on the structural factor as an element of transformation, while functional and social factors will be analyzed to a lesser extent.

Structural transformation

The structural level of transformation refers to the institutional concept, normative framework, division of competences, and the state's capacity to coordinate civilian and military resources. The basis of the functioning of the state is the structure of its institutions, authorities and resources. The ability to act jointly within the assigned competences to achieve the most important national interests and goals is the foremost imperative. The structure is also at the basis of the concept of total defense. In the traditional models of Scandinavia, Israel, or Switzerland, this architecture was material, infrastructural, and personnel. With artificial intelligence, it becomes informational, network-structured and dynamically adaptive.

In its document *EU Defense Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defense Readiness* from 2025, the European Union (EU) emphasized the importance of speed, agility, and risk assessment for defense. In the same way, it is stated that the EU needs a fundamental change in the way of thinking and procedures inherited from the past at all levels, from the member state, the industry, and the EU institution. The document highlights the structural challenges that are one of the key factors in the transformation of the "New Defense" model of the new defense policy, which is based on lessons

from Ukraine and the potential of revolutionary technologies in the field of defense (EC 2025, 7).

Araya and King (2022, 4), discussing the impact of artificial intelligence on defense and security, state that it represents a structural transformation in the nature of national security. The study implies that a greater focus is needed on the development and integration of advanced and transformative technologies, including cyber networks and autonomous systems. The basis of the structure of such systems is artificial intelligence. According to Steinmo (2010), modern states function as complex adaptive systems. In his research, he examines the transformation of the state across political, economic, and social dimensions.

The structural transformation factor considers a wide range of activities from defense based on developed industry to an algorithmic architecture where institutional capacity depends on the ability to learn and predict based on data. The introduction of artificial intelligence into the concept of total defense opens the possibility for predictive risk assessment, real-time crisis management, automated vulnerability analysis of critical infrastructure, optimization of logistics, mobilization, and support of civil society. In its concept of “civil preparedness”, NATO (2024) increasingly emphasizes the need for data-driven resilience, which places the structural level of total defense in a digital context. At the same time, countries like Finland and Estonia are developing models in which artificial intelligence is part of the entire national defense system, including cyber command, digital identification, and coordination. Thus, the structure of total defense is transformed from a system of fixed organizational lines into an architecture of algorithmically supported integration, in which data is the key resource.

In addition to the above, the structural factor in the transformation of the concept of total defense implies a transition from a traditional, static, and material-oriented architecture to a dynamically adaptive, networked, and algorithmically supported structure. The process can be broken down into several stages. The first phase includes the mapping of the existing structure, in which institutions, capacities, resources, and competences should be identified. Then the process continues with the analysis of critical points in the coordination of civil and military forces. A special process in this phase should be the assessment of the state’s digital and informational capacity, i.e., how much data is collected, processed and how much is used in the decision-making process. In the second phase, it is necessary to define the new principles of the organization, i.e. a new or changed structure. This new structure should enable the transition to a networked algorithmically supported architecture, in which the key resource is information. In this way, the system could learn and, based

on the available data, provide assessments to decision-makers in real time. The final segment in this phase would be the full integration of civilian, military, and private resources into one coordinated system.

The third stage of requirements is crucial in the context of algorithmic resilience; it represents technological integration. And it is realized by introducing artificial intelligence in risk management, cybersecurity, logistics, mobilization, and support to civil society. This is achieved in practice by developing autonomous and automated systems that contribute to speed and flexibility. The last segment of this phase would be the creation of standards to enable coordination among all actors, both at the national level and beyond. The fourth phase should test the adaptation of institutional capacities, primarily through changes in organizational design. Organizational units such as advanced decision centers, digital commands, data analysis units, and other AI-supported systems would have to be tested here. After the testing segment, changes to the normative framework would ensure flexible protocols, faster decision-making, and the legitimacy of integrating new actors. The last segment of this phase would include training and development of human resources for working with technologies and algorithmic systems.

The aforementioned four phases of structural transformation do not end with implementation but are only one cycle of the process, which should involve constant testing, iterative upgrades, and continuous learning. All this would lead to constant improvement of algorithms, processes, and institutional structure. The foregoing implies that structural transformation is an ongoing process, and that it essentially represents the basic phase in transforming the concept of total defense.

Functional transformation

The functional factor in the context of the transformation of the total defense concept as well as the implementation of algorithmic resistance represents the framework mechanisms of action and the format of vertical integration of the system. The functional transformation of total defense in the age of artificial intelligence refers to the accelerated evolution of the process of analysis, coordination, and operational action. While traditional systems of total defense were based on a reactive approach, in which institutions respond to already manifested risks, the integration of algorithmic systems enables a gradual transition to a model in which a crisis is identified and neutralized long before it becomes an operational threat. As Bollmann (2021) shows in his study of the digital transformation of Scandinavian defense structures, command and control

processes have become dependent on entirely new forms of data connectivity, sensor systems, and predictive models, which accelerate the decision-making and reshape the way security mechanism's function.

In the Scandinavian models of total defense, digitization has already made artificial intelligence an integral part of everyday activities, from situational awareness analysis to the coordination of civil-military structures. New systems function as “digital intermediaries” (Guo and Zhang 2026) that combine data from energy networks, public services, cyber systems and military platforms, creating a functional entity that the authors describe as network-enabled readiness (Khaledi and Saifoddin 2023). This transforms the classical model, which was dependent on hierarchical lines of command, into a network system that can change and adjust priorities and routes of action in real time.

Predictive analytics is a key aspect of this functional transformation. As research on digitization and crisis management in the Nordic countries shows, algorithms can analyze information flows from social networks to sensor systems and identify emerging risks, allowing resources to be directed before a crisis escalates (Wrangle, Bengtsson and Brommesson 2024). This is a significant innovation compared to the classic total defense, in which the system reacts only after the threat is manifested.

Multidomain connectivity becomes another feature of functional transformation. Israel's digitized defense model, described in several open analyses, shows how machine learning-based systems integrate the intelligence, operational, and logistics domains into a single platform, fundamentally changing operational functionality and speed of reaction (Aravantinos 2024). In this way, artificial intelligence becomes not only a technological addition to existing structures but a functional “core” that allows it to connect civil services, military structures and critical infrastructures in real time.

An additional functional aspect relates to informational and cognitive defense. When analyzing the Estonian model, systems for early detection of disinformation, analysis of emotional trends, and recognition of coordinated campaigns are becoming the standard in modern concepts of total defense (Teperik et al. 2022). Here, artificial intelligence acts as a system of protection for the cognitive security of society and institutions.

As a whole, the functional transformation of total defense in an era of artificial intelligence represents a transition from static, vertical, and reactive mechanisms to dynamic, network-organized, and predictively oriented action systems. In the broadest sense, the functional level includes mechanisms of action such as mobilization, command, crisis management, communication,

logistics, infrastructure protection, and operations in information, cyber, and cognitive space. Artificial intelligence changes this level through automation, optimization, and intelligent connection of processes.

Social transformation

Social transformation represents the most complex and deepest dimension of modern total defense. The basic task of this transformation is to build social cohesion and improve the algorithmic culture of security. While functional and structural transformation describe changes in institutional and operational mechanisms, social transformation reflects changes in culture, values, patterns of behavior, and relations between the state and citizens. Society's resilience is not exclusively an institutional capacity but above all, a social norm built through a conscious security policy and a culture of collective responsibility.

In the Scandinavian and Baltic models, social resilience increasingly rests on digital competence, institutional transparency, and citizens' trust in national security mechanisms. As Anthes (2015) shows in his analysis of Estonia, citizens become active participants in the security system not through classical mobilization, but through participation in digital services, cyber exercises, and common platforms for information processing. This changes the classic model of social mobilization: citizens become not only beneficiaries of defense, but an integral part of its cognitive and informational structure.

The cultural dimension of this transformation is evident in the way that digital literacy is becoming the new basis of security culture. In Estonia, Finland, and Sweden, digital competence is treated as a prerequisite for understanding modern risks from disinformation to cyber operations. The development of these competencies not only serves the individual security of citizens but also the strengthening of overall social resilience. Research on civil-military cooperation in Sweden shows that it is trust in institutions and trust in digital systems that are the basis for the successful operation of total defense (Tillberg, Berndtsson and Tillberg 2025).

From a societal perspective, artificial intelligence introduces a new dimension of trust. Trust in algorithms, their transparency and the mechanisms governing their oversight becomes as important as trust in public institutions. If the algorithms are perceived as opaque or biased, they can undermine the legitimacy of the entire defense system. The literature on strategic culture emphasizes that countries with limited capacities must build a culture of security in which technology and institutions reinforce a mutual trust, while citizens

actively participate in a common system of resistance (Agustanto, Runturambi and Puspitasari 2025).

Overall, the societal transformation of total defense in the age of artificial intelligence entails the development of a culture in which citizens, institutions, and algorithmic systems operate in a unique architecture. The Israeli concept of “society in arms”, the Scandinavian model of “people’s defense” and the Baltic idea of “digital citizenship” all rest on the assumption that social mobilization is key to multi-layered resilience. Rather than relying on the traditional model of a “society in arms,” contemporary total defense is evolving toward a “society in an algorithm,” in which citizens become active participants in cognitive and informational resilience, while trust emerges as a strategic resource of national security.

Contribution to the concept of total defense of the Republic of Serbia

The proposal of an improved model of the concept of total defense of the Republic of Serbia must be based on the real capacities of the state, while simultaneously following the principles of algorithmic resistance that are already visible in the successful Nordic, Baltic, and Israeli frameworks. Starting from the specifics of the Serbian security environment, civil-military infrastructure, and the level of society’s digital transformation, the model of total defense must be conceived as an integrated architecture that unites state institutions, the private sector, the academic community, and citizens in a unique system of resistance. This model should not be a copy of foreign solutions but an adaptation of the best practices confirmed in the Nordic and Baltic regions to the conditions of Serbia, bearing in mind its neutrality, geopolitical position, political and legal order.

The key assumption of the new model must be that total defense is not only a reaction mechanism to crises, but a system of continuous protection. Serbia already has parts of such a system within the security sector, intelligence services, civil protection and infrastructure operators, but they operate in a fragmented way, with limited data exchange and different levels of digitization. The introduction of artificial intelligence help to bridge these institutional divides by creating an integrated “social security ecosystem” that operates predictive analytics and dynamic coordination.

The first element of the proposed model would be the determination of the institution in whose jurisdiction the development and implementation of this concept

would take place. The current model, which envisages the competence of the Ministry of Defense, certainly cannot provide a modern approach to total defense based on the model of engagement of the entire society (*Whole of Society Approach*). The establishment of the National Center for the Development of the Total Defense Concept, which would function as a government body with clearly defined competencies and resources, would enable integration and represent a kind of hub for directing the actions of state and social capacities. The center would not only be a technical institution, but an analytical-command structure similar to the Finnish NCSC-FI (*National Cyber Security Centre Finland*) or the Estonian CERT-EE (*Küberintsidentide käsitlemine CERT-EE*). He would be in charge of collecting data from several sectors, such as the military, political, information, energy, telecommunications, public health, cyber domain, and education, in order to build a unique national situational awareness framework. Serbia has the administrative capacity to form such a body, because there are already institutions such as the Office for Information Technology and e-Government, the Regulatory Body for Electronic Communications and Postal Services (RATEL), and the Department for Emergency Situations of the Ministry of Interior, but their structural connection is necessary.

The second element concerns the introduction of artificial intelligence in support of civil-military coordination, which is a key lesson from the Swedish and Norwegian models. Serbia has formally developed civil-military cooperation mechanisms, but they mostly function in the context of emergency situations. In the age of artificial intelligence, this coordination must become continuous, based on algorithmic systems that monitor the status of resources, people, critical infrastructure, and communication flows. This would allow defense mechanisms to be activated without delay, and the decision-making structure would become more flexible. The artificial intelligence integration system would proceed according to the presented concept of structural, functional, and social factors.

The third element of the model concerns the construction of national cognitive defense, the most sensitive segment of algorithmic resilience. In recent years, Serbia has been exposed to disinformation, cyber-attacks, political influence, and campaigns targeting public discourse. In line with Estonia's experience, it is necessary to develop a system that combines algorithmic detection of manipulative content, quick reaction of state institutions, and education programs. Here, it is particularly important to connect media houses, scientific institutes, and security structures in a network that functions as a national cognitive security filter. Serbia already has capacities in this area, but they are neither centralized nor formally integrated into the defense framework.

The fourth element is the development of an ethical, legal, and regulatory framework that will enable the safe application of artificial intelligence. In this

sense, Serbia can draw on the experiences of the EU, International Telecommunication Union (ITU), and United Nations Educational, Scientific and Cultural Organization (UNESCO), but also adapt the rules to the specifics of its security culture. It is crucial to define accountability protocols, transparency standards, and oversight mechanisms over algorithmic systems, in order to prevent abuses and build citizens' trust. Without this dimension, even the best technical system remains without social legitimacy.

The fifth element refers to the role of the private sector, which is indispensable in all modern models of total defense. Serbia has a developed information and telecommunications technology (ICT) industry, a growing number of "startups" and several universities dealing with machine learning. All these actors must be included in the defense architecture as partners, not as external entities. The Finnish and Estonian models show that the private sector is becoming the bearer of key segments of the algorithmic infrastructure, from cyber protection to predictive systems. Serbia has the capacity to develop a similar approach with institutional support and funding through targeted programs.

Finally, the proposed model of Serbia's total defense should be based on the idea that the societal resilience is inextricably linked to rapidly developing technologies. Instead of relying on classical concepts of mobilization, the new model should develop algorithmically supported mechanisms of cooperation, prediction, and protection, which will enable Serbia to respond to the complex risks of the modern security environment. With this approach, Serbia can build a system that is not only adaptive, but also strategically flexible, and that offers proactive security management rather than reaction.

Conclusion

The paper starts from the thesis that the accelerated development of artificial intelligence essentially transforms the concept of total defense, moving it from the classic civil-military model to an integrated system of algorithmic resistance. The analysis of theoretical frameworks, as well as the comparative experiences of the Nordic and Baltic States, showed that total defense in the 21st century can no longer be understood exclusively as a reaction mechanism to armed aggression, but as a dynamic, multi-domain and socially rooted system of risk management.

The key results of the work indicate that artificial intelligence does not act only as a technological support to the existing defense structures, but as a

structural factor, that changes the very foundations of the organization, functioning, and legal arrangement of the concept of total defense. In this sense, the introduction of the concept of algorithmic resistance enables the transition from a reactive to a proactive logic of defense, in which threats are identified, analyzed, and neutralized before they escalate into an open crisis.

The analysis of the three levels of transformation—structural, functional, and social—demonstrates that the sustainability of total defense 2.0 depends on their simultaneous and coordinated development. Structural transformation provides an institutional and normative basis, functional transformation enables effective real-time action, while social transformation provides legitimacy, trust, and cohesion without which even the most advanced algorithmic systems cannot function effectively.

A key contribution of the paper lies in the proposed enhanced model of the Republic of Serbia's total defense concept, which builds on the principles of modern successful practice of algorithmic resistance, but adapted to national specificities, institutional capacities, and geopolitical position of the state. The proposed model underscores the need to integrate state institutions, the private sector, the academic community, and citizens into a single system, in which data, algorithms, and human resources work in sync.

At the same time, the paper highlights the limitations and risks associated with the application of artificial intelligence in the field of total defense, including issues of algorithmic bias, cyber vulnerability, ethical responsibility and preservation of democratic control. For this reason, algorithmic resistance should not be reduced to a technocratic project, but must be supported by a clear legal framework, transparency and continuous education of the society as a whole.

It can be stated that Total Defense 2.0 represents an evolutionary response to the complex security challenges of the modern age, in which the boundaries between peace and war, the physical and the digital domains, and the state and society are becoming increasingly blurred. In this context, artificial intelligence emerges as a key catalyst of a new strategic defense logic. However, its effectiveness depends on the state's ability to integrate it into a coherent, legitimate and socially accepted system.

Future research should focus on the empirical analysis of the implementation of algorithmic resilience, the development of indicators of its effectiveness, as well as comparative studies of different national models in the context of regional and collective security. In this way, the concept of total defense can continue its development as a relevant and sustainable answer to security challenges in the age of artificial intelligence.

Стратешка логика тоталне одбране у добу вештачке интелигенције: алгоритамска отпорност

Вељко БЛАГОЈЕВИЋ³, Александар ПАВИЋ⁴

Апстракт: Рад истражује утицај вештачке интелигенције на трансформацију концепта тоталне одбране у савременом безбедносном окружењу. Полазећи од схватања тоталне одбране као свеобухватног система друштвене и институционалне отпорности, рад анализира вештачку интелигенцију као структурни фактор који мења организацију одбране, процесе одлучивања и деловања државе. Компаративном анализом искустава балтичких и скандинавских држава, идентификују се кључни модели интеграције алгоритамских система у националне механизме одвраћања, управљања кризама и ратовања. Укључивање вештачке интелигенције као структурног фактора у концепт тоталне одбране трансформише њену организациону архитектуру, померајући тежиште са традиционалног цивилно-војног концепта ка интегрисаном систему отпора и управљања отпорношћу и отпору читавог друштва. На основу ових налаза формулишу се предлози за стратешки приступ концепту тоталне одбране Србије и његову трансформацију у савремени модел који интегрише политичке, економске, војне, информационе и технолошке капацитете у јединствену архитектуру алгоритамске отпорности. Циљ рада је да покаже како вештачка интелигенција постаје темељ нове стратешке логике тоталне одбране, у којој алгоритми делују као катализатор отпорности и одвраћања у добу сложених безбедносних претњи. Истовремено, рад указује на потенцијалне ризике употребе вештачке интелигенције у одсуству одговарајућег правног оквира, наглашавајући потребу за јачањем друштвене кохезије у погледу поверења у институције, отпорности на информационо ратовање и активног ангажовања јавности у савременом концепту тоталне одбране.

Кључне речи: тотална одбрана 2.0, вештачка интелигенција, стратешка логика, алгоритамска отпорност, национална безбедност

³ Виши научни сарадник, Институт за међународну политику и привреду, Београд, Србија. Е-пошта: veljko@diplomacy.bg.ac.rs, ORCID: <https://orcid.org/0000-0001-6981-0560>.

⁴ Докторанд, Универзитет одбране – Војна академија, Београд, Србија. Е-пошта: aleksandar.pavic@mod.gov.rs, ORCID: <https://orcid.org/0009-0005-6737-0094>.

Увод

У добу у којем се границе између мира и рата, цивилног и војног, физичког и сајбер простора све више замагљују, концепт одбране државе мора да преиспита сопствене теоријске и оперативне основе. Савремене претње, укључујући хибридне операције, недржавне актере, сајбер нападе и дезинформационе кампање указују на то да традиционални модел војне одбране више није адекватан. У ширем теоријском контексту, ово питање се повезује са концептом друштвене безбедности (*societal security*) Копенхашке школе, који истиче значај заштите виталних функција друштва, као и са парадигмама мултидоменског ратовања које наглашавају интеграцију свих инструмената националне моћи.

Како се наглашава у недавно објављеној студији Брукингс института (*Brookings Institute*), савремени непријатељи могу паралисати функционисање државе не испаљујући ниједну ракету, већ „убијајући систем изнутра“, посредством поремећаја инфраструктуре, информационе ентропије и сајбер-операција (Noyes and Humpal 2025). У том контексту, јавља се потреба за концептом који обухвата друштво у целини и мобилише све расположиве ресурсе, моделом који ће државу учинити не само отпорном већ и адаптивном у време кризе.

Концепт тоталне одбране који се традиционално односио на мобилизацију цивилних и војних капацитета у време рата, поново добија на значају. Како наводи Григалашвили (Grigalashvili 2023), савремени концепт тоталне одбране заснова се на два фундаментална принципа: отпорности (*resistance*) и еластичности, односно отпорности на поремећаје (*resilience*). Истраживање Џордана (Jordan 2024, 315) показује да су балтичке државе, под притиском дешавања у непосредном безбедносном окружењу, поново усвојиле свеобухватан приступ одбрани у којем само друштво представља кључни елемент отпора.

Наведени примери показују да концепт тоталне одбране није само традиционални концепт који баштине мале и средње државе, већ да је привукао и пажњу у научним круговима великих сила, укључујући Сједињене Америчке Државе (САД). Реафирмација модела тоталне одбране као одговора на савремене изазове и претње националној безбедности захтева, поред традиционалних инструмената и промену напредних технологија. Међутим, пошто се технологије развијају брже него што институције успевају да прилагоде регулаторни оквир, улазимо у доба у којем примена вештачке интелигенције више није само могућност, већ

стратешка нужност. Симпсон и сарадници (Simpson et al. 2021) још су 2021. године указали на то да вештачка интелигенција може да трансформише командно-информационе системе. Ипак, међутим, ако се примени без темељне претходне анализе, и сама може постати извор критичних рањивости. Стога, интеграција вештачке интелигенције у концепт тоталне одбране захтева нову стратешку логику, која није само технолошка, већ и организациона, а у извесној мери и културна.

На основу наведеног, у раду се поставља хипотеза да укључивање вештачке интелигенције као структурне компоненте тоталне одбране трансформише њену организациону архитектуру, померајући тежиште са традиционалног цивилно-војног концепта ка интегрисаном систему управљања отпорношћу друштва посредством података, алгоритама и предиктивне аналитике. Циљ рада је да тај процес анализира применом компаративне анализе, представи примере добре праксе и предложи модел за Србију.

Методолошки, рад се ослања на компаративну анализу одабраних модела тоталне одбране више држава, као и на анализу садржаја стратешких докумената, академских чланака и извештаја истраживачких института, ради идентификовања потенцијалних организационих и технолошких модела примене вештачке интелигенције. У раду се, такође, формулишу препоруке за концепт тоталне одбране Републике Србије, посебно у погледу институционалне организације, технологије, људских ресурса и правног оквира.

Поред увода и закључка, рад се састоји од четири тематска поглавља. У првом поглављу разматрају се теоријски оквир и савремени приступи концепту тоталне одбране. Друго поглавље представља савремени концепт тоталне одбране, такозвану верзију 2.0. Треће поглавље разматра вештачку интелигенцију као трансформациони фактор развоја концепта. Последње поглавље предлаже модел за Србију, након чега следе закључци и препоруке за даља истраживања.

Теоријски оквир концепта тоталне одбране

Концепт тоталне одбране развијао се кроз различите историјске и политичке фазе, али је његова суштина остала непромењена. Еволуција од масовне мобилизације током два светска рата, преко Хладног рата до савремених доктрина отпорности и свеобухватне дигиталне одбране

одражава значајне промене у глобалном стратешком окружењу. Савремене безбедносне претње довеле су до концептуалног помака, у којем се тотална одбрана више не заснива искључиво на територијалној одбрани, већ на дугорочној отпорности друштва као целине (Buzan and Waever 2003; Linkov and Trump 2019). Одбрана државе није искључиво војна одговорност, већ системски подухват који укључује друштво у целини. Иако се традиционално повезује са мањим државама изложеним егзистенцијалним претњама, тотална одбрана је поново привукла пажњу у академским и стратешким расправама, посебно након руске анексије Крима 2014. године, ескалације сукоба у Украјини и убрзаног развоја дигиталних технологија, сајбер претњи и вештачке интелигенције. Овај концепт подразумева да се одбрана државе заснива на интеграцији друштва, државних институција, економије и војних капацитета у јединствен систем националне безбедности.

Корени тоталне одбране могу се пратити до модела масовне мобилизације из 19. века, пре свега у Пруској, док се њен савремени облик развио током Хладног рата, нарочито у скандинавским државама. Шведска и Финска развиле су систем такозване „тоталне одбране“ (*totalförsvar*), који интегрише војне и цивилне ресурсе у свеобухватан модел националне припремљености за кризе, рат и окупацију. Како истичу Сунделиус и Елдеблад (Sundelius and Eldeblad 2023), тотална одбрана подразумева структурну интеграцију цивилних и војних капацитета ради обезбеђивања континуитета државних функција. У постхладноратовском периоду концепт је еволуирао, јер су државе попут Естоније и Израела укључиле сајбер отпорност, друштвену кохезију и стратешке комуникације, чиме је проширен његов концептуални обухват. Посебну пажњу заслужују концепти тоталне одбране балтичких држава у контексту прилагођавања савременом безбедносном окружењу. Балтичке државе усвојиле су свеобухватан приступ националној одбрани. Летонија је већи нагласак ставила на образовање јавности, док је Литванија приоритет дала развоју међународне сарадње. Естонија је била најуспешнија у примени свеобухватног приступа одбрани (Jordan 2024). Она је усвојила такозвану дистрибуирану отпорност (*distributed resilience*), која интегрише информационо-комуникациони сектор и цивилно друштво (Tikk, Kaska and Vih 2010).

Савремена литература наглашава да се тотална одбрана најбоље разуме кроз два комплементарна концепта: институционалну координацију (*whole-of-government*) и друштвену мобилизацију (*whole-of-society*). Балтичке државе, између осталих, интегришу све друштвене подсистеме – политички,

економски, информациони и безбедносни – у заједничку архитектуру отпора (Jordan 2024, 315). Мали безбедносни системи не могу да надокнаде стратешке слабости количином наоружања, већ синтезом својих ресурса у функционалан систем одбране. То је основни принцип на којем почива тотална одбрана у савременом стратешком окружењу.

Доминантни теоријски приступи концепту тоталне одбране заснивају се на ангажовању и државних институција и друштва у целини. Концепт на тај начин има кључну улогу у кредибилитету националне одбране и одвраћања. Ови приступи утемељени су и у теорији војне стратегије. У савременим доктринама тотална одбрана постала је тесно повезана са појмовима отпорности (*resistance*) и еластичности (*resilience*) (Grigalashvili 2023, 240). Холингов концепт адаптивне цикличности показује да сложени системи могу да опстану апсорбујући поремећаје, реорганизујући структуру и задржавајући функционалност (Walker et al. 2004). У студијама безбедности, ова теорија развијена је кроз приступе који отпорност дефинишу као *способност система да се припреми, реагује, опорави и адаптира* (Linkov, Trump and Hynes 2019). Отпорност није само физичка или инфраструктурна, већ и психолошка и културна категорија. Друштво мора бити способно да издржи притиске кризе без урушавања вредносне структуре и воље за отпором.

С друге стране, рад Лоренса Фридмана (Lawrence Freedman) (2013) смешта тоталну одбрану у шири оквир *стратегије одвраћања у условима ограничених ресурса*. Тотална одбрана омогућава мањим државама да повећају цену агресије за потенцијалног нападача посредством друштвене мобилизације, отпора окупацији и дугорочне дефанзивне стратегије. У контексту стратешких концепата малих држава, њихов највећи ресурс јесте предвидљива организациона архитектура која омогућава брзо реаговање и минимизира почетну штету.

Надаље, савремена литература све чешће тумачи тоталну одбрану кроз призму теорије комплексности. Савремене претње имају мултидоменску структуру, што значи да не следе линеарну логику класичног ратовања. Бузан и Вивер (Buzan and Waever 2003) тврде да је безбедност „структурно распршена“ у различитим секторима; војном, политичком, економском, друштвеном и сајбер простору. У таквом систему национална одбрана постаје мрежно организована, а сви подсистеми државе међусобно зависни. Отказивање једног домена може изазвати системске ефекте, нарочито у случају дигиталних претњи које се развијају брже од традиционалних институционалних капацитета за реаговање. То

подразумева да тотална одбрана у 21. веку више није традиционални модел мобилизације, већ динамички систем адаптивног одговора.

На крају, разматрање улоге вештачке интелигенције као трансформационог фактора у теоријском концепту тоталне одбране уводи нову димензију овог концепта. Док ранији теоријски приступи државу посматрају као примарног носиоца отпора, доба вештачке интелигенције помера тежиште ка технолошкој инфраструктури као подједнако важном стратешком фактору. Вештачка интелигенција трансформише саме основе командовања и управљања увођењем предиктивних способности, аутономне детекције и алгоритамског доношења одлука. Међутим, исти аутори упозоравају да некритичко увођење вештачке интелигенције ствара нове рањивости, укључујући алгоритамску пристрасност, сајбер зависност и структурну изложеност непоузданим подацима. У том смислу, у раду се заступа став да вештачку интелигенцију пре треба разумети као структурни фактор тоталне одбране, него као алат који се накнадно додаје постојећим моделима. Интеграција вештачке интелигенције помера концепт ка „алгоритамској отпорности“, дефинисаној као способност система да предвиди, апсорбује и прилагоди се ризицима посредством динамичке анализе података. Интеграција вештачке интелигенције у традиционални концепт тоталне одбране подиже га на нови ниво и може представљати основу онога што аутори дефинишу као „тоталну одбрану 2.0“.

Стратешка логика концепта „тотална одбрана 2.0“

Стратешка логика у савременом безбедносном окружењу представља интелектуални оквир који повезује политичке циљеве, расположиве ресурсе и динамику оперативног окружења у јединствени, кохерентни систем деловања. Она почива на идеји да стратегија не може бити низ изолованих одлука, већ мора имати унутрашњу рационалност и „граматику“ која објашњава зашто одређени приступ функционише у условима комплексних, хибридних и технолошки посредованих претњи. Како истиче Греј (Gray 1999), стратегија је одржива само када постоји јасна логичка узрочно-последична веза између политике, војне моћи и начина њене употребе. Слично томе, Фридман (Freedman 2013) наглашава да стратегија у модерном добу функционише као „наративна логика“ која обједињује циљеве, методе и перцепције актера. У ери брзих технолошких промена и вештачке интелигенције, стратешка логика постаје још важнија

јер омогућава да се сложени подаци, мултидоменска реалност и несигурност преточе у одржив и адаптиван модел деловања.

Концепт тоталне одбране, који је након завршетка Хладног рата делимично изгубио на значају, поновно је постао актуелан током друге деценије 21. века. Како су поједини теоретичари приметили, стари рецепти примењују се на нове претње. На пример, након Хладног рата Шведска је напустила даљи развој свог модела тоталне одбране и усмерила се на јачање управљања ванредним ситуацијама и способности за експедиционе војне операције, што је био типичан приступ већине европских држава. Обновљено интересовање за претходни модел подстакле су промене у регионалном безбедносном окружењу настале услед агресивне руске политике. Сходно томе, Шведска је 2019. године спровела анализу и изнела предлоге у документу под називом *Отпорност – концепт тоталне одбране и развој цивилне одбране 2021–2025*. Тај документ представља прву фазу ревитализације концепта тоталне одбране, односно његове нове верзије 2.0, како је разматрано у тексту *Шведска тотална одбрана* Варшавског института (Warsaw Institute 2018). Посебан нагласак стављен је на јачање отпорности на хибридне претње. Централни циљ документа јесте јачање способности друштва да самостално функционише током првих дванаест недеља кризе или потенцијалног рата. Предложене мере предвиђају мобилизацију свих грађана и прелазак на ратни режим живота, организације и рада. Концепт се заснива на претпоставци да сваки грађанин има индивидуалну улогу и одговорност, при чему су свакодневне активности прилагођене подршци функционисању друштва у време кризе или рата. *Табела 1* приказује класификацију и еволуцију стратешког приступа шведском концепту тоталне одбране (Angstrom and Ljungkvist 2024, 517).

Табела 1. Шведске стратегије тоталне одбране, 1948–2022.

		Руковођење и командовање	
		<i>децентрализовано</i>	<i>централизовано</i>
Цивилно-војне улоге	<i>Одвојене</i>	„Ћелија“(1948–1972)	„Димњак“(1972–1993)
	<i>Интегрисане</i>	„Тврђава“(2014–2022)	„Кластер“(1994–2014)

Извор: Аутори; према: Angstrom and Ljungkvist 2024, 517

Табеларни приказ еволуције модела руковођења и командовања, у корелацији са односом цивилних и војних улога, указује на поступну трансформацију безбедносног управљања од институционалне сегментације ка функционалној интеграцији. Рани модел „ћелије“ (1948–1972), заснован на децентрализованом командовању и јасно одвојеним цивилно-војним надлежностима, обезбеђивао је високу отпорност система, али по цену ограничене стратешке кохерентности. Насупрот томе, модел „димњака“ (1972–1993) уводи централизовано руковођење уз задржану институционалну подвојеност, што је допринело ефикаснијој контроли, али и појави функционалних „силоса“ и слабе међусекторске координације. Постхладноратовски период карактерише модел „кластера“ (1994–2014), који кроз интеграцију цивилних и војних улога у централизованом систему омогућава већу синхронизацију политика и операција, али истовремено повећава зависност од центра одлучивања. Коначно, модел „тврђаве“ (2014–2022) одражава адаптацију на хибридне претње и мултидоменско окружење, комбинујући интегрисане цивилно-војне капацитете са децентрализованим командовањем, чиме се јача оперативна флексибилност и системска отпорност, уз изазов очувања јединственог стратешког управљања.

Непосредно након шведских мера, у новој студији анализиран је концепт тоталне одбране 2.0 у контексту балтичког региона. Поред различитих мера усмерених на унапређење концепта, посебан нагласак стављен је на развој научних и технолошких заједница, економије и одбрамбене индустрије. Концепт наглашава улагања у технологије као део укупних капацитета одбране и друштвене отпорности, укључујући повећање производње критичних производа, дронове, вештачку интелигенцију, робусне сајбер способности и исплативе свемирске технологије. Мера у којој нордијске државе координишу и деле користи од ових технологија са балтичким партнерима непосредно ће унапредити регионалну отпорност и укупну ефикасност тоталне одбране (Saxi, Sundelius and Swaney 2020, 13).

Џоунс и Лав (Jones and Love 2022) увели су 2022. године концепт „еластичност и отпорност 2.0“ (*Resilience and Resistance 2.0*), тврдећи да он служи као катализатор јачања друштвене отпорности и отпора инвазији и потенцијалној окупацији ревизионистичких сила. Ослањајући се на искуства почетне фазе сукоба у Украјини, аутори су указали на потребу за континуираном проценом и унапређивањем мера тоталне одбране. Наглашавају значај мобилизације друштва у целини под руководством владе. Развој одговарајућег институционалног оквира у миру представља

основу за успешно спровођење концепта у рату. Сви владини програми морају бити легитимни и јасно разумљиви и јавности и државним институцијама. Истовремено, они морају потенцијалном непријатељу упутити кредибилну поруку одвраћања (Jones and Love 2022). Овај приступ представља унапређени концепт тоталне одбране настао као одговор на кризу. Ако се правилно примени, он може повећати отпорност нације и одвратити агресију.

Ван Варк (Van Vark 2025) разматра концептуалне разлике међу државама чланицама Организације Северноатлантског уговора (*NATO - North Atlantic Treaty Organization*) у погледу концепта тоталне одбране. Предлог генералног секретара НАТО-а Марка Рутеа (*Mark Rutte*) да се војна потрошња повећа на 3,5% БДП-а, уз додатних 1,5% намењених јачању друштвене отпорности и инфраструктуре, сигнализира обновљену посвећеност Алијансе одбрани не само територије већ и демократских вредности друштва држава чланица. Овај двоструки нагласак на војним способностима и општој друштвеној припремљености подсећа на модел „тоталне одбране“ који се дуго примењује у нордијским државама (Van Vark 2025). Оживљени модел финансирања друштвене отпорности, а тиме и јачања способности Алијансе да одговори на нове безбедносне изазове, показује да концепт тоталне одбране наставља да еволуира у складу са променама глобалног безбедносног окружења. На тај начин постаје јасно да војна моћ сама по себи није довољна за одбрану државе и да национална одбрана мора бити заједничка одговорност друштва у целини. Ревитализовани концепт треба да осигура да друштва, државе и савезници делују синхронизовано, структурно и функционално у односу на потенцијалног непријатеља.

Може се закључити да концепт „тоталне одбране 2.0“ представља природну еволуцију класичног концепта тоталне одбране, прилагођену савременом мултидимензионалном безбедносном окружењу. Док традиционални концепт тоталне одбране првенствено интегрише војне и цивилне ресурсе ради супротстављања непосредној агресији, верзија 2.0 проширује овај приступ укључивањем нових технологија и мултидоменске перспективе. Те технологије огледају се пре свега у примени вештачке интелигенције, сајбер безбедности и напредних система наоружања и војне опреме. Истовремено, друштвена отпорност захтева развој системских капацитета који омогућавају цивилним и јавним институцијама да функционишу под различитим видовима притиска, укључујући поремећаје основних услуга, здравства, критичне инфраструктуре и јавне свести. Посебан изазов представљају хибридне

претње које комбинују сајбер и когнитивне операције, економску принуду и геополитичку манипулацију – димензије које класична тотална одбрана није систематски разматрала.

На крају, мултидоменски приступ, заснован на интеграцији нових оперативних домена као што су свемир и сајбер простор, омогућава координацију у физичком, информационом и дигиталном простору, што доводи до динамичнијег и флексибилнијег одбрамбеног става. Тотална одбрана 2.0 није само војна или цивилна стратегија, већ холистички модел отпорности државе и друштва, у којем технологија и интелектуални капитал постају кључни чиниоци превенције криза и одговора на њих.

Трансформација три нивоа и тотална одбрана 2.0 у добу вештачке интелигенције

Нови изазови са којима се концепт тоталне одбране суочава у добу напредних технологија, мултидоменског ангажовања снага и средстава, асиметричних претњи и хибридног ратовања захтевају подједнако свеобухватан и интегрисан одговор. Традиционални концепт тоталне одбране, који се првенствено ослањао на војну компоненту, док је цивилни сектор имао улогу подршке, више није довољан за одговор на савремене безбедносне изазове. Због тога се у овом раду концепт тоталне одбране 2.0 усваја као нужан одговор. Интеграција вештачке интелигенције у систем безбедности не представља само технолошку надоградњу, већ дубоку трансформацију концепта тоталне одбране. Ова трансформација обухвата промене на три међусобно повезана нивоа: структурном, функционалном и друштвеном. Иако су ова три нивоа већ уграђена у северноевропске моделе тоталне одбране, тек са појавом вештачке интелигенције добијају кохерентну системску динамику која институције одбране и безбедности, националну инфраструктуру, критичне ресурсе и друштво интегрише у јединствену архитектуру алгоритамске отпорности.

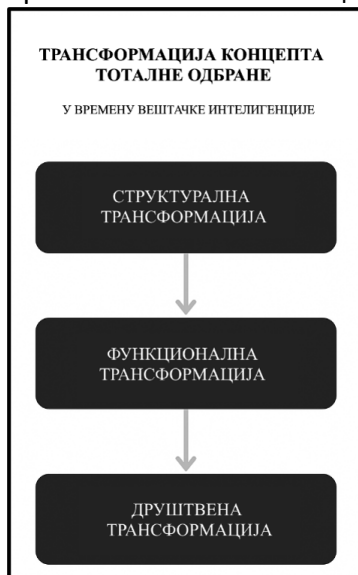
Трансформација концепта на ова три нивоа треба да обезбеди алгоритамску отпорност нације, државе или савеза, чиме се успоставља нови приступ спровођења концепта. Алгоритамска отпорност означава способност државе, њених институција и друштва да користе вештачку интелигенцију, анализу великих података и аутоматизоване процесе предвиђања, апсорбовања, прилагођавања и опоравка од сложених мултидоменских претњи. У добу експоненцијалног технолошког напретка,

отпорност више није само организациона или инфраструктурна категорија, већ и алгоритамска способност која омогућава системима да уче, анализирају и проактивно реагују на кризе у настајању. Истраживања реаговања на кризе и вештачке интелигенције показују да алгоритамски модели могу значајно унапредити рано откривање ризика и подићи ниво системске отпорности (Ilcic, Fuentes and Lawler 2025), док се напредак генеративне вештачке интелигенције у сајбер безбедности све више посматра као кључни фактор заштите критичне инфраструктуре и очувања друштвене стабилности (Radanliev, Santos and Ani 2025).

У оквиру тоталне одбране 2.0, алгоритамска отпорност представља интегративни механизам који повезује војни, цивилни, сајбер и когнитивни домен у јединствен систем националне безбедности. Она омогућава откривање хибридних претњи пре њихове ескалације, аутоматску стабилизацију институција под притиском и подршку доносиоцима одлука посредством предиктивних модела и когнитивне аналитике. На тај начин алгоритамска отпорност трансформише тоталну одбрану 2.0 из реактивног модела одбране у проактиван, динамичан и адаптиван систем способан да функционише у реалном времену.

Као што је приказано на *Слици 1*, трансформацију треба разумети као низ јасно дефинисаних фаза. Прва фаза обухвата структурне промене на нивоу друштва, државе и савеза. Овај први ниво обезбеђује основу за даљи развој и поставља темељ унапређеног концепта тоталне одбране. Након успостављања оптималне структуре система, следећа фаза јесте функционална трансформација. Нове и напредније функције треба да обезбеде ефикасније коришћење расположивих ресурса и оптимизују реаговање на свим нивоима, од појединца до друштва у целини. Способности које пружају технологије попут вештачке интелигенције од суштинског су значаја за овај процес. Коначно, трећи ниво представља друштво које разуме, познаје и прихвата нове токове у области безбедности.

Слика 1. Трансформација концепта тоталне одбране
у ери вештачке интелигенције



Извор: Илустрација аутора

Свака држава представља сложен систем, без обзира на то да ли је реч о малој, средњој држави или великој сили. Структура таквог система сама по себи је сложена. Међутим, добра институционална структура не гарантује нужно ефикасно функционисање система. То значи да функционални ниво мора представљати природну надоградњу добро структуриране државе, засновану на јасној расподели надлежности и ресурса. Последњи ниво, који се односи на друштво, можда је и најосетљивији. Без јавног прихватања и разумевања функција државних структура нема кохезије у систему. То представља један од најважнијих изазова у примени концепта тоталне одбране. Неразумевање улога појединаца, група, правних лица, великих државних система и других релевантних актера главни је извор недоследности у процесима планирања, организовања и остваривања концепта тоталне одбране. Један од потенцијалних извора кохезије јесте широка примена ресурса вештачке интелигенције на сва три нивоа трансформације разматрана у овом раду. Управо су структурна, функционална и друштвена трансформација концепта тоталне одбране неопходне за увођење вештачке интелигенције у овај концепт.

Вештачка интелигенција може се разумети као структурни трансформатор који треба да обезбеди нову логику управљања одбраном, али и да допринесе актуелизацији, оптимизацији и активацији парадигме предвидети–спречити–одговорити (*predict–prevent–respond*). У суштини, моћ алгоритма треба да постане централни део управљачке (*command & control*) инфраструктуре. Поред бројних предности, оваква надоградња доноси и већ познате ризике и ограничења, који су повезани са вештачком интелигенцијом. То су напади противничких система (*adversarial attacks*), манипулација подацима (*data poisoning*), аутоматизација одлука и етички ризици. У овом раду посебан нагласак стављен је на структурни фактор као елемент трансформације, док су функционални и друштвени фактори анализирани у мањој мери.

Структурна трансформација

Структурни ниво трансформације односи се на институционални концепт, нормативни оквир, поделу надлежности и способност државе да координише цивилне и војне ресурсе. Основу функционисања државе чине структура њених институција, органа власти и ресурса. Способност заједничког деловања у оквиру додељених надлежности ради остваривања најважнијих националних интереса и циљева представља најважнији императив. Структура је, такође, у основи концепта тоталне одбране. У традиционалним моделима Скандинавије, Израела и Швајцарске ова архитектура била је материјална, инфраструктурна и кадровска. Са вештачком интелигенцијом, она постаје информациона, мрежно структурирана и динамички адаптивна.

Европска унија (ЕУ), у документу *План трансформације одбрамбене индустрије (EU Defence Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defence Readiness)* из 2025. године, нагласила је значај брзине, агилности и процене ризика за одбрану. У документу се, такође, наводи да је ЕУ потребна темељна промена начина размишљања и процедура наслеђених из прошлости на свим нивоима, од држава чланица и индустрије, до институција ЕУ. Истакнути су структурни изазови као један од кључних фактора трансформације модела нове одбрамбене политике „*New Defense*“ која је заснована на лекцијама из Украјине и потенцијалу револуционарних технологија у домену одбране (ЕС 2025, 7).

Араја и Кинг (Araya и King 2022, 4), разматрајући утицај вештачке интелигенције на одбрану и безбедност, наводе да она представља структурну трансформацију природе националне безбедности. Студија

указује на потребу за већим усмерењем на развој и интеграцију напредних и трансформативних технологија, укључујући сајбер мреже и аутономне системе. Основу структуре таквих система чини вештачка интелигенција. Према Стајнму (Steinmo 2010), савремене државе функционишу као сложени адаптивни системи (*complex adaptive systems*). У свом истраживању он разматра трансформацију државе у политичкој, економској и друштвеној димензији.

Структурни фактор трансформације обухвата широк спектар активности од одбране базиране на развијеној индустрији, до алгоритамске архитектуре у којој институционални капацитет зависи од способности учења и предвиђања на основу података. Увођење вештачке интелигенције у концепт тоталне одбране отвара могућност за предиктивну процену ризика, управљање кризом у реалном времену, аутоматизовану анализу рањивости критичне инфраструктуре, оптимизацију логистике, мобилизације и подршке цивилног друштва. НАТО (NATO 2024) у својим концептима „цивилне спремности“ (*civil preparedness*) све више истиче потребу на отпорности заснованој на подацима (*data-driven resilience*), што структурни ниво тоталне одбране поставља у дигитални контекст. Истовремено, државе попут Финске и Естоније развијају моделе у којима је вештачка интелигенција део целовитог националног одбрамбеног система, укључујући сајбер команде, дигиталну идентификацију и координацију. Тако се структура тоталне одбране трансформише из система фиксних организацијских линија у архитектуру алгоритамски подржане интеграције, где је кључни ресурс податак.

Поред наведеног структурни фактор у трансформација концепта тоталне одбране подразумева прелазак са традиционалне, статичке и материјално оријентисане архитектуре ка динамички адаптивној, мрежној и алгоритамски подржаној структури. Процес се може разложити у неколико фаза. Прва фаза обухвата мапирање постојеће структуре, у којој треба да се идентификују институције, капацитети, ресурси и надлежности. Потом се процес наставља анализом критичних тачака у координацији цивилних и војних снага. Посебан поступак у овој фази треба да буде процена дигиталног и информационог капацитета државе, односно количине података који се прикупљају и обрађују и степена њихове употребе у процесу одлучивања. У другој фази потребно је да се изврши дефинисање нових принципа организације, односно нова или измењена структура. Та нова структура би требало да омогући прелазак на мрежну и алгоритамски подржану архитектуру, где је кључни ресурс информација. На овај начин би систем могао да учи и да на основу расположивих података даје процене

доносиоцима одлука у реалном времену. Последњи сегмент у овој фази би била потпуна интеграција цивилних, војних и приватних ресурса у један координисан систем.

Трећа фаза захтева је кључна у контексту алгоритамске отпорности; представља технолошку интеграцију. Реализује се увођењем вештачке интелигенције у управљање ризицима, сајбер безбедност, логистику, мобилизацију и подршку цивилном друштву. Ово се у пракси постиже развојем аутономних и аутоматизованих система који доприносе брзини и флексибилности. Последњи сегмент ове фазе би била креирање стандарда који би омогући координацију свих актера, како на националном нивоу, тако и шире. Четврта фаза би требало да тестира прилагођавање институционалних капацитета, пре свега кроз промене у организационом дизајну. Овде би морало да организационе јединице буду тестиране као што су напредни центри одлучивања, дигиталне команде, јединице за анализу података, и други напредни системи подржани вештачком интелигенцијом. После сегмента тестирања уследиле би промене у нормативном оквиру, које би обезбедиле флексибилне протоколе, бржи механизми одлучивања, легитимност интеграције нових актера. Последњи сегмент ове фазе би обухватили обука и развој људских ресурса за рад са технологијама и алгоритамским системима.

Претходно наведене четири фазе структурне трансформације се не завршавају имплементацијом већ је то само један циклус процеса који треба да представља стално тестирање, итерације надоградње и константно изучавање. Све то би довело до сталног унапређења алгоритама, процеса и институционалне структуре. Претходно наведено имплицира да структурна трансформација је процес који је константно траје, али и да суштински представља основну фазу у процесу трансформације концепта тоталне одбране.

Функционална трансформација

Функционални фактор у контексту трансформације концепта тоталне одбране али и спровођења алгоритамске отпорности представља оквирни механизми деловања и формат вертикалне интеграција система. Функционална трансформација тоталне одбране у добу вештачке интелигенције односи се на убрзану еволуцију процеса анализе, координације и оперативног деловања. Док су традиционални системи тоталне одбране били засновани на реактивном приступу, у коме институције одговарају на већ манифестоване ризике, интеграција алгоритамских система омогућава

постепени прелаз ка моделу у коме се криза идентификује и неутралише много пре него што постане оперативна претња. Као што показује Болман (Bollmann 2021) у студији о дигиталној трансформацији скандинавских одбрамбених структура, процеси командовања и управљања постали су зависни од потпуно нових облика повезивања података, сензорских система и предиктивних модела, који убрзавају темпо одлука и преобликују начин функционисања безбедносних механизма.

У скандинавским моделима тоталне одбране, дигитализација је већ довела до тога да вештачка интелигенција постане интегрални део свакодневних активности, од анализе ситуационе свести до координације цивилно-војних структура. Нови системи функционишу као „дигитални посредници“ (Guo and Zhang 2026) који обједињују податке из енергетских мрежа, јавних служби, сајбер система и војних платформи, стварајући функционалну целину који аутори описују као мрежно омогућену спремност (*network-enabled readiness*) (Khaledi and Saifoddin 2023). На тај начин класични модел, који је био зависан од хијерархијских линија командовања, се трансформише у мрежни систем који може да мења и прилагођава приоритете и правце деловања у реалном времену.

Предиктивна аналитика представља кључни аспект ове функционалне трансформације. Како показују истраживања о дигитализацији и управљању кризама у нордијским државама, алгоритми могу да анализирају токове информација од друштвених мрежа до сензорских система и да идентификују ризике у настајању, што омогућава да се ресурси усмеравају пре него што криза ескалира (Wrangle, Bengtsson and Brommesson 2024). Ово је значајна новина у односу на класичну тоталну одбрану, у којој систем реагује тек након што је претња испољена.

Мултидоменска повезаност постаје још једна карактеристика функционалне трансформације. Израелски модел дигитализоване одбране, описан у више отворених анализа, показује како системи засновани на машинском учењу интегришу обавештајне, оперативне и логистичке домене у јединствену платформу, што из корена мења оперативну функционалност и брзину реакције (Aravantinos 2024). На овај начин, вештачка интелигенција не постаје само технолошки додатак постојећим структурама, већ функционално „језгро“ које омогућава да у реалном времену повезује цивилне службе, војне структуре и критичне инфраструктуре.

Додатни функционални аспект односи се на информациону и когнитивну одбрану. У анализама естонског модела, системи за рано откривање дезинформација, анализу емоционалних трендова и

препознавање координираних кампања постају стандард у савременим концептима тоталне одбране (Tererik et al 2022). Овде вештачка интелигенција делује као системска заштита која штити когнитивну безбедност друштва и институција.

У целини, функционална трансформација тоталне одбране у добу вештачке интелигенције представља прелаз са статичких, вертикалних и реактивних механизма на динамичке, мрежно организоване и предиктивно оријентисане системе деловања. У најширем смислу функционални ниво обухвата механизме деловања као што су мобилизацију, командовање, управљање кризама, комуникацију, логистику, инфраструктурну заштиту и операције у информационом, сајбер и когнитивном простору. Вештака интелигенција мења овај ниво кроз аутоматизацију, оптимизацију и интелигентно повезивање процеса.

Друштвена трансформација

Друштвена трансформација представља најсложенију и најдубљу димензију савремене тоталне одбране. Основни задатак ове трансформације изградња друштвене кохезије и унапређење алгоритамске културе безбедности. Док функционална и структурна трансформација описују промене у институционалним и оперативним механизмима, друштвена трансформација одражава промене у култури, вредностима, обрасцима понашања и односима између државе и грађана. Отпорност друштва није искључиво институционални капацитет, већ пре свега друштвена норма која се гради свесном безбедносном политиком и културом колективне одговорности.

У скандинавским и балтичким моделима, друштвена отпорност све више се заснива на дигиталној компетентности, транспарентности институција и поверењу грађана у механизме националне безбедности. Како показује Антес (Anthes 2015) у анализи Естоније, грађани постају активни учесници безбедносног система не кроз класичну мобилизацију, већ кроз учешће у дигиталним сервисима, сајбер вежбама и заједничким платформама за обраду информација. Овим се мења класични модел друштвене мобилизације: грађани не постају само корисници одбране, већ интегрални део њене когнитивне и информационе структуре.

Културна димензија ове трансформације огледа се у томе што дигитална писменост постаје нова основа безбедносне културе. У Естонији, Финској и Шведској, дигитална компетентност третира се као предуслов за

разумевање савремених ризика од дезинформација до сајбер операција. Развој ових компетенција не служи само индивидуалној безбедности грађана, већ и јачању укупне друштвене отпорности. Истраживање о цивилно-војној сарадњи у Шведској показује да управо поверење у институције и поверење у дигиталне системе представља темељ успешног деловања тоталне одбране (Tillberg, Berndtsson and Tillberg 2025).

У друштвеном смислу, вештачка интелигенција уводи нову димензију поверења. Поверење у алгоритме, њихову транспарентност и механизме надзора над њима постаје подједнако важно као и поверење у јавне институције. Ако се алгоритми доживљавају као непрозирни или пристрасни, могу нарушити легитимитет целокупног система одбране. Литература о стратешкој култури наглашава да државе ограничених капацитета морају градити културу безбедности у којој технологија и институције узајамно јачају поверење, док грађани активно учествују у заједничком систему отпора (Agustanto, Runturambi and Puspitasari 2025).

У целини, друштвена трансформација тоталне одбране у добу вештачке интелигенције подразумева развој културе у којој грађани, институције и алгоритамски системи делују у јединственој архитектури. Израелски концепт „наоружаног друштва“ (*society in arms*), скандинавски модел „народне одбране“ и балтичка идеја „дигиталног држављанина“ (*digital citizenship*) заснивају се на претпоставци да је друштвена мобилизација кључна за вишеслојну отпорност. Уместо класичног модела „друштва под оружјем“, развија се модел „друштва у алгоритму“, где грађани постају активни учесници когнитивне и информационе отпорности, а поверење постаје стратешки ресурс националне безбедности.

Допринос концепту тоталне одбране Републике Србије

Предлог унапређеног модела концепта тоталне одбране Републике Србије мора да буде заснован на реалним капацитетима државе, док истовремено следи принципе алгоритамске отпорности који су већ видљиви у успешним нордијским, балтичким и израелским оквирима. Полазећи од специфичности српског безбедносног окружења, цивилно-војне инфраструктуре и нивоа дигиталне трансформације друштва, модел тоталне одбране мора бити постављен као интегрисана архитектура која обједињује државне институције, приватни сектор, академску заједницу и грађане у јединствен систем отпорности. Овај модел не треба да буде копија страних

решења, већ прилагођавање најбољих пракси које су потврђене у нордијском и балтичком региону на услове Србије, имајући у виду њену неутралност, геополитички положај, политички и правни поредак.

Кључна претпоставка новог модела мора да буде то да тотална одбрана није само механизам реакције на кризе, већ систем непрекидне заштите. Србија већ поседује делове оваквог система у оквиру сектора безбедности, обавештајних служби, цивилне заштите и инфраструктурних оператора, али они делују фрагментирано, са ограниченом разменом података и различитим нивоима дигитализације. Увођење вештачке интелигенције може да омогући премошћавање ових институционалних подела стварањем интегрисаног „друштвено-безбедносног екосистема“ који функционише на основу предиктивне анализе и динамичке координације.

Први елемент предложеног модела би било одређивање институције у чијој надлежности би био развој и имплементација овог концепта. Постојећи модел који предвиђа надлежност Министарства одбране, сасвим извесно не може обезбедити савремени приступ тоталној одбрани по моделу ангажовања читавог друштва (*Whole of Society Approach*). Успостављање Националног центра за развој концепта тоталне одбране, који би функционално био орган Владе са јасно дефинисаним надлежностима и ресурсима, омогућило би интеграцију и представљао својеврсно чвориште за усмеравање деловања државних и друштвених капацитета. Центар не би био само техничка институција, већ аналитичко-командна структура слична финском NCSC-FI (*National Cyber Security Centre Finland*) или естонском CERT-EE (*Küberintsidentide käsitlemine CERT-EE*). Био би задужен за прикупљање података из више сектора — војног, политичког, информационог, енергетског, телекомуникационог, јавног здравља, сајбер домена и образовања, ради изградње јединственог националног оквира ситуационе свести. Србија има административни капацитет да формира овакво тело, јер већ постоје институције као што су Канцеларија за информационе технологије и е-Управу, Регулаторно тело за електронске комуникације и поштанске услуге (РАТЕЛ), Сектор за ванредне ситуације Министарства унутрашњих послова, али је неопходно њихово структурно повезивање.

Други елемент односи се на увођење вештачке интелигенције у подршци цивилно-војне координације, што је кључна лекција из шведског и норвешког модела. Србија формално има развијене механизме цивилно-војне сарадње, али они углавном функционишу у контексту ванредних ситуација. У добу вештачке интелигенције ова координација мора постати континуирана, заснована на алгоритамским системима који прате статус ресурса, људства, критичне инфраструктуре и комуникационих токова. Ово

би омогућило да се механизми одбране активирају без кашњења, а структура одлучивања постане флексибилнија. Систем интеграције вештачке интелигенције развијао би се у складу са представљеним концептом структурних, функционалних и друштвених фактора.

Трећи елемент модела односи се на изградњу националне когнитивне одбране, која представља најосетљивији сегмент алгоритамске отпорности. Србија је последњих година изложена дезинформацијама, сајбер нападима, политичким утицајима и кампањама које циљају јавни дискурс. У складу са искуствима Естоније, неопходно је развијати систем који комбинује алгоритамску детекцију манипулативних садржаја, брзу реакцију државних институција и програме едукације. Овде је посебно важно повезати медијске куће, научне институте и безбедносне структуре у мрежу која функционише као национални филтер когнитивне безбедности. Србија већ поседује капацитете у овој области, али они нису централизовани нити формално интегрисани у оквир одбране.

Четврти елемент је развој етичког, правног и регулаторног оквира који ће омогућити безбедну примену вештачке интелигенције. У том смислу, Србија се може ослонити на искуства ЕУ, Међународне телекомуникационе уније (*International Telecommunication Union – ITU*) и Организације Уједињених нација за образовање, науку и културу (*United Nations Educational, Scientific and Cultural Organization – UNESCO*), али и прилагодити правила специфичностима своје безбедносне културе. Кључно је дефинисати протоколе одговорности, стандарде транспарентности и механизме надзора над алгоритамским системима како би се спречиле злоупотребе и изградило поверење грађана. Без ове димензије, чак и најбољи технички систем остаје без друштвене легитимности.

Пети елемент односи се на улогу приватног сектора, који је неизоставан у свим модерним моделима тоталне одбране. Србија има развијену индустрију информационо-телекомуникационих технологија (ИКТ), растући број „стартапа“ и више универзитета који се баве машинским учењем. Сви ови актери морају бити укључени у архитектуру одбране као партнери, а не као спољни ентитети. Фински и естонски модели показују да приватни сектор постаје носилац кључних сегмената алгоритамске инфраструктуре, од сајбер заштите до предиктивних система. Србија има капацитет да развије сличан приступ уз институционалну подршку и финансирање кроз циљане програме.

На крају, предложени модел тоталне одбране Србије треба да буде заснован на идеји да је отпорност друштва нераскидиво повезана са

технологијама које се брзо развијају. Уместо да се ослања на класичне концепте мобилизације, нови модел треба да развија алгоритамски подржане механизме сарадње, предвиђања и заштите, који ће омогућити Србији да одговори на сложене ризике савременог безбедносног окружења. Овим приступом Србија може да изгради систем који није само адаптиван, већ и стратешки флексибилан, и који уместо реаговања нуди проактивно управљање безбедношћу.

Закључак

Рад полази од тезе да убрзани развој вештачке интелигенције суштински трансформише концепт тоталне одбране, померајући га са класичног цивилно-војног модела ка интегрисаном систему алгоритамске отпорности. Анализом теоријских оквира, као и компаративних искустава нордијских и балтичких држава, показано је да тотална одбрана у 21. веку више не може бити схваћена искључиво као механизам реакције на оружану агресију, већ као динамички, мултидоменски и друштвено укорењен систем управљања ризицима.

Кључни резултати рада указују да вештачка интелигенција не делује само као технолошка подршка постојећим одбрамбеним структурама, већ као структурни фактор који мења саме основе организације, функционисања и правне уређености концепта тоталне одбране. У том смислу, увођење концепта алгоритамске отпорности омогућава прелазак са реактивне на проактивну логику одбране, у којој се претње идентификују, анализирају и неутралишу пре него што ескалирају у отворену кризу.

Анализа три нивоа трансформације – структурног, функционалног и друштвеног – указује да је одрживост тоталне одбране 2.0 условљена њиховим истовременим и усклађеним развојем. Структурна трансформација обезбеђује институционалну и нормативну основу, функционална трансформација омогућава ефикасно деловање у реалном времену, док друштвена трансформација обезбеђује легитимитет, поверење и кохезију без којих ни најнапреднији алгоритамски системи не могу бити делотворни.

Посебан допринос рада огледа се у формулисању предлога унапређеног модела тоталне одбране Републике Србије, заснованог на принципима савремене успешне праксе алгоритамске отпорности, али

прилагођеног националним специфичностима, институционалним капацитетима и геополитичком положају државе. Предложени модел указује на неопходност интеграције државних институција, приватног сектора, академске заједнице и грађана у јединствен систем, у којем подаци, алгоритми и људски ресурси делују синхронизовано.

Истовремено, рад указује и на ограничења и ризике примене вештачке интелигенције у области тоталне одбране, укључујући питања алгоритамске пристрасности, сајбер рањивости, етичке одговорности и очувања демократске контроле. Управо из тог разлога, алгоритамска отпорност не сме бити сведена на технократски пројекат, већ мора бити праћена јасним правним оквиром, транспарентношћу и континуираном едукацијом читавог друштва.

Може се констатовати да тотална одбрана 2.0 представља еволутивни одговор на комплексне безбедносне изазове савременог доба, у којем се границе између мира и рата, физичког и дигиталног, државе и друштва све више бришу. У том контексту, вештачка интелигенција постаје кључни катализатор нове стратешке логике одбране, али њена ефективност зависи од способности државе да је интегрише у кохерентан, легитиман и друштвено прихваћен систем.

Будућа истраживања требало би усмерити на емпиријску анализу имплементације алгоритамске отпорности, развој индикатора њене ефикасности, као и на компаративна проучавања различитих националних модела у контексту регионалне и колективне безбедности. На тај начин, концепт тоталне одбране може да настави свој развој као релевантан и одржив одговор на изазове безбедности у добу вештачке интелигенције.

Превод са енглеског на српски језик: аутори

Dr. Veljko Blagojević's part of this paper present findings of a study developed as a part of the research project "Serbia and challenges in international relations in 2026", financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade, during the year 2026.

Bibliography / Библиографија

- Agustanto, Pulung, Arthur Josias Runturambi, and Puspitasari. 2025. "Potential Cultural Strategy for Preventing National Resilience from Terrorism in Indonesia". *Enrichment: Journal of Multidisciplinary Research and Development* 3 (3): 601–615.
- Angstrom, Jan, and Kristin Ljungkvist. 2024. "Unpacking the varying strategic logics of total defence". *Journal of Strategic Studies* 47 (4): 498–522. DOI: <https://doi.org/10.1080/01402390.2023.2260958>.
- Anthes, Gary. 2015. "Estonia: A model for e-government". *Communications of the ACM* 58 (6): 18–20. DOI: <https://doi.org/10.1145/2754951>.
- Aravantinos, Elias. 2025. "The Fusion of Technology and Defense: Israel's Military-Technology Complex". *Strategy International*. November 21. <https://strategyinternational.org/2024/11/21/publication150/>.
- Araya, Daniel, and Meg King. 2022. *The Impact of Artificial Intelligence on Military Defence and Security*. Waterloo: Centre for International Governance Innovation.
- Bollmann, Anders Theis. 2021. "Danish Defense Transformation and the Technopolitics of Relevant Military Contributions". *Scandinavian Journal of Military Studies* 4 (1): 62–77. DOI: <https://doi.org/10.31374/sjms.60>.
- Buzan, Barry, and Ole Waever. 2003. *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.
- [EC] European Commission. 2025. EU Defence Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defence Readiness, COM(2025) 845 final. Brussel, Communication from the Commission to the European Parliament and the Council. November 19. https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf.
- Freedman, Lawrence. 2013. *Strategy: A History*. London: Oxford University Press.
- Gray, Colin S. 1999. *Modern Strategy*. Oxford: Oxford University Press.
- Grigalashvili, Vepkhvia. 2023. "Total Defence: A Comprehensive Approach to National Defence Governance". *International Journal of Scientific and Management Research* 6 (5): 240–248.
- Guo, Shesen, and Ganzhou Zhang. 2026. "Chronicling transitions in Baltic media: a longitudinal topic analysis of The Baltic Times' coverage from the post-

- Soviet era to European integration (1998–2024)”. *Journal of Baltic Studies* 57 (2): 423–454. DOI: <https://doi.org/10.1080/01629778.2025.2587631>.
- Ilcic, Andrés, Miguel Fuentes, and Diego Lawler. 2025. “Artificial intelligence, complexity, and systemic resilience in global governance”. *Frontiers in Artificial Intelligence* 8: 1562095. DOI: <https://doi.org/10.3389/frai.2025.1562095>.
- Jones, Derek, and Bryant Love. 2022. “Resilience and Resistance 2.0: initial lessons of Ukraine and the implications of resilience and resistance efforts to deter and respond to invasion and occupation by revisionist powers”. *Bezpieczeństwo. Teoria i Praktyka* XLVIII (3): 21–40. DOI: <https://doi.org/10.48269/2451-0718-btip-2022-3-001>.
- Jordan, Józef W. 2024. “Evolution of the concept of total defence in the Baltic”. *Rozprawy Społeczne/Social Dissertations* 18 (1): 315–344. DOI: <https://doi.org/10.29316/rs/188761>.
- Khaledi, Arian, and Amirali Saifoddin. 2023. “Three-stage resilience-oriented active distribution systems operation after natural disasters”. *Energy* 282: 128360. DOI: <https://doi.org/10.1016/j.energy.2023.128360>.
- Linkov, Igor, and Benjamin D. Trump. 2019. *Risk, Systems and Decisions*. Cham: Springer.
- Linkov, Igor, Benjamin D. Trump, and William Hynes. 2019. *Resilience-based Strategies and Policies to Address Systemic Risks*. September 9. [https://one.oecd.org/document/SG/NAEC\(2019\)5/en/pdf](https://one.oecd.org/document/SG/NAEC(2019)5/en/pdf).
- [NATO] North Atlantic Treaty Organization. 2024. “Resilience, civil preparedness and Article 3”. November 13. <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- Noyes, Alexander, and Jesse R. Humpal. 2025. “Why the US needs a total defense strategy based on resilience”. *Brookings*. October 21. <https://www.brookings.edu/articles/why-the-us-needs-a-total-defense-strategy-based-on-resilience/>.
- Radanliev, Petar, Omar Santos, and Uchenna Daniel Ani. 2025. “Generative AI cybersecurity and resilience”. *Frontiers in Artificial Intelligence* 8: 1568360. DOI: <https://doi.org/10.3389/frai.2025.1568360>.
- Saxi, Håkon Lunde, Bengt Sundelius, and Brett Swaney. 2020. “Baltics Left of Bang: Nordic Total Defense and Implications for the Baltic Sea Region”. *Strategic Forums*. January. <https://digitalcommons.ndu.edu/strategic-forums/9/>.
- Simpson, Jacob, Rudolph Oosthuizen, Sondoss El Sawah, and Hussein Abbass. 2021. “Agile, Antifragile, Artificial-Intelligence-Enabled, Command and Control”. *arXiv*: 2109.06874. DOI: <https://doi.org/10.48550/arXiv.2109.06874>.

- Steinmo, Sven. 2010. *The Evolution of Modern States: Sweden, Japan, and the United States*. New York: Cambridge University Press.
- Sundelius, Bengt, and Jan Eldeblad. 2023. "Societal Security and Total Defense: The Swedish Way". *PRISM* 10 (2): 92–111.
- Teperik, Dmitri, Solvita Denisa-Liepniece, Dalia Bankauskaitė, and Kaarel Kullamaa. 2022. *Resilience Against Disinformation - A New Baltic Way to Follow?*. Tallinn: International Centre for Defence and Security.
- Tikk, Eneken, Kadri Kaska, and Liis Vih. 2010. *International Cyber Incidents: legal considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE).
- Tillberg, Lotta Victor, Joakim Berndtsson, and Peter Tillberg. 2025. "Navigating Collaboration: Understanding Civil-Military Interactions in Swedish Total Defence From a Security Network Perspective". *Scandinavian Journal of Military Studies* 8 (1): 40–56. DOI: <https://doi.org/10.31374/sjms.288>.
- Van Vark, Annelies. 2025. "NATO: total defence 2.0". *Leiden University*. June 23. <https://www.leidenlawblog.nl/articles/nato-total-defence-2-0>.
- Walker, Brian, C. S. Holling, Stephen R. Carpenter, and Ann Kinz. 2004. "Resilience, Adaptability and Transformability in Social–ecological Systems". *Ecology and Society* 9 (2): 5. DOI: <https://doi.org/10.5751/ES-00650-090205>.
- Warsaw Institute. 2018. "The Swedish 'Total Defence'". June 15. <https://warsawinstitute.org/swedish-total-defence/>.
- Wrange, Jana, Rikard Bengtsson, and Douglas Brommesson. 2024. "Resilience through total defence: Towards a shared security culture in the Nordic–Baltic region?". *European Journal of International Security* 9 (4): 511–532. DOI: <https://doi.org/10.1017/eis.2024.15>.