Czech Republic: EU and NATO member
The security of EU and NATO member states comes first
Date of publication: June 1, 2026

CENTRAL CYBER SHIELD OF DEMOCRACY

Cyber rearmament of EU and NATO member states is a fundamental prerequisite for fulfilling alliance commitments, as the global hybrid war of the 21st century takes place in both physical and digital space simultaneously and with each passing day poses a growing threat to democratic civilization and increases the risk of escalating security crises and armed conflict.

CENTRAL CYBER SHIELD OF DEMOCRACY

“The most dangerous and destructive threats in the world are attacks on shared values and mutual trust, without which the family, society, state and international order disintegrate.”

The central cyber shield forms the basic pillar of the new security architecture for the EU and NATO member states. Without it, it will not be possible to fulfill the alliance commitments that require the immediate cyber rearmament of democratic countries, because the global hybrid war of the 21st century, which European and world statesmen have long warned about, is taking place in the physical and digital worlds simultaneously. For this reason, it is necessary to address security threats in both dimensions simultaneously and in a coordinated manner, because hybrid threats penetrate the physical world through cyberspace and have such a destructive potential that they can fundamentally disrupt and, in extreme cases, destroy member states even before an armed conflict breaks out.

EU AND NATO MEMBER STATES

The security of EU and NATO member states requires fulfilling alliance commitments in the physical world and in cyberspace simultaneously, with cyber rearmament through a central cyber shield and balanced funding of both domains being a necessary condition.

The Central Cyber Shield represents an extremely important, comprehensive and long-term alliance strategy, which was created on the basis of seventeen years of systematic research, interdisciplinary analyses and practical verification. However, given its complexity and scope, it cannot be realistically expected that its technical essence and strategic mechanisms will be fully understood by the usual political or advisory structures, since their security policy is focused mainly on the physical space. However, this political and security imbalance between the physical and digital dimensions is gradually worsening the security of EU and NATO member states, as hybrid attacks on democracy are continuous and lead to the disintegration of democratic civilization and the escalation of armed conflict, while military attacks have not yet taken place.

The majority of political leaders have no idea what atrocities and atrocities are taking place in cyberspace. The democratic world is not at all prepared for their existence or their catastrophic impacts. As a result of the global hybrid war of the 21st century, unleashed by authoritarian regimes, a digital underworld gradually emerged, in which millions of people involved in various forms of cybercrime operate today . Their activities have a devastating impact on collective defense, shared values, and mutual trust, on which the security and cohesion of the family, society, EU and NATO member states, and the entire international order are based. As a result, the risk of serious security crises, the escalation of which can even result in armed conflicts, increases daily. One possible solution could be the activation of the Central Cyber Shield, which took seventeen years to develop and whose main goal is to strengthen the defense of the democratic world against these threats.

This is not a lack of professional skills of political representatives, advisors, analysts and many other authorities, but a natural systemic limitation of their capacities, as they have to ensure a very wide range of other agendas. Therefore, the protection of democracy in cyberspace, international security and the management of society and the state in the digital era cannot be considered a normal part of political activity, as it is a large and highly complex area of cyber security policy. For this reason, the establishment of an International Alliance Council is necessary, whose task will be to prepare the conditions for the activation of the Central Cyber Shield and coordinate the process of cyber rearmament for the purpose of collective protection of EU and NATO member states in cyberspace, as a prevention of armed conflict.

The uniqueness of the alliance strategy of the Central Cyber Shield lies in the fact that it is based not only on theoretical knowledge and expert analyses, but also on long-term practical

experience gained in confronting a risky and conflict environment. It was precisely in these conditions that it was necessary to develop the capabilities of adaptation, crisis decision-making, threat identification and the creation of preventive defense mechanisms. On this basis, a comprehensive system of preventive, defense and stabilization measures was subsequently created across the security, technological, institutional, economic and geopolitical levels.

The Central Cyber Shield was built primarily to create conditions for the fulfillment of alliance commitments of EU and NATO member states in cyberspace, because these commitments can no longer be fulfilled in physical space alone in the digital age. Cyberspace has become an integral part of collective defense, and underestimating it would threaten the security, defense capability, and stability of democratic states.

International Alliance Council – guarantor of fulfillment of alliance commitments in cyberspace

---

The establishment of the International Alliance Council is considered a historic step, as the fulfillment of alliance commitments of the European Union and NATO member states requires their fulfillment not only in the physical world, but also in cyberspace. The International Alliance Council is therefore established to oversee and coordinate the fulfillment of these commitments within the framework of the process of cyber rearmament, thereby contributing to strengthening the protection of democratic civilization, the collective defense of member states in cyberspace, international security and the prevention of the escalation of armed conflicts.

Events in cyberspace increasingly affect the security, social, economic, environmental and legal stability and future of the member states of the European Union and NATO. Without the existence of the International Alliance Council, the fulfillment of the alliance commitments of the member states of the European Union and NATO would therefore be critically endangered in the current security environment, as the physical and digital spaces are interconnected through hybrid threats that enable the transfer of risks and attacks from cyberspace to the physical world.

The International Alliance Council will become a key institutional body for the implementation of alliance commitments by the member states of the European Union and NATO precisely because of the historically fundamental changes in the security environment of the 21st century, when a significant part of the digital space in which social, political and public communication takes place is not fully under the direct control of states, but is managed by private technology companies or regimes with centralized control over their own cyber capabilities. This asymmetry increases the vulnerability of the security infrastructure of member states and complicates the coordinated implementation of alliance commitments, especially in the context of the growing importance of hybrid threats that connect cyberspace with the physical security environment.

Institutional structure of the International Alliance Council

In order to be able to fulfill alliance commitments not only in the physical world but also in cyberspace simultaneously, it is essential that the institutional structure of the International Alliance Council be built on a multi-level governance model that connects the political, strategic, executive and operational levels.

The highest decision-making body of the International Alliance Council would be the Assembly of the Heads of Government of the democratic member states of the European Union and NATO, which would approve strategic priorities, security objectives and key decisions related to the implementation of alliance commitments in cyberspace. The executive representative of the Council would be the Secretary General, responsible for political and strategic management, coordination of international cooperation and implementation of approved decisions. The Secretary General would be supported by an executive committee composed of alliance representatives of the member states, whose task would be to prepare strategic decisions, coordinate their implementation and oversee the process of cyber rearmament. The key operational component of the Council would be the Cyber Command, responsible for planning, coordinating and managing joint activities in the field of collective defense in cyberspace, activating the Central Cyber Shield and responding to cyber and hybrid threats.

CENTRAL CYBER SHIELD OF DEMOCRACY

Ladislav Boldi – **Author and guarantor of the Central Cyber** Shield of Democracy. The security of EU and NATO member states requires fulfilling alliance commitments in both physical and cyberspace simultaneously.

Institutional background:
Digital Policy Institute - Millennium 3000

- Founder of the social network Politinn - the first European new generation platform
- Founder of the ONLINE DEMOCRACY mobile application
- Founder of the democratic celebrations and the prestigious "Democratic Personality of the Year" awards
- Author of the concept of " disinfocracy ", the most destructive hybrid regime of the 21st century that is erasing democracy from our minds.

Biography: Ladislav Boldi

Ladislav Boldi grew up in extremely harsh conditions. After his biological mother abandoned him shortly after birth, he spent 19 years in foster care, where he faced brutal violence, torture, inhuman treatment, indescribable suffering and a daily struggle for survival. After his release from foster care, he was forced to live on the streets as a homeless person, as the state and authorities refused to provide him with any assistance, and without an identity document, he effectively did not exist in the system.

In order to survive on the street, which eventually became his only home, he was forced to eat expired or rotten food and leftovers from garbage cans and accept offers to fight in the streets for fifteen crowns, which provided him with at least a basic livelihood. These activities were not the result of a choice, but the only means of survival. He saved his life only because he gradually learned to solve problems and conflict situations in conditions of direct threat to his life. Despite the cruelty of fate, he decided to put his experience to good use for the benefit of society and the state. He invested all his efforts and savings in education. At the age of 40, he graduated from high school via distance learning and subsequently graduated from a university in the field of public and international relations. Thanks to his deep experience in conflict environments, in 2015 he developed the concept of “social terrorism”, the aim of which was to warn EU and NATO member states against the radicalization of citizens on social networks, which in some cases can have more serious consequences than armed conflict.

The threats that Ladislav Boldi has been drawing attention to for a long time, however, do not only concern social terrorism, but also the gradual decline in trust in democratic institutions as a result of hybrid threats emerging in the digital space, the impacts of which are manifested in growing security and social tension. In the environment of global migration processes, he also draws attention to the fact that their organization and coordination are increasingly taking place in cyberspace, which fundamentally changes the nature of these phenomena and requires their solution at this level. At the same time, he emphasizes the phenomenon known as "digital cancer", which represents a serious threat to the psychological stability of the population in the digital age, associated with an increase in digital violence, stress, depression, suffering, social isolation and overall weakening of mental health, especially in the younger generation. However, his proposals, projects, security strategies and expert recommendations were rejected by politicians and journalists because of his past and poor social background.

Ladislav Boldi did not give up, and despite the long-term rejection of him by those around him, he continued for more than 17 years in the systematic development of the Central Cyber Shield, the aim of which is to enable the member states of the European Union and NATO to begin the process of cyber rearmament as a necessary prerequisite for fulfilling alliance commitments in both dimensions of the current security environment. It is for this purpose that the Central Cyber Shield was created as a collective defense tool also in the digital space, since security threats in the conditions of the global hybrid war of the 21st century operate simultaneously in the physical and cyber spheres, which leads to a continuous escalation of security risks and an increase in the probability of armed conflict.

Structures are developing in cyberspace that are described in analytical and security terminology as the digital underworld, which gradually emerged as a result of the global hybrid war of the 21st century. This digital underworld today includes various forms of cybercrime , organized crime and other criminal activities, which represent one of the most significant security threats of the digital era. It was Ladislav Boldi's many years of personal experience in a conflict environment that led him to build an alliance strategy, the result of which is the Central Cyber Shield - the most technologically advanced security system aimed at protecting EU and NATO member states and democratic civilization.

Boldi's proposals and concepts in the fight against and defense against the global hybrid war of the 21st century should therefore be judged solely by their content, quality, vision, and contribution to the EU and NATO member states, not by his past, for which he is de facto not responsible. In addition, the best and most durable security strategies are never created in political debates, conference rooms, or in an administrative environment over coffee, but from direct experience in a conflict environment and when confronted with a real threat. Only a life-threatening confrontation with evil will reveal which procedures really work, which fail, and which strategies are able to withstand critical situations and under extreme pressure. Practical experience gained in a conflict environment thus becomes a key source of knowledge for the creation of modern security doctrines.

Life and professional profile of Ladislav Boldi : ***"Those who slandered, defamed, humiliated, discriminated, ridiculed, condemned and turned their backs on me should know that every path I took, every bad experience, everyone I went through something with, and everything I ever did – all of this ultimately proved that I was walking in the right direction. And only***

thanks to this did I manage to build a lot of good and lasting things for society and for the state."

THE END OF TRADITIONAL POLITICS – THE RISE OF AI POLITICS IN EU AND NATO MEMBER STATES

The member states of the European Union and NATO are entering a historic transformation period that will fundamentally change the protection and governance of society, the functioning of the state, and the form of democracy in the digital era. Traditional politics, focused primarily on the governance of the physical world, gradually cease to fully correspond to the reality of the 21st century, in which a significant part of social, political, economic, and security communication is moving into cyberspace.

Traditional political models in EU and NATO member states are currently facing an extremely difficult situation, unable to adequately respond to the speed of technological development and the dynamics of the digital environment. As a result, an imbalance is emerging in the governance of society and the state, which threatens not only the security of member states, but also their ability to fulfill alliance commitments. Security is a fundamental prerequisite for the stable functioning of democracy, effective state administration and the protection of the public interest.

Although the member states of the European Union and NATO have made significant progress in the digitalization of public administration, security and defense, they have practically forgotten about building a democratic infrastructure for the functioning of society and the state in cyberspace. This critical deficiency today threatens the balanced management of society and the state in both physical and digital space and at the same time weakens the ability of democratic countries to face the security challenges of the 21st century. Building a fully-fledged democratic environment in cyberspace is therefore one of the most important tasks of the coming decades, because it will determine the collective defense of democratic states, the building of central protection mechanisms, the strengthening of cyber resilience and the gradual transition from traditional politics to AI politics based on the principle of ONLINE DEMOCRACY.

AI policy represents a new model of governance of society and the state based on the use of artificial intelligence operating systems that will be able to analyze large volumes of data in real time, evaluate the needs of citizens, model the impacts of public policies, propose optimal solutions, support decision-making processes and coordinate the performance of public administration. These systems will integrate economic, security, social, educational, health, transport, energy, environmental and other strategic areas into a single data environment that will enable continuous optimization of the functioning of the state. As a result of a higher degree of automation of decision-making and administrative processes, there will also be a

significant reduction in the need for human capacity in all areas of political management, public administration and related administrative structures, including the number of political, clerical and other executive roles, to the extent that it will enable a more autonomous functioning of the governance system of society and the state.

AI policy will be safe and democratically legitimate only if it is based on an already built digital democratic infrastructure, on the principle of which ONLINE DEMOCRACY will function. In practice, this means that democratic processes must not only be supported by new technologies, but directly structured and anchored in the digital environment, where they become a full-fledged part of state governance. Without these conditions, it will not be possible to effectively and responsibly govern the state in a balanced way in both physical and digital space, and politicians will not be able to fulfill alliance commitments.

AI politics will operate on the principle of ONLINE DEMOCRACY, based on a digital democratic infrastructure built in accordance with the highest security and technological standards for the protection and development of democracy in cyberspace. This model will fundamentally transform the functioning of the political system and create new forms of interaction between citizens, politicians and public administration, including the emergence of e-voters, e-candidates and other digital tools of democratic participation. At the same time, a new principle of shared power between citizens and the state will emerge within AI politics. Citizens will be increasingly involved in decision-making processes through digital democratic platforms, they will be able to continuously express their needs and interests, participate in the creation of public policies and resolve selected issues in real time. This process represents one of the most significant changes in the democratic system since the emergence of representative democracy, as it will enable a more direct connection between citizens and the exercise of public power.

In order to effectively fulfill alliance commitments in the digital era, as is expected, a profound transformation of all traditional politics towards AI politics operating on the principle of ONLINE DEMOCRACY will be necessary, including the transition of traditional political parties to AI political parties. Only under the assumption of balanced management of society and the state in both physical and digital space can the ability to fulfill these commitments responsibly be ensured.

Unless there is an immediate transformation of traditional political parties into AI political parties and a systematic building of digital democratic infrastructure for the development of ONLINE DEMOCRACY, which is a basic prerequisite for a new security architecture, EU and NATO member states face extremely serious consequences, including:

- Loss of ability to fulfill NATO alliance commitments.
- The breakdown of social and state governance as a result of hybrid attacks on democracy.
- The collapse of the functioning of public administration due to the inability to transform from traditional politics to AI politics.
- A threat to the democratic order itself and its basic principles.
- Weakening of the legitimacy of the state and loss of its authority in the eyes of citizens.
- The collapse of trust in democracy, political leaders and public institutions.

- The growing and difficult-to-control expansion of organized crime and criminal structures of the digital underworld, which form an integral part of the global hybrid war of the 21st century.
- Destabilization of the security, political and social balance of EU and NATO member states.
- Threats to digital statehood, sovereignty, national identity and legitimacy of states in cyberspace.
- Massive spread of disinformation, propaganda and manipulation of public opinion, often supported by AI systems.
- Loss of the ability to distinguish between lies and truth in personal, professional and public life.
- An explosion of information chaos and societal disorientation.
- Accelerated polarization of society and deepening conflicts of opinion.
- Radicalization of individuals and groups in the online environment (social terrorism) with spillover into the real world.
- An increase in frustration, anger and hatred leading to the weakening of interpersonal relationships.
- Erosion of social cohesion and disruption of ties between states.
- Transfer of digital conflicts into physical space, including the risk of violent clashes.
- Increasing security tensions and the emergence of new forms of extremism.
- Manipulation of electoral processes and influencing voting behavior.
- Destabilization of electoral systems and weakening of their credibility.
- Disruption of equality of political competition.
- Reducing the transparency of decision-making processes.
- Concentration of power in technological and data structures.
- Misuse of data for political and power purposes.
- Strengthening the influence of foreign actors on the internal politics of EU and NATO member states.
- Intensification of hybrid attacks on democratic institutions of EU and NATO member states.
- Automation of AI propaganda and its mass dissemination in cyberspace.
- The emergence of closed information bubbles and fragmentation of public discourse.
- The weakening of traditional media and their controlling role as a result of the global hybrid war of the 21st century.
- The rise of data-driven populism and emotional manipulation of AI politics.
- Deepening citizens' dependence on technological platforms and AI systems.
- The inability of institutions to respond to rapid technological developments in the world.
- The collapse of coordination between the digital and physical levels of state power.
- Weakening of the state's strategic management capabilities in the conditions of the global hybrid war of the 21st century.
- Erosion of the ability of EU and NATO member states to carry out basic decision-making and budgetary processes.
- Threat to the economic, social and legal stability of states, including their long-term prosperity and development of EU and NATO member states.

The Central Cyber Shield was conceived as a strategic tool for this exceptionally challenging transformation period. The threats mentioned and their consequences simultaneously

represent clear evidence that without the timely establishment of an AI policy based on the principle of ONLINE DEMOCRACY and a digital democratic infrastructure, the system of governance of society and the state in the EU and NATO member states may gradually disintegrate, which would fundamentally weaken the ability of democratic institutions to ensure security, stability, effective state governance and the fulfillment of alliance commitments. The task of the Central Cyber Shield is therefore not only to protect the democratic system from hybrid threats, but also to create conditions for the fastest and safest possible transition from traditional politics to AI politics operating on the principle of ONLINE DEMOCRACY, which will enable balanced governance of society and the state in both physical and digital space and strengthen the ability of EU and NATO member states to responsibly fulfill their security, value, legal and alliance commitments.

Politicians of the European Union and NATO member states are reaching the limits of their security capacities, as they cannot effectively address new hybrid and cyber threats within state structures alone. Key technological ecosystems, digital platforms, data infrastructure and innovation capacities are largely owned and managed by the private sector. Without visionaries, strategists and experts from the private sector, they remain helpless and cannot cope on their own with such fundamental challenges as the global hybrid war of the 21st century, the comprehensive analysis of which took almost 17 years. It is these authorities who have the technological know-how focused on building a digital democratic infrastructure and the ability to create and implement strategic solutions. Therefore, without addressing them and actively involving them, it is impossible to build a modern security architecture of the 21st century or ensure the collective defense of the EU and NATO member states.

The United States and China have been engaged in a long-term massive technological and investment development focused on building vast digital ecosystems encompassing global internet platforms, social networks, cloud infrastructures, artificial intelligence, semiconductors, quantum technologies, robotics, autonomous systems, and especially cybersecurity and sophisticated data services. Both superpowers are aware that technological dominance means economic, security and geopolitical power, and therefore they are concentrating huge financial, research and strategic capacities precisely on technological development. Their strength lies in the very close connection of the private sector and state support, the speed of decision-making and the ability to immediately transfer technological innovations to a global scale. At the same time, they systematically support technological visionaries, innovators, strategic system developers and creators of modern security and cyber solutions, because they are aware that these people represent the key to future power, stability and global influence. They create exceptional conditions for research, development, investment and implementation of technological projects, on which the security of states, the functioning of economies and the stability of modern society increasingly depend. Thanks to this, they today determine the pace of development of artificial intelligence, social platforms, data systems, modern security technologies and cyber strategies, which fundamentally affect the functioning of the entire world. Technological primacy has become for them not only a question of economy, but above all a question of strategic influence, power and the ability to shape the future shape of global society in the digital age.

In contrast, in the field of technology and innovation, Europe has long encountered a combination of an extensive system of regulations, directives, orders, prohibitions and administrative restrictions that slow down and complicate the development of the innovation

environment. Proposals for building comprehensive security architectures, including central cyber defense systems, are often postponed or deliberately blocked in the early stages of the political process in the European environment due to institutional fragmentation, power priorities and, in some cases, clientelistic ties at the level of EU Member States, the European Parliament and the European Commission.

In the European institutional framework, political functions have traditionally been prioritized over the implementation of technological, innovative and strategic projects, including large-scale scientific, technological and security initiatives, as well as over the systematic support of technological visionaries, innovators and experts in modern cyber and security systems from the private sector. This structural preference of political roles over technological development creates the risk that international projects essential for the digital security of EU and NATO member states will not be fully implemented, even though their long-term strategic and security stability across key areas of public and political life depends on them. This structural development gradually leads to a weakening of Europe's competitiveness in the global technological space, to a deepening dependence on external technological solutions from the United States and China, and to a de facto lagging behind in areas where Europe could be among the world leaders with a more effective institutional setup.

It is important for political leaders in the EU and NATO member states to clearly distinguish between two different concepts of democracy protection. While the European Democracy Shield is built primarily on the principle of digital regulations, legislative guidelines and support for pro-democracy organizations defining the boundaries of permissible content and is intended only for the member states of the European Union, the mission of the Central Cyber Shield is not to regulate anything. Its principle lies in building and developing a political, security, value and legal system that protects and strengthens trust not only between allies but also within democratic societies, thereby directly contributing to increasing the defense capabilities of alliance structures, strengthening information resilience and reducing the vulnerability of member states to hostile influence.

No democratic society will ever develop socially, economically or technologically effectively under the massive onslaught of excessive laws and power ambitions that create a conflict environment in the EU and NATO member states. Democracy can only survive if society is educated on shared values, building mutual trust and strengthening social cohesion, not on the basis of power management through increasing laws, prohibitions and orders, as is increasingly applied not only in the physical, but now also in the digital space. Therefore, it is necessary to activate the central cyber shield and with its help build a modern digital democratic infrastructure that will enable the protection and development of democracy on the principle of shared values, social stability and mutual trust in both worlds — physical and digital — simultaneously.

The Central Cyber Shield is an international integrated security system that should become a new pillar of the security architecture of the European Union and NATO member states, as there is no comparable mechanism of similar scope and conceptual solution in current global security practice. Its seventeen-year development has led to the construction of a digital democratic infrastructure based on ten alliance security pillars that integrate the most modern capabilities for responding to the global hybrid war of the 21st century.

If steps towards the establishment and activation of the Central Cyber Shield are not initiated in a timely manner, the fulfillment of alliance commitments will be seriously jeopardized. Without mutual trust, the alliance, cohesion, and a functional collective defense system cannot be maintained in the long term, which would lead to the gradual weakening of democratic institutions and the stability of the member states of the European Union and the North Atlantic Treaty Organization.

DEMOCRATIC WORLD IN THE FLAMES OF THE GLOBAL HYBRID WAR OF THE 21ST CENTURY

In the digital world, the roof of the democratic house is burning, but no regulations, analyses, directives, bans, or orders can extinguish this fire.

The roof of the democratic house is burning in the digital space, but few people notice this disaster. This state of affairs is a direct consequence of the ongoing global hybrid war of the 21st century, of which the digital underworld is an integral part, where there is an uncontrollable growth of organized crime, social terrorism in the form of radicalization of citizens on social networks, cyber attacks on democracy, as well as digital violence, tyranny, slavery, abuse and many other forms of escalating crime and cyber threats.

While the European Union and NATO are focusing on analyzing why this fire started and who caused it, in the meantime these abominations and atrocities are spreading massively in cyberspace and are being transferred to the physical world through criminal structures, including authoritarian regimes. These abominations and atrocities generate hundreds of billions to trillions of dollars in profits annually, threatening not only member states but also democratic civilization itself and causing massive economic damage. In the fight against the global hybrid war of the 21st century, which is perceived as one of the greatest threats, as it takes place in both worlds, physical and digital, a possible systemic solution appears to be the activation of a central cyber shield – the most technologically advanced defense system in the context of current international security threats.

The fate of democracy in EU and NATO member states depends on the Central Cyber Shield .

Website:
https://www.cyberneticshieldofdemocracy.eu

Alliance Strategy 2026: Cyber rearmament through the Central Cyber Shield as a tool for the necessary fulfillment of alliance commitments of EU and NATO member states in cyberspace.

The Czech Republic may submit a proposal to open a debate on the fulfillment of alliance commitments at the NATO summit on 7–8 July 2026 in Ankara on the implementation of alliance commitments, which are currently primarily assessed according to the level of defense spending in the physical space. However, this approach no longer fully corresponds to the current development of the international security environment, because alliance commitments must also be fulfilled in cyberspace, which has become a key part of the security and defense reality of the 21st century, in modern conditions. Despite the ongoing discussions about its role in the collective defense system, the Czech Republic declares its readiness not only to fulfill these commitments, but also to actively participate in their modernization by submitting a strategic proposal in the form of the Central Cyber Shield concept, which is understood as one of the key pillars of the new EU and NATO security architecture. The current global hybrid war of the 21st century is taking place simultaneously in both physical and digital space, which is fundamentally changing the nature of security threats. For this reason, it is necessary to initiate a process of cyber rearmament of democratic states, which will enable an effective response to hybrid threats, security risks and international conflicts in their digital and physical form. Only in this way can a coordinated approach be ensured to protect stability and prevent the daily increase in the risk of escalation of armed conflicts.

CYBER-REAR ARMING AND ITS FINANCING AS THE BASIS OF A MODERN SECURITY ARCHITECTURE

Cyber rearmament is a long-term strategic investment in the digital security, resilience and stability of EU and NATO member states, which is of a fundamentally preventive nature. Its key principle is that investment in cyber rearmament will gradually reduce the future need for spending on conventional military infrastructure, as it will strengthen conflict prevention, increase the ability to respond promptly to hybrid threats and significantly contribute to reducing the escalation of international tensions and the risk of armed conflict.

Cyber rearmament represents a comprehensive set of international political, security, technological and legal measures that create space for building a stable value and institutional framework of cyberspace. It includes the construction of a digital democratic infrastructure in cyberspace, which will enable the development of the concept of ONLINE DEMOCRACY - the first political system operating in the digital world. At the same time, it will strengthen the digital sovereignty, identity and legitimacy of EU and NATO member states in cyberspace and protect their digital statehood, including democratic and national integrity.

A crucial area will also be defense against the global hybrid war of the 21st century, which penetrates from cyberspace into the physical world in the form of the spread of disinformation, hate propaganda, and manipulation of public opinion, and poses a high risk of escalating international tensions and armed conflicts.

Cyber rearmament is also a crucial element of the security architecture, on which the stability and future security of EU and NATO member states in the modern world actually depend. In the current environment, traditional dimensions such as airspace or territorial integrity alone can no longer be considered sufficient protection, because for the first time in history, security threats are occurring in parallel in the physical and digital worlds at the same time. Cyberspace has become an equal operational environment in which conflicts are formed, escalated and transferred to the real world. For this reason, cyber defense is crucial for the very fate of the security stability of states.

An integral part of the Central Cyber Shield should be the concept for building a cyber army of EU and NATO member states. This would form its key operational and implementation element and represent the future basic capacity for building, operating and long-term development of the entire cyber defense system, including its ongoing functioning and ability to respond to dynamically evolving threats in the digital space.

It is necessary to start from the fact that undemocratic regimes such as China, Russia, Iran and others have long had state-controlled and organized cyber armies and structures that they systematically use to conduct hybrid operations. These operations include, in particular, the building of a digital underworld, disinformation campaigns, hate propaganda , manipulation of the information environment, cyberattacks and other forms of action with direct impacts on the physical world.

In this context, a fundamental question arises as to whether it is possible to fully and long-term fulfill alliance security obligations in the conditions of the ongoing global hybrid war of the 21st century without building comparable defense capacities at the EU and NATO levels.

General Jean-Pierre Perrin said in an interview with Seznam Zprávy: "Perceiving a threat does not mean scaring someone. It is about building self-confidence. Every day, the North Atlantic Alliance faces deliberate provocations, hybrid and, above all, cyber attacks from Russia. The line between peace, crisis and conflict has never been as thin as it is today." The fundamental building block of self-confidence is trust. However, it is currently gradually dissolving and disappearing - not only within democratic societies, where people are losing faith in the principles and functioning of democracy, but also between the member states of the European Union and the North Atlantic Alliance. This dangerous trend can have catastrophic impacts on the very essence of the alliance, which is a key pillar of the alliance's security and a necessary prerequisite for effective defense in the modern world. Unfortunately, this pillar is not yet fully embedded in the security architecture, and therefore, in the interests of international security, its priority is to strengthen it through the activation of the Central Cyber Shield within the framework of a modern 21st century security infrastructure.

The proposed distribution of security investments represents the optimal strategy for a modern 21st century security architecture for the EU and NATO:

1. **2.5% of GDP for the activation of the Central Cyber Shield:** This strategic investment is key to the systematic defense against the global hybrid war of the 21st century, taking place in the physical and digital worlds simultaneously. Its goal is to protect the political, security, value and legal system, mutual trust and shared values, including the protection of digital statehood, sovereignty, national identity and legitimacy of the state in cyberspace, as well as the protection of critical infrastructure and state institutions from coordinated hybrid threats.
2. **2.5% of GDP for military infrastructure:** This part of the funding ensures the development of conventional defence capabilities, including airspace protection, land and maritime defence, ensuring the physical territorial integrity and sovereignty of Member States, as well as the development of strategic and operational capacities of the armed forces of EU and NATO Member States.

As part of the necessary cyber rearmament of the European Union and NATO member states, funding must be distributed evenly and balanced to ensure a true balance and a common level of resilience across the entire Alliance, as hybrid threats originating from cyberspace can reach such intensity in the modern environment that they can fundamentally disrupt and, in extreme cases, completely destroy member states even before an armed conflict breaks out.

If the United States decides to condition security guarantees within the North Atlantic Treaty Organization and the activation of Article 5 on the fulfillment of commitments of 5% of GDP, it will be necessary to strategically reassess this approach. It would be much more prudent to extend this principle to the so-called “digital Article 5”, directly based on the Cyber Strategy 2026 of US President Donald Trump. In a key passage, it states: “Freedom and security in cyberspace must not be taken for granted. Adversaries and cybercriminals use cyberspace to spread authoritarianism, suppress democracy, and weaken our national and economic security.” Cyber Strategy Donald Trump's 2026 thus opens a direct path to the activation of

the Central Cyber Shield, which protects democracy and ensures maximum security for NATO and EU member states.

NATO Deputy Secretary General Jean-Charles Ellermann-Kingombe made a memorable statement that also paves the way for the introduction of a "digital Article 5" in cyberspace: "NATO is expected to be able to fight and protect itself on land, in the air and at sea, but also in space and in cyberspace. All of these domains have a digital foundation that is vulnerable to cyber attacks. Cyber protection is therefore central to all dimensions of preparation for modern warfare and is essential for armed forces. We need to build a digital backbone. We need to put in place procedures to share huge amounts of data and train the people who will operate the new systems. So there are a lot of things that we need to do – and we need to do them quickly."

The Central Cyber Shield will be a unique system that will provide a so-called complete security service for EU and NATO member states. This means a continuous and uninterrupted provision of protection, coordination and reaction capabilities in the digital space within a single interconnected and managed entity. This service will represent a unified security support mechanism across member states and will become a key element of the modern security architecture of the EU and NATO. [1, 2, 3, 4, 5, 6, 7, 8, , 9, 10, 11, 12, 13,14]

WARNING

The democratic world must start taking action instead of debating, regulating, prescribing and analysing!

Hybrid attacks against democratic civilisation are already reaching such an intensity and scope that without the activation of the central shield, there is a real threat of the gradual disintegration of families, societies, the Member States of the European Union and NATO, and the very foundations of the international order.

The Member States of the European Union and NATO find themselves in a situation where their biggest problem is no longer the lack of information about hybrid threats, but endless debates, slow decision-making, excessive bureaucracy, complex approval processes

and the long-term prioritisation of theories, analyses, studies, assessments and consultations over decisive actions. In the environment of the ongoing global hybrid war of the 21st century, inaction, postponements and administrative delays are becoming a strategic advantage for the enemy and the doom of democratic civilisation. While hybrid threat actors, including authoritarian regimes, are conducting long-term and continuous attacks against EU and NATO member states and democratic civilization, representatives of democratic governments often only debate, analyze the situation and adopt new regulations or guidelines. However, these steps alone will not stop the attackers or deter them from hostile actions.

Every wasted second that hybrid threat actors use to attack democratic states jeopardizes the fulfillment of alliance commitments, increases security risks for democratic civilization and reduces the collective defense capability of the EU and NATO.

CONTENTS

Section 1

What is the greater threat - the 21st century global hybrid war or armed conflict?

The global hybrid warfare of the 21st century, unleashed by authoritarian regimes, has gradually given rise to a digital underworld in which millions of individuals are now involved in various forms of cybercrime . Their activities have a devastating impact on the collective defense, shared values, and mutual trust upon which the security and cohesion of the family, society, EU and NATO member states, and the international order depend.

There are a number of compelling reasons why political authorities in democratic states, representatives of the European Union, NATO member states and international organizations should thoroughly reassess current security priorities. At the same time, they should ask themselves a fundamental strategic question: What poses a greater threat to EU and NATO member states and democratic civilization today? A potential armed conflict in the future, or the global hybrid war of the 21st century, which is already taking place every day in physical and digital space, disrupting collective defense and security infrastructure, destroying shared values and critically weakening mutual trust, without which the family, society, state and international order gradually disintegrate.

Not only the security, but also the future of the Member States of the European Union and democratic civilization is increasingly threatened by an exceptionally serious threat, which arises from the fact that the decisive technological platforms, communication infrastructure, algorithmic systems and cyber capabilities of the 21st century are outside the direct control of states, either in the hands of private technology companies or are part of the power structures of authoritarian regimes. While traditional defense and weapons systems have been built, owned and managed by states for centuries as a fundamental tool for protecting their sovereignty and security, this fundamental change has created an unprecedented security asymmetry. Democratic states are thus responsible for protecting their citizens, institutions and democratic order, but a significant part of the space in which public opinion is formed and information and influence operations take place is outside their direct influence. It is this structural imbalance that gradually led to the emergence of a globally interconnected conflict environment in which the global hybrid war of the 21st century began to take shape.

The emergence of a global conflict environment and security asymmetry

The emergence of a globally conflictual environment is primarily a consequence of the growing security asymmetry, where the member states of the European Union and NATO do not have full control over key technological platforms, which are either in the hands of private technology companies whose interests are predominantly economic, not security, or have become part of the power structures of authoritarian regimes that use them to act against democratic countries.

In a global conflict environment, the global hybrid war of the 21st century was born

The global hybrid war of the 21st century represents a complex and historically newly emerging security phenomenon. It is a form of multi-level conflict that combines various instruments of power influence, violence, terror, coercion and destabilization, both in physical and digital space simultaneously. It is characterized by a wide range of tools and forms of action. The key ones include the spread of disinformation, conducting information and influence operations, the spread of hate propaganda and the manipulation of public opinion through modern communication technologies and social networks. As a result of these influences, democratic civilization loses the ability to distinguish between truth and lies and thus finds itself in a state of critical threat.

The global hybrid war of the 21st century has enabled the emergence of a digital underworld

The long-term impact of the global hybrid war of the 21st century and its penetration into the digital space has resulted in the emergence of a phenomenon that can be described as the digital underworld. It is a globally interconnected, decentralized environment formed by a network of actors, structures and platforms, in which various forms of cybercrime, information operations and coordinated influence activities take place. This space has gradually developed as a by-product of the conflict environment and the asymmetry between the technological and cyber capabilities of states and non-state actors.

The digital underworld keeps the global hybrid war of the 21st century operational.

The digital underworld forms the essential operational infrastructure of the global hybrid war of the 21st century, enabling its full-fledged functioning. This space functions as an active catalyst of hybrid action, enabling, accelerating and multiplying various forms of information operations, cybercrime and influence activities. The digital underworld is systematically used by millions of actors involved in various forms of cybercrime , as well as by authoritarian regimes, and the scale of these activities is extremely high, encompassing hundreds of thousands to millions of individual incidents per day.

Central Cyber Shield - A Strategic Weapon Against the 21st Century Global Hybrid War

Concerns about the future security of the European Union and NATO member states have led to the need to build a Central Cyber Shield as a fundamental pillar of a new security architecture that meets the conditions of the 21st century. This need arises from the fact that the impacts of the global hybrid war of the 21st century and the emerging digital underworld have a fundamental and long-term destructive impact on the security environment of democratic civilization, and in many aspects, in terms of the daily accumulation of risks, they can be comparable to, or even more serious than, traditional armed conflicts.

The idea of this concept began to take shape seventeen years ago, when its author, based on his experience in conflict environments, identified a fundamental change in the power balance in the digital space. He drew attention to the fact that crucial technological, communication

and cyber capabilities are concentrated mainly in the hands of the private sector, while democratic states do not have the appropriate tools to fully promote their security and strategic interests in the digital environment. At the same time, he identified a growing trend in which authoritarian regimes systematically integrate these capabilities into their power and security structures, thereby deepening structural security asymmetry.

This asymmetry has been assessed as a long-term strategic risk that requires the creation of a new integration and coordination architecture capable of strengthening the position of democratic states in cyberspace and ensuring more effective protection of their security, democratic and alliance interests.

The author of the alliance strategy, such as the Central Cyber Shield, identified at an early stage that the prevailing security paradigm of democratic states is based primarily on regulatory, legislative and ex post reaction mechanisms, including normative frameworks, directive harmonisation and administrative-control tools. At the same time, he concluded that this approach is structurally limited and unable to sufficiently respond to the pace, complexity and adaptive nature of modern hybrid, information and cyber operational environments.

For this reason, he developed the concept of a multi-layered preventive security architecture, based on anticipatory-operative protocols, predictive-reactive security loops, and continuous cyber immunization regimes for critical systems.

The core of this approach is the implementation of integrated preventive operational programs that include sequential detection of emergent threat vectors, preemptive intervention mechanisms, adaptive exposure management of digital ecosystems, dynamic segmentation of operational domains, real-time orchestration of multi-layered defense structures, and continuous activation of distributed security protocols in a state of high operational readiness. These mechanisms are complemented by the ability to preemptively project risk scenarios, controlled reduction of attack surfaces, and systematic increase in the resilience of critical digital and institutional subsystems, creating a model in which the preventive component forms the basic architectural principle of the entire system.

This preventive architecture represents a key prerequisite for stabilizing the strategic position of EU and NATO member states in cyberspace, strengthening their systemic autonomy, and ensuring the long-term resilience of democratic institutions against hybrid threats that are reflected simultaneously in the digital and physical dimensions of security.

This framework also includes the use of predictive threat models based on real-world experience in cyber and hybrid operations, behavioral actor analysis, digital infrastructure hardening , cyber domain segmentation, security operations orchestration, and continuous threat sharing. intelligence across the structures involved. These mechanisms enable early identification of hybrid operational scenarios and their neutralization in the early stages of development.

Thanks to the Central Cyber Shield, the member states of the European Union and NATO will gain the ability to fundamentally strengthen their position and effectively confront the most serious systemic threat of our time, which is the global hybrid war of the 21st century. This has gradually taken shape as a result of the weakening of structural control and the disruption

of the balance in cyberspace, which has come predominantly under the influence of the private sector and authoritarian regimes during the digital transformation.

The security asymmetry created by the concentration of key technologies, digital platforms and cyber capabilities in these two spheres has led to a weakening of trust in democratic institutions, an escalation of security risks in cyberspace and a growing intensity of hybrid attacks on democratic systems. From this perspective, a fundamental strategic conclusion is the need for the alliance commitments of the European Union and NATO member states to be fulfilled simultaneously in both physical and cyberspace, as both dimensions are now fully interconnected and interdependent. [15, 16, 17, 18,19]

Section 2

Central Cyber Shield – the basis for collective security within NATO and the EU

"NATO is expected to be able to fight and protect itself on the ground, in the air and at sea, but also in space and in cyberspace. However, all of these domains have a digital foundation that is vulnerable to cyber-attacks. Cyber protection is therefore a central element in all dimensions of preparation for modern warfare and is crucial for the armed forces. We need to build a digital backbone network. We need to put in place procedures to share huge amounts of data, train the people who will operate the new systems. So there are a lot of things we have to do, and we have to do them quickly."

Author of the quotation: Jean-Charles Ellermann-Kingombe, NATO Assistant Secretary General for Cyber Defense and Digital Transformation[20]

The current NATO defense funding methodology no longer fits the 21st century threat structure and requires immediate reform. This conclusion is not based on theoretical reasoning, but on the empirically demonstrable fact that a critical part of the security risks have shifted to cyberspace, which today represents the primary environment in which systematic disruption of democratic states occurs. The key shortcoming of the current approach is not the existence of defense mechanisms per se, but their incorrect prioritization. While a significant amount of funding continues to be allocated to conventional military capabilities, the space that directly affects the stability of states, their political processes and collective defense capability remains structurally and financially undersized.

In this context, it is necessary to formulate a fundamental strategic thesis: the security of NATO Member States and the European Union today is primarily determined by the level of stability in cyberspace. This space can no longer be understood as an additional domain, but as the basic infrastructure on which the functioning of a democratic state is built. Today, all key processes – from public opinion formation to electoral mechanisms to the decision-making processes of governments and security institutions – are dependent on the digital environment. Any disruption of this environment is therefore not merely technical, but a direct attack on the very foundations of democracy.

At the same time, cyberspace has become an environment in which a systematic action is taking place that can be characterized as a structural destabilization of democratic systems. This state can be analytically described as "disinfocracy" – a form of hybrid action in which manipulative content is massively disseminated, information integrity is undermined and trust in democratic institutions is gradually eroded. Unlike traditional threats, this process has neither a clear beginning nor an end; it is continuous and affects all levels of society. The result

is a weakening of the citizens' ability to orient themselves in reality, a questioning of the legitimacy of state institutions and a gradual erosion of social cohesion.

The fundamental problem is that current tools for responding to this type of threat are inadequate. Regulatory approaches based on bans, commands and directives are unable to ensure the protection of a democratic environment in cyberspace. These tools are ex-post reactive, have limited effectiveness in the global digital environment, and often themselves raise additional tensions, including concerns about freedom of expression and the legitimacy of state intervention. Above all, however, they fail to address the root of the problem, which is the absence of a systematically built digital democratic infrastructure.

It is this absence that represents the greatest structural weakness of the current security system. Democracies have entered the digital era without adequate infrastructure capable of protecting the basic principles of democratic functioning in the online environment. The result is a situation in which a key space for the formation of public opinion, political debate and social interaction is not under the control of democratic mechanisms and is exposed to intense destabilizing influences.

The solution to this situation cannot be a partial modification of existing instruments, but a systemic change of approach. This is the establishment and activation of the **Central Cyber Shield**, which is a key element of the proposed reform of the defense financing methodology. The Shield is not just a technology project, but a comprehensive security framework that aims to create a fully-fledged digital democratic infrastructure at the level of NATO Member States and the European Union.

The essence of this concept is that protecting democracy in the digital environment cannot be based on restrictions, but on actively building an environment that is structurally resistant to manipulation, disinformation and hybrid operations. In this sense, a digital democratic infrastructure would be the equivalent of a physical defense – a system that not only responds to attacks, but prevents them by minimizing their effectiveness.

A key aspect of this infrastructure is the protection of trust. Trust in democratic institutions, electoral processes, the media and international alliances such as NATO and the European Union is a fundamental condition for their functioning. In cyberspace, however, this trust is systematically eroded. If it is not actively protected, there is a gradual decay that inevitably carries over into the physical world. As a result, the legitimacy of the state is weakened, political instability increases and the ability to respond to security threats is reduced.

For this reason, it is necessary to redefine the very principle of collective defense. The current model, based on NATO Article 5, must be extended to include its digital dimension. The introduction of the so-called digital Article 5 means that an attack on the information and cyber infrastructure of one Member State will be considered an attack on all. However, this principle cannot be merely declaratory. It must be backed by adequate capacity, coordination and, above all, funding.

This is where we get to the heart of the proposed reform. Redirecting part of defense budgets to finance the Central Cyber Shield is not an alternative to existing spending, but a necessary complement to it and a condition for its effectiveness. Without ensuring stability in

cyberspace, it is impossible to ensure the functionality of military structures, logistics systems and decision-making processes. In other words, collective defense in the physical world is directly dependent on the existence of collective defense in cyberspace.

Ignoring this fact creates a major strategic risk. If cyberspace remains inadequately protected, it will continue to serve as a major entry point for destabilizing states. This process may lead to the gradual disintegration of democratic systems, the weakening of international alliances and, in the extreme case, their de facto paralysis. This is not just a technological or security issue, but a question of the existence of the current democratic order.

The reform of NATO's defense funding methodology must therefore be based on a clear priority: the systematic establishment and funding of the Central Cyber Shield as a fundamental pillar of collective security. This represents the only realistic response to the nature of the current threats and the only way to ensure that the collective defense of the European Union and NATO Member States will be operational not only formally but also in practice in the digital age.[21, 22, 23]

Section 3

AI political parties can lead humanity to prosperity, but also to destruction

---

The emergence of AI political parties represents one of the most fundamental civilizational turning points in modern history. It is not just an evolution of existing political structures, but a profound transformation of the nature of politics, power and democratic decision-making. This process is not the result of an ideological shift, but a logical consequence of technological developments that have fundamentally transformed the way people communicate, acquire information and form their ideas and opinions in recent decades. Politics, which for centuries has been firmly anchored in physical space – in parliamentary halls, town squares, regions and communities – is gradually moving into the digital world, where its dynamics are determined by algorithms, data flows and artificial intelligence.

AI political parties are not a mere technological innovation, but a phenomenon with global impact, capable of fundamentally affecting not only individual states but also the international order. For the Member States of the European Union, the North Atlantic Treaty Organization and the entire democratic world, these new political structures can be a path to unprecedented prosperity, efficiency and stability. At the same time, however, they carry the potential to destabilize states and global society, to bring them to systemic disintegration and, in extreme cases, to threaten the security of civilization. With the help of AI, political parties are becoming the real bearers of political power, able to analyze the mood of society, identify key issues, propose solutions and optimize decision-making processes with a speed and accuracy that is unattainable for human actors. That is why it is essential to build the Central Cyber Shield – a key security mechanism against radical, manipulative and undemocratic actors that will ensure stability and protect the democratic nature of political processes.

The emergence of AI political parties has already moved beyond the experimental stage and similar structures are taking shape around the world. The most visible activity is in countries where state control over the digital space enables rapid technology development. A typical example is China, where there are no separate AI political parties yet, but there are already signs of AI being used to support the political process – for example, through AI avatars, chatbots or systems that analyze public opinion and spread state-approved messages. These tools support administrative efficiency and state communication, paving the way for the possible future involvement of AI in political structures, but they are not yet separate entities with autonomous political power.

The spread of these technologies beyond their original geographical boundaries is a logical consequence of the globalized digital environment. Social networks, content sharing platforms and global communication channels allow models and algorithms developed in China to penetrate democratic states, where they can influence public opinion, polarize society and destabilize political processes. AI political parties that may establish themselves here do not necessarily follow democratic principles; on the contrary, they may emulate authoritarian or totalitarian ideologies. Voters exposed to such targeted and personalized

propaganda may make decisions driven by algorithms and psychological manipulation rather than informed choice, dramatically increasing the risk of destabilizing democratic institutions.

For the Member States of the European Union and NATO, this development represents an extremely critical danger. Traditional regulations, bans, or efforts to limit digital communication have proven ineffective; AI political parties can manipulate public opinion with unprecedented speed, accuracy, and depth that no single piece of legislation can manage.

This situation highlights the urgent need for the creation of the Central Cyber Shield of Democracy – a robust security mechanism whose activation will enable the immediate start of building an integrated political, security, value and legal system in cyberspace based on the principle of ONLINE DEMOCRACY. The backbone of this system is a digital democratic infrastructure that will provide effective and efficient protection against disinfocracy – the most devastating hybrid threat of the 21st century. The Central Cyber Shield will protect EU and NATO Member States from AI political parties far better than any form of digital regulations, bans or commands, while verifying the identity of political entities, ensuring transparency of their activities and securing the entire digital space from being misused for propaganda, hatred or ideological manipulation.

But time plays a critical role. Once AI political structures with authoritarian tendencies begin to establish themselves in the democratic world, the options for prevention and intervention will be severely limited. Every day that digital space remains unprotected increases the risk that these structures will affect key elections, political decisions and the stability of public institutions. Sophisticated tools for psychological manipulation, targeted propaganda and predicting voter behaviour mean that traditional methods of defense – information campaigns, social media regulation or sanctions – are fundamentally ineffective.

Therefore, it is imperative that NATO and EU Member States urgently create a comprehensive institutional, technological and legislative backdrop that allows for a managed and secure transition from traditional political parties to emerging AI political entities that can coexist for a transitional period before they are gradually replaced in the digital age. At the same time, it is necessary to activate the Central Cyber Shield, which will act as a robust protective framework for ONLINE DEMOCRACY, ensuring the safe, transparent and trustworthy functioning of political processes, including verification of the identity of political actors, data integrity, protection of electoral mechanisms and resilience to manipulation and cyber threats.

Without such a comprehensive protection system in place, there is a serious and systemic risk that AI political parties already emerging in the world may gain dominant influence in the future and, in extreme scenarios, promote forms of digital authoritarianism, not only in EU and NATO Member States, but also in the wider global space. There is a real risk that such a development will lead to the collapse of democratic structures, the destruction of the institutional framework and the disintegration of the basic mechanisms of democratic governance.[24, 25, 26]

Section 4

Digital regulation will not restore or strengthen citizens' trust in democracy

---

The decline in trust in democracy and its institutions – not only at the national but also at the international level – is now increasingly evident as a key consequence of the transformation of the digital environment. Social media content plays a crucial role here, systematically creating user addiction. This addiction, compounded by the targeted manipulation of emotions – fear, anger, surprise or laughter – represents the greatest security threat to democracy and stability in EU and NATO Member States.

Hidden forms of disinformation, propaganda, hate and manipulation are integrated into attractive, interactive and emotionally engaging formats that draw users into an ever deeper disinformation space. It is this combination of addiction and covert influence that has enabled the development and dominance of disinfocracy – the most destructive hybrid regime of the 21st century, which has been systematically operating on social media for more than fifteen years. The result is a gradual weakening of citizens' ability to rationally orient themselves in public space, polarization of society and erosion of trust in democratic institutions.

Neither the European Union nor the NATO alliance has yet grasped this issue as a structural security risk. In fact, a paradoxical situation arises: users are cut off from their personal lives, personal development and active participation in public life due to digital dependence, and the care for the common good of the state and society is weakened. Instead, their attention is drawn to content that primarily elicits emotional responses and maximizes engagement, while covertly reinforcing the disruption of democratic processes.

From the point of view of democratic systems, this process has devastating consequences: the ability of citizens to distinguish between facts and manipulation is gradually weakening, limiting their active participation in public life. This trend also erodes trust in international Organizations such as the European Union and NATO, whose legitimacy is based on the trust of Member States and citizens. If this trust is systematically eroded, the ability of these organizations to perform their functions effectively is undermined.

The fundamental problem with the current approach is that any digital regulation – bans, commands or directives – cannot inherently solve the problem of user dependency or eliminate the mechanisms that perpetuate it. Regulation can only go so far in reducing visible manifestations, but it cannot eliminate the core problem: the economic model of platforms and their ability to maximize attention through emotionally engaging content.

At the same time, the current state of affairs creates space for actors to exploit the digital environment for their own benefit, often at the expense of the public interest. The economic incentive to maximize engagement encourages the dissemination of content that evokes strong emotions and marginalizes material that promotes information, education or constructive public debate. As a result, the digital environment actively contributes to the spread of ideologies and strategies that destabilize democratic values.

From the individual's perspective, this trend manifests itself in a loss of control over one's own time and attention. Dependence on social networks limits the space for personal development, education, professional growth and participation in public life, which has a major impact on individual and social well-being. This imbalance between short-term emotional gratification and long-term goals poses a critical risk to democracy and the collective security of EU and NATO Member States.

Restoring trust in democracy cannot be achieved by restrictive measures, but only by a systemic change in the approach to the digital environment. A key element is to build an integrated political, security, values and legal framework that will enable effective governance of cyberspace and the protection of democratic principles. Part of this framework is the concept of ONLINE DEMOCRACY, which transforms the user from a passive consumer to an active participant in public life.

ONLINE DEMOCRACY enables citizens to engage in decision-making processes, share their views in a structured way and participate in policy-making with a direct impact on their lives. It strengthens transparency, accountability and trust – key prerequisites for the long-term functioning of democratic systems. At the same time, it creates space for the digital environment to support activities that contribute to society's development instead of undermining it.

The Central Cyber Shield is a systemic solution that replaces the ineffective regulations that have been in place to date. Its main mission is to build a digital democratic infrastructure that enables the protection and strengthening of citizens' trust and effectively defends the dominance of disinfocracy in the global information space. Without its existence, neither the stability of democratic systems nor their collective defense can be ensured in the conditions of the 21st century.

Section 5

Protecting democracy in cyberspace – a condition for its survival in the physical world

---

The mission of the Central Cyber Shield is to ensure the collective defense of democratic countries, European Union and NATO Member States against the complex spectrum of 21st century hybrid threats. Instead of introducing digital regulations and directives, which are in direct conflict with the strategic fight against these threats, as they focus mainly on administratively dealing with their consequences (deleting content, bans, commands or orders), the first ever political, security, value and legal system in cyberspace will be built – ONLINE DEMOCRACY. Its structural architecture will not only prevent the spread of disinformation, hatred, propaganda and manipulation of public opinion, but also eliminate their causes. This is an existential necessity, as the fate and survival of democracy in the physical world depends on ensuring the protection of democracy in cyberspace.

As part of the strategic fight against 21st century hybrid threats, it is completely unacceptable to rely on digital regulations, directives, monitoring, analysis, bans or deletion of content in cyberspace, as these measures only respond to the effects of the spread of disinformation, hatred, propaganda and manipulation of public opinion, and do not address the causes. For this reason, the protection of the population and the state, national security, the integrity of democratic institutions and the trust of citizens in the functioning of international organizations such as the European Union, NATO and the United Nations can never be guaranteed.

Democracy is a value system based on freedom, the rule of law and human dignity and cannot be protected by commands, prohibitions or military force. Its real protection must be ensured by building an integrated political, security, value and legal system in cyberspace – ONLINE DEMOCRACY that links the digital and physical worlds. It is in cyberspace that all social and political communication and decision-making processes take place today, on which democracy in the physical world is existentially dependent.

In the context of modern security and the fight against hybrid threats, an integrated political and security system in cyberspace means a state in which digital space is not perceived only as “technology” (cables and servers), but as a full-fledged part of the state with the same rules as in the physical world.

In the fight against the spread of disinformation, hatred, propaganda and manipulation of public opinion, it is absolutely crucial to build a digital democratic infrastructure in cyberspace, which is a basic prerequisite for the emergence of a functional ONLINE DEMOCRACY. Without it, no preventive, security or political measures against hybrid threats can be effectively implemented, as they would lack the basic framework to ensure the credibility, legitimacy and stability of democratic processes. In a digital environment with more than five billion users, it

is therefore essential to move away from ineffective reactive regulations that only address the consequences and instead build an integrated system that actively prevents hybrid attacks through its internal integrity and robust architecture.

The Central Cyber Shield is conceived as a system built on ten pillars, which together form a complex and interconnected framework for the protection of democratic processes. Only such a coherent system can ensure resilience to hybrid threats and safeguard confidence in democracy. The individual pillars include an integrated legal order of cyberspace, digital sovereignty of citizens, transparent algorithms for public debate, secure digital identities, active detection and elimination of attack narratives at the source, protection of critical information infrastructure, educational resilience of society, an ethical framework for artificial intelligence, international security coordination, and timely political attribution of attacks. This ten-pillar model abandons the ineffective method of reactive bans and instead builds a proactive digital fortress that does not refute hybrid aggression ex post, but by its systemic integrity renders it ineffective before it reaches public opinion.

The fragmentation of regulatory approaches creates so-called ‘safe havens’ in cyberspace for attackers who exploit the legislative vacuum to wage information warfare with impunity. Instead of a united defense front, this creates a dangerous asymmetric space where democratic institutions are paralyzed by their own bureaucracy, while hybrid threats operate in real time. The current reactive model, based on deleting content, completely ignores the algorithmic nature of the current manipulation; instead of addressing the cause, it merely attempts to alleviate the visible symptoms of social decay. To prevent further escalation of violence and destabilization of states, it is essential to replace these isolated and dysfunctional directives with a single digital architecture. It must be built on the principles of preventive deterrence and technological integrity, which are the only ones that can restore order in cyberspace and ensure that digital disinformation stops transforming into real destruction of the democratic world.

The integration of the Central Cyber Shield into international structures (EU, NATO) is a key evolution in defense: the transition from physical weapons to the protection of cognitive and information space. In an era when the boundary between peace and conflict blurs into the grey zone of hybrid action, it is no longer possible to separate territorial security from digital security. Indeed, the absence of a unified technological and value platform in cyberspace makes Article 5 of the Washington Treaty vulnerable; an attack that disrupts the internal stability of a state through massive manipulation and trust erosion can be as devastating as a conventional invasion, but without adequate infrastructure, it remains below the threshold of an armed response. Building the Shield is thus not just a technical innovation, but a strategic imperative that defines a new level of deterrence. Only through this digital architecture can the Alliance guarantee its operational capability and ensure that collective defense is a real guarantee of sovereignty in the 21st century, not just an empty declarative concept in a digitally destabilized world.

Rather than building central authorities on truth, the focus should be on building an integrated architecture of trust in democracy. In cyberspace, where content cannot and must not be controlled through subjective censorship, the systemic integrity of the environment itself must provide protection. This digital democratic infrastructure does not replace human judgement, but provides it with a solid and secure framework – from unmanipulable digital

identities to transparent algorithms to clearly defined legal responsibilities of actors. By protecting processes (how information is disseminated and verified) rather than specific words (what is said), the system creates an immunity environment where disinformation loses its destructive power without sacrificing freedom of expression. This shift from content to infrastructure is the only possible way to protect five billion users from both technological dictatorship and hybrid disruption.

ONLINE DEMOCRACY represents the first ever integrated political, security, values and legal system in cyberspace. This new global authority is not another authority, but the universal operating system of digital civilization – the missing link between technological progress and the social contract. Building this legitimate structure allows democratic principles to be written directly into code and network protocols, transforming cyberspace from an uncontrolled battlefield into a safe and transparent space. Without this systemic anchoring, attempts to defend against disinformation, hatred, propaganda and manipulation of public opinion will remain a futile battle with windmills; without digital statehood, neither law, security nor freedom can be guaranteed in the online world.

WARNING

If state and international regulation of cyberspace is limited to repressive mechanisms – i.e. directives, bans, commands and deletion of content – while ignoring the profound erosion of social cohesion that this content causes, it is not defending democracy, but building digital authoritarianism.

Real defense requires systemic anchoring of values and law directly in the architecture of the network (digital statehood), not just tools for text censorship. Without this distinction, the pursuit of security turns into an instrument of control which, instead of protecting freedom, destroys the very essence of democratic dialogue.

ONLINE DEMOCRACY and its Central Cyber Shield are therefore not a choice, but an existential necessity. Without this infrastructure to anchor the same level of legal and security certainty in cyberspace that we enjoy in the physical world, modern states remain empty shells whose sovereignty ends at the first internet cable. Only the integration of the ten pillars of the Shield into the very DNA of the digital world will allow states and international institutions, as well as NATO, to take the initiative again and transform cyberspace from a tool of destruction into a secure pillar of civilization.

However, the lack of policymakers' digital preparedness is a strategic security risk. National and international security positions require leaders who come into office already fully trained for hybrid conflicts. If decision-making processes are based on theoretical knowledge instead

of real-world experience with the physical and cyber battlefield, the result is flawed decisions with a destructive impact on the state's security architecture. ONLINE DEMOCRACY and its Central Cyber Shield therefore require a new elite – leaders who have undergone authentic training in digital conflict environments and for whom cyberspace is a natural operating field.

The year 2014, when hybrid aggression fully exposed the vulnerability of the digitally connected society, set a dangerous precedent for manipulation with impunity. The absence of robust defense mechanisms at the time allowed cyberspace to become an incubator for information warfare. The mass spread of disinformation, hatred and propaganda gradually gave birth to the phenomenon of disinfocracy, which took full control of social networks and began to shape public opinion and political reality uncontrollably.[27]

The mass spread of disinformation, hatred and propaganda in cyberspace gave birth to the information war, which subsequently resulted in the phenomenon of disinfocracy through social networks.

Disinfocracy is the most destructive hybrid regime of the 21st century, which has been operating for more than fifteen years on social networks and causing information disorientation of the public. Because of this, bad political and personal decisions are made, resulting in ruined interpersonal relationships, growing quarrels, hatred, frustration, anger, fear, despair, helplessness and hopelessness, broken families, increasing conflicts between people, chaos, critically weakened security, social, economic and legal stability of the country, deepening poverty, mental disorders and suffering, terrorism, wars, violence, radicalization, extremism, gradual loss of trust in the state and the international system, and crumbling democracy in the world.

Atrocities are taking place in cyberspace, the extent of which is not fully known to citizens or NATO Member States. This digital horror includes not only the spread of disinformation, manipulation of public opinion, hatred, digital violence or information warfare, but also online masquerade (maskirovka) – digital invasion of democratic countries, cyber-occupation of states – authoritarianism, restriction of personal freedom and freedom of expression, censorship, radicalization on social networks – i.e. social terrorism, digital cancer, influence operations including the activities of intelligence services, hybrid attacks on democracy, etc, which penetrate the physical world through mobile devices and existentially threaten democracy, subvert the state and critically undermine economic and technological development and national security. These destructive processes collectively constitute a phenomenon known as "disinfocracy".

In order to effectively counter disinfocracy, the most destructive hybrid regime of the 21st century, policymakers must have direct experience with conflict in cyberspace. However, most of them lack this experience. Relying on consultants is no substitute for the lack of insight into the dynamics of the lightning spread of hatred and sophisticated manipulation. In crises, elites therefore resort to outdated directives and ineffective prohibitions that fail in the digital world.

This lack of ‘frontline’ experience makes security structures inadequate. A political system without a functional cyber counterpart is strategically unsustainable in a modern civilization and directly threatens the essence of democracy.

The only effective defense is ONLINE DEMOCRACY – an integrated political, security, values and legal system anchored in a digital architecture. This structure permanently links the physical and digital worlds and guarantees the resilience of democratic processes against hybrid threats.

The Central Cyber Shield was created as the ultimate security guarantee for this new infrastructure. It prevents the transmission of hybrid threats from digital devices to reality and creates a safer space for the five billion users of the internet and social networks. It is more effective than any bureaucratic regulation, whose inconsistent implementation among states paradoxically exacerbates chaos and destabilization. Without the Central Cyber Shield, neither the stability of the EU democracies nor NATO’s operational capability can be ensured today. It is an existential necessity for the collective defense of modern civilization.

Section 6

The principle of collective defense of democracy in cyberspace

---

The Central Cyber Shield (Bohemia: Central Cyber Shield) represents the highest form of protection for democratic infrastructure in the digital space. Its existence is essential today because the future of democracy in the physical world is directly dependent on ONLINE DEMOCRACY – a system that links digital and physical space through a single political, security, values and legal framework. The digital civilization, which today consists of more than five billion internet and social network users, requires a stable, legitimate and trustworthy infrastructure that goes well beyond the possibilities of traditional directives, regulations, prohibitions or commands. These existing mechanisms are proving to be fragmented, uncoordinated and ultimately often counterproductive.

The main task of the Central Cyber Shield is to ensure the collective defense of democracy in cyberspace, which is practically non-existent today. NATO may have Article 5 for collective defense in the physical world, but in cyberspace the allies and the European Union as a whole remain defenseless. To date, there is no functional collective cyber defense mechanism to counter disinfocracy – the most destructive hybrid regime of the 21st century. This fundamental deficit directly threatens the security, resilience and stability of the democratic world. The Central Cyber Shield closes this gap and provides a universal collective defense framework that can be used not only by NATO Member States, but also by EU Member States, other democracies and international institutions. This ensures that national defenses are no longer limited to physical space, but are fully extended to cyberspace, where a crucial part of political, social and security communication takes place today.

The collective defense of democracy cannot be ensured by bans, directives or censorship. Only by building an integrated political, security, values and legal system – ONLINE DEMOCRACY – can the physical and digital worlds be linked and a unified framework for protecting democratic infrastructure be provided. This system fully integrates all forms of management, monitoring, prevention and response against hybrid threats that no single state or international organization can effectively manage on its own. Political systems operating exclusively in the physical world without a digital counterpart are now strategically unsustainable and pose an existential risk to stability, security and the very essence of democracy.

The existential requirement of collective cyber defense: The extension of Article 5 to digital Article 5

At present, even the NATO alliance is not fully defensible. While strategic investments in military infrastructure continue, there is a gradual weakening of collective defense caused by the massive spread of disinformation, hatred, propaganda and manipulation of public opinion, especially on social media. Out of these processes was born the information war, which has

evolved into the phenomenon known as disinfocracy – the most destructive hybrid regime of the 21st century, which systematically erodes citizens' trust, destabilizes democratic institutions and threatens the ability of Member States to cooperate effectively.

As a result of these developments, some Member States are rightly questioning whether NATO can fully meet its commitments, including investment in defense capabilities and compliance with alliance agreements, as a key prerequisite for defense – confidence in democracy and institutional stability – is directly threatened. The existential solution is therefore to introduce a so-called digital Article 5, which would actively protect the alliance against the spread of disinformation, hatred, propaganda and manipulation through the Central Cyber Shield. This instrument will ensure comprehensive protection of trust, stability of democratic institutions and real defense capability of the Member States and the entire NATO Alliance in the digital age, making it an indispensable pillar of collective defense in the 21st century.[28]

The structure of the Central Cyber Shield is built on the principle of collective defense and consists of ten pillars, which together represent a comprehensive and integrated system for the protection of digital democratic infrastructure:

- **ONLINE DEMOCRACY**: The first political system in cyberspace that ensures legitimate decision-making, collective defense and the interconnection of the digital and physical worlds through a comprehensive system of protection and development of digital statehood, national identity, legitimacy and sovereignty of the state. This system guarantees the protection of human rights, freedom of expression, human dignity and the right to a digital existence.
- **Digital democratic infrastructure:** A single platform replacing fragmented regulations and providing a coordinated framework for political, security and legal measures, ensuring collective defense and an impenetrable digital shield for EU Member States, NATO and all democratic allies.
- **Politinn social network:** Europe's first next-generation democracy platform, ensuring the protection and development of democracy in the digital and physical world. In cyberspace, it builds a coherent political, security, value and legal system, enables the evolutionary development of electoral processes through e-voters and e-candidacies, and guarantees legitimate decision-making, thus ensuring the collective defense and stability of digital civilization for EU and NATO Member States.
- **Cyber Strategy 2026 – Fighting Disinfocracy:** Disinfocracy is the most destructive hybrid regime of the 21st century. Instead of ineffective restrictive measures, regulations, directives and selectively enforced bans that only exacerbate chaos and violence, this pillar builds an integrated political, security, values and legal system in cyberspace that prevents the rise of threats and conflicts in the form of disinformation, hatred, propaganda and manipulation of public opinion that aggressively penetrate the physical world through social networks and mobile devices.
- **Central Cyber Shield for NATO:** With the introduction of digital Article 5, we are necessarily adapting NATO to the realities of the 21st century. In doing so, we codify the principle that disinfocracy – the most destructive hybrid social media regime of the 21st century – requires an immediate allied response. Systemic disruption of democratic processes thus becomes an attack on the entire Alliance and cyber collective defense an integral part of our indivisible security.

- **Digital World Organization (DWO):** The best way to collectively defend democracy is to build a new world order in cyberspace. Building this order without the Central Cyber Shield, of which the Digital World Organization (DWO) is a part, is doomed to failure. For the first time in history, humanity is living in two worlds simultaneously – the physical one and the digital one. This new dimension of reality makes it essential for the DWO to build an innovative political, security, value and legal system in cyberspace for the more than five billion users of the Internet and social networks.
- **Cyber Strategy 2026 – Fighting the "Digital Cancer":** This pillar serves as an active defensive shield and prevention against destructive digital content that corrodes the human psyche and society. Rather than passively watching, it is building a system that guarantees a safe environment in cyberspace and protects the lives and physical and mental health of more than five billion Internet and social network users. The goal is to stop the technological degradation of humans, prevent digital addiction and eliminate toxic algorithms that trigger depression, anxiety and self-destructive behaviour. In this way, Cyber Strategy 2026 protects human integrity and ensures that the digital world remains a space for development, not a tool for destroying human health and dignity.
- **Cyber Strategy 2026 – Cyber Rearmament:** It is a strategic modernization of defense mechanisms, an integral part of which is the establishment of an integrated political, security, value and legal system. Kvalita a účinnost kybernetického přezbrojení přímo závisí na stabilitě tohoto nového řádu, který transformuje technologickou sílu v nástroj ochrany digitální státnosti. In the framework of Cyber Strategy 2026, this rearmament gains equal weight with conventional military investments, because without the systemic strength of legal and value anchoring in cyberspace, any technical protection against sophisticated attacks remains dysfunctional.
- **Cyber Strategy 2026 – Combating Social Terrorism:** Strategic pillar of Cyber Strategy 2026 aimed at eliminating radicalization of citizens in the social networking environment. We define social terrorism as a process of targeted disruption of society through digital platforms, where hate, fear and disinformation are systematically spread to destabilize legitimate institutions and the democratic order. The tragic consequences of this phenomenon do not remain in cyberspace, but through digital violence and psychological manipulation directly expand into the physical world, where they trigger real conflicts, aggression and the breakdown of social cohesion. This pillar builds an active prevention and protection system that prevents digital devices from turning into tools of radicalization, thus guaranteeing the safety of citizens and the stability of the state.
- **Building a security, value and legal system in cyberspace:** Building the pillars of digital statehood, sovereignty and national identity that ensure the legitimacy of the state in cyberspace. This comprehensive system is the real protection that no restrictive measures, digital regulation, directives, bans or orders can provide. While bureaucratic commands are ineffective in the digital world and are often ignored by states, this pillar creates a functional order that uncompromisingly guarantees the protection of human rights, freedom of expression and human dignity. For all democratic countries, EU and NATO Member States, this sovereign infrastructure is the only way to protect national identity from decay and ensure the survival of democracy in the physical world.

Each of the ten pillars replaces previous ineffective regulations, directives and bans that were fragmented, uncoordinated and short-sighted. Together, they provide a stable, legitimate and

secure framework for more than five billion internet and social network users. This system actively promotes social cohesion and ensures a fully functional connection between digital and physical space, creating a unified and impenetrable architecture of modern civilization.

The Central Cyber Shield is not only a tool for protecting democratic infrastructure, but also a guarantor of collective defense in cyberspace. It is a key element without which the EU and NATO Member States, as well as all other countries of the world and the international community as a whole, cannot ensure their stability and security. This system is historically unique and existentially necessary; only through the ten pillars of the Central Cyber Shield can the existence of democracy in both worlds be guaranteed simultaneously, the protection of human rights and the public good be ensured, and the overall security resilience of modern civilization be strengthened.

Section 7

ONLINE DEMOCRACY will connect the digital and physical worlds

Each state has its own political, security, value and legal system that determines the functioning of society, guarantees the protection of citizens' rights and freedoms and ensures the stability of democratic processes. This system is firmly anchored in the physical world, but its full-fledged equivalent in cyberspace is still missing. It is this systemic fracture that is the root cause of the growing threats, conflicts and destabilizing phenomena that emerge in the digital environment and are then uncontrollably transmitted to the physical world through social networks and mobile devices.

Cyberspace is a global and borderless environment with more than five billion Internet and social network users. Unlike the physical world, however, there is no single legitimate and functional system of social governance that is consistent with the political, security, value and legal structures of each state. This systemic absence creates an uncontrolled environment in which there is a massive spread of disinformation, hatred, propaganda and manipulation of public opinion, which inevitably leads to polarization of society, escalation of conflicts and systemic disruption of democratic processes.

So far, the approach of states and international institutions, including the European Union, has been limited to the introduction of digital regulations, directives and orders. However, this model is proving to be fundamentally inadequate and systemically unworkable. Regulations are applied only to a limited number of countries and entities, while other countries do not apply them at all. In an environment that is inherently global and interconnected, this creates a critical asymmetry: the rules apply only to a fragmented part of the digital space, while the rest of it remains outside any control. The result is deepening chaos, fragmentation and ever-increasing security and social tensions.

This disparity creates a paradoxical situation where regulations that are supposed to protect democracy do not actually stop the spread of hybrid threats, but instead contribute to their escalation. Disinformation, propaganda and manipulation spread across digital borders regardless of local legislation. Any restrictive measure in one part of cyberspace is easily circumvented by other jurisdictions, making the current fragmented approach unsustainable and strategically ineffective in the long term.

It follows that digital regulation alone can never be a real solution. It does not address the root of the problem, which is the absence of a comprehensive and legitimate system of governance in cyberspace. Protecting democracy in the digital environment cannot therefore be based on piecemeal restrictive measures, but requires a profound systemic transformation. Only the creation of full-fledged digital statehood and governance in cyberspace can provide the stability and security that current fragmented directives lack.

The only long-term sustainable solution is to build a fully-fledged political, security, value and legal system in cyberspace that is consistent with the principles of democratic states in the

physical world. This system must be based on the principles of ONLINE DEMOCRACY and be firmly anchored in a robust digital democratic infrastructure that ensures the legitimacy, transparency and credibility of all processes taking place in the digital environment.

The Central Cyber Shield plays a key role in this process. It is not just a technological tool, but a complex systemic framework that enables the definition and enforcement of uniform rules for the functioning of the digital civilization. Its main task is to ensure the protection of more than five billion users of the Internet and social networks, to strengthen resistance to hybrid threats and to prevent their destructive transfer to the physical world.

Through ONLINE DEMOCRACY, the Central Cyber Shield thus creates the basic pillars for the emergence of a new, globally interconnected system that integrates the physical and digital worlds into one functional whole. Unlike fragmented regulations, this mechanism provides a unified, consistent and systemically anchored approach to the protection of democracy, human rights and security. It is the linking of the Shield with ONLINE DEMOCRACY that ensures that technological defense is not just a passive filter, but a legitimate instrument of digital statehood that guarantees the stability of modern civilization.

Without this system in place, cyberspace will continue to be a source of instability, conflict and hybrid threats that will gradually erode not only the digital environment but also the very foundations of democratic states. In the modern digital civilization, it is no longer possible to separate the functioning of society in the physical and virtual worlds. The two spaces must be inextricably linked by a single legitimate and functional system that ensures their stability, security and long-term sustainability.

Section 8

Digital statehood: The political and legal basis of the state and democracy in cyberspace

Digital statehood is a complex and systemically interconnected framework that aims to transfer the exercise of state sovereignty, democratic processes and citizen protection to cyberspace. It is not just about technological infrastructure, but about fully extending the state's existence into the digital dimension, which is now a key environment for the functioning of modern society. The basic principle of digital statehood is the creation of a functional political, security, value and legal system that fully corresponds to the structures of the physical world in cyberspace and at the same time complements them in a necessary way.

In this context, it is necessary to distinguish strictly between two key levels of protection, which are often mistakenly confused, although they are fundamentally different in nature and function.

The first level is the technical and security protection of the state in cyberspace. This includes in particular the security of critical infrastructure, communication and network systems, government databases, cloud storage, energy and transport nodes, health and financial information systems, military technologies and authentication systems. This level of defense is aimed against cyber attacks, hacking operations, sabotage or industrial espionage and is necessary to ensure the elementary functionality of the state and its technological stability. However, this is primarily about defending infrastructure, not about protecting the very essence of democracy.

The second, no less crucial level is the protection of digital statehood as a value, political and legal system. This protection is aimed at preserving the integrity of democracy in cyberspace – that is, defending freedom of expression, human rights and dignity. Ensuring the legitimacy and security of digital democratic processes, such as online elections (e-voting), e-referendums and digital participation of citizens in governance, is a key priority at this level. It is no longer just about technical encryption, but about guaranteeing legal indisputability and citizens' trust in digital institutions. Defense against disinformation, manipulation of public opinion and psychological operations also fall under this umbrella. These forms of hybrid threats do not attack the technical infrastructure, but the very essence of democratic decision-making and the value anchoring of society.

It is at this second level that the immunity system of democracy plays a key role. Its fundamental pillar is to protect, build and maintain trust in democracy. This immunity system is a set of systemic, preventive and adaptive mechanisms that draw their strength from the authentic trust of citizens in the institutions and values of the state. Thanks to this, it is able to recognize, analyze and neutralize harmful information influences naturally, without the need for repressive interventions. This approach is fundamentally different from traditional forms of regulation: instead of ineffectively reinforcing control over content, it focuses on restoring trust as a key factor in the resilience of the whole system to manipulation.

The fundamental problem with the current approach to security is that most states focus almost exclusively on the first level – i.e. technical protection of infrastructure. However, the second dimension, representing the protection of digital statehood itself as a carrier of democratic values, remains underestimated and insufficiently addressed in the system. This mismatch creates a critical security gap; modern hybrid threats do not primarily target only the technical background, but attack directly the value and decision-making system of society.

One of the key pillars of digital statehood is therefore ONLINE DEMOCRACY, which represents a new model of democratic governance in a digital environment. This model allows for direct involvement of citizens in decision-making processes, radically increases transparency and fundamentally strengthens the legitimacy of the entire political system. ONLINE DEMOCRACY thus transforms passive digital consumers into active digital citizens, creating a necessary value counterpart to the current fragmented and inefficient system of governance.

ONLINE DEMOCRACY is also a tool for the protection of the value system, as it creates a structured and credible space for public debate and decision-making. A key tool for the implementation of this model is the social network Politinn – a new generation European platform that serves as an institutional and communication environment for authentic interaction between citizens, politicians and institutions. This platform is not a mere communication tool, but a fundamental building block of digital statehood, which enables the organic connection of all its components into one functional and legitimate whole.

The basic system framework is the digital democratic infrastructure, which provides a functional link between the technical and value levels. This infrastructure creates an environment in which a secure technological base can coexist with a stable democratic system. It includes, among other things, digital identities of citizens, secure communication channels, verification mechanisms, transparent data structures and institutional tools for effective management and control of processes. Only this complex infrastructure can transform cyberspace from an uncontrolled environment into a legitimate part of the state.

The institutional backbone of the entire system is the National Security Center for the Defense of Democracy in Cyberspace, which links the technical protection of the state with the protection of its value system. This center coordinates not only the active defense against cyber attacks, but also the comprehensive protection of democratic processes against hybrid threats. It acts as an integrating element that ensures synergy between the technological security of the infrastructure and the defense of the integrity of digital statehood, thus creating a united front against attempts to destabilize society both externally and internally.

Another integral part of digital statehood is hybrid political agendas that reflect the organic interconnection of the physical and digital worlds. This is followed by electronic elections (e-elections), which represent a technologically advanced tool for secure, transparent and inclusive participation of citizens in democratic processes. Together, these elements ensure that political activity and the act of voting are fit for the dynamics of the 21st century, while guaranteeing the integrity and indisputability of election results thanks to a robust digital infrastructure.

This entire complex system is integrated through the Central Cyber Shield, which performs an indispensable dual function. On the one hand, it ensures the technical protection of the

infrastructure, while on the other hand it protects digital statehood itself as a carrier of democratic values. It is this ability to simultaneously connect and defend both of these planes that makes the Central Cyber Shield a key tool for ensuring the stability, sovereignty and security of modern digital civilization.

Digital statehood thus represents not only a technological innovation, but above all a fundamental shift in civilization. Without building it, the state remains critically vulnerable – not only technically, but especially in terms of values, trust and legitimacy. These areas are absolutely crucial for the long-term stability and functioning of democracy. Thus, in the modern era, the absence of digital statehood means a resignation to protecting the very essence of a free society in an environment that today determines our future.

Section 9

The immunity system of democracy

The immunity system of democracy is part of an integrated political, security, value and legal system. It is primarily about building and developing trust in democracy, which is a fundamental prerequisite for the resilience of the state and international institutions such as the EU, NATO and others. As an integral part of the Central Cyber Shield, this system represents a set of active mechanisms that protect the democratic system from internal decay, authoritarian tendencies, populism and extremism. It is the fundamental structure that ensures the security, social, economic, environmental and legal stability of the state and the international order through a digital democratic infrastructure.

The immunity system of a democracy functions similarly to the immunity system of the human body. If it is strong, it can naturally resist external and internal threats, stabilize social relations and maintain the cohesion of society. However, if it is weakened, the democratic system loses its ability to recognize and eliminate destructive influences, leading to the gradual destabilization of the entire social and political environment.

A critical moment in the breakdown of the immunity system of democracy is when citizens are no longer able to reliably distinguish between truth and lies. This state of affairs is a direct result of the systematic spread of disinformation, manipulation of public opinion, hatred and propaganda that is flooding cyberspace on a massive scale. In an environment where there is no clear and credible frame of reference for reality, information disorientation occurs, which fundamentally affects the decision-making of individuals and society as a whole.

This disorientation gradually grows into a deep distrust that distorts interpersonal relations and the relationship of citizens to the state. People begin to confront each other on the basis of different interpretations of reality, which leads to increasing conflicts, quarrels and, gradually, hatred. This hatred then escalates into radicalization, aggressive behavior and physical violence. Society is thus entering a state of internal disintegration, when it ceases to function as a coherent whole.

In this context, an information war is being waged not only between states, but above all within societies themselves. Its actors are not only political or state structures, but also citizens themselves, who – often unwittingly – become part of the dissemination of manipulative content. Information warfare thus fundamentally weakens the immunity system of democracy by systematically eroding trust as its basic building block.

From this information war, a phenomenon known as disinfocracy is gradually taking shape – the most destructive hybrid regime of the 21st century. This regime is based on a systematic and long-term distortion of the information environment aimed at destabilizing society through chaos, mistrust and polarization. Disinfocracy does not act once, but continuously – it erodes trust and thus disintegrates the entire immunity system of democracy.

The consequences of this action are profound and complex. Family and community ties are breaking down, conflicts between individuals and groups are increasing, and fear, frustration, powerlessness and hopelessness are spreading. At the same time, the security, social, economic and legal stability of the state is weakening. Information disorientation leads to poor personal and political decisions that further deepen the destabilization of society.

Disinfocracy attacks directly the immunity system of democracy – that is, trust. As trust declines, society's ability to resist manipulation and maintain democratic order weakens. The weaker the trust, the faster the breakdown of democratic structures. This process is acceleratory: weakening trust leads to the further spread of disinformation and conflict, which in turn further weakens trust.

In an extreme case, the immunity system of a democracy can collapse completely. In such a state, society is no longer able to distinguish between legitimate and illegitimate information, between truth and manipulation, or between democratic and undemocratic principles. The result is the breakdown of the democratic system as such, because without trust, democracy cannot be sustained or restored.

Protecting the immunity system of democracy is therefore one of the highest priorities of the modern state and the international community. It is not just about protecting the information space, but about protecting the very essence of the democratic establishment. A key instrument of this protection is the establishment of a functional political, security, value and legal system in cyberspace that can systematically strengthen trust, stabilize the information environment and resist the destructive effects of disinfocracy through the Central Cyber Shield.

Without this system and its Central Cyber Shield, a free society remains vulnerable and its immunity system gradually fails under the onslaught of foreign interests and chaos. On the contrary, its establishment and consistent implementation are the basic prerequisite for maintaining the stability, security and long-term existence of the democratic order in the conditions of digital civilization.

Section 10

Concept for the establishment and operation of the Central Cyber Shield

---

The establishment of the Central Cyber Shield is a fundamental step in civilization that cannot be reduced to a technological or security initiative. It is about the creation of a new global institution, which must have not only a digital form, but above all a real, physical one. This Shield must be built as a large, highly secure technological complex, located in a democratic country, which will become the central control and coordination node for the protection of democracy in cyberspace. It is not an ordinary institution, but a giant international center, unparalleled in its size, significance and function in modern history.

This complex must be conceived as a large-capacity infrastructure that will house several thousand top experts from all over the world. The highest level of human know-how in the fields of cybersecurity, protection of democratic processes, political systems, law, data analysis, information operations and strategic management is concentrated in one place. It is this concentration of expertise that is crucial, because the current state of affairs, where these capabilities are dispersed across states and institutions, leads to fragmentation, slow responsiveness and low effectiveness in addressing global threats.

The Central Cyber Shield must be conceived as a space where all states interested in protecting their citizens, their sovereignty and their digital statehood will be represented. It is not exclusively about democratic countries, although they should be the ones to give birth to it. Cyberspace is global and indivisible and therefore its protection cannot be limited to one group of states. On the contrary, this system must be open to other countries that want to ensure the stability of their environment and to counter hybrid threats that know no borders. Every state, every international institution, every organization that is responsible for the security, stability and functioning of society must have the opportunity to participate and be part of this system.

This center must bring together government structures, security forces, intelligence services, cyber specialists, cyber counter-intelligence, international organizations, defense alliances, technology companies, research institutions, think tanks, strategic services, as well as experts in the protection of democratic values, freedom of expression and human rights. The whole must function as one coordinated organism, capable of responding in real time to any threat, not only at the level of individual states, but at the level of the entire digital civilization.

The physical existence of this center is crucial not only in terms of operational management, but also in terms of legitimacy and trust. It creates a clearly defined global authority, not based on a dictate of power, but on a shared responsibility to protect democracy, human rights and the stability of society. In an environment where trust is being systematically eroded through disinformation, manipulation and information warfare, the existence of such a center is crucial to restoring citizens' trust in the democratic system.

A fundamental principle of the Central Cyber Shield is the separation and close interconnection of two basic areas that are not sufficiently coordinated today. The first area is technical infrastructure protection, i.e. protection of networks, data flows, communication systems, critical infrastructure, public and private digital systems and overall cyber security. The second area is the protection of the very essence of democracy, i.e. the protection of trust, legitimacy, freedom of expression, the rule of law and the resilience of society to disinformation, hatred, propaganda and manipulation of public opinion.

These two areas cannot be separated because technical security without value system protection cannot prevent the disintegration of society, and conversely, value protection without technological security is unable to counter modern hybrid threats. It is only by linking them in one integrated system that a truly functional defense mechanism capable of protecting democracy as a whole is created.

At the same time, the Central Cyber Shield is a key pillar for building the digital democratic infrastructure on which ONLINE DEMOCRACY is based as a new integrated political, security, value and legal system in cyberspace. This system will make it possible to link the digital and physical worlds into a single functional unit in which democratic processes are legitimate, transparent and resistant to manipulation. Without the existence of this center, it would not be possible to effectively build, manage or protect such a system.

In a broader context, the Central Cyber Shield is thus contributing to the emergence of a new form of global order that responds to the realities of the digital age. This new world order is not based on traditional power structures, but on the interconnection of technology, values and law within a unified system that protects not only states, but above all individuals. Every person on the planet has the right to the protection of their life, health, dignity and freedom, not only in physical space but also in the digital space that has become an integral part of human existence.

Without the construction of the Central Cyber Shield, the contemporary world remains fundamentally imbalanced. Political, security and legal systems exist only in the physical world, while cyberspace, where most communication and decision-making takes place, remains without a corresponding systemic framework. This state of affairs is unsustainable in the long term and is the main cause of the emergence and escalation of hybrid threats that are being transferred from the digital environment to reality in the form of conflicts, violence, destabilization of states and weakening of democracy.

Therefore, it must be clearly stated that the Central Cyber Shield is not an optional project, but an absolute necessity. Without its existence, neither the security, stability nor the future of modern civilization can be assured. This project represents a historic opportunity to create a workable, legitimate and globally coordinated democracy protection system that meets the challenges of the 21st century and is capable of protecting not only states but the very fabric of human society.

The Central Cyber Shield is designed as a comprehensive international system that integrates the political, security, values and legal framework of digital statehood. This system functions as the global brain of democracy, whose purpose is to protect the sovereignty of states, the stability of the democratic order, the defense of the immunity system of democracy and the

prevention of hybrid threats in cyberspace. For the system to be effective, each state and key international institution must be fully represented, with each representation having a clearly defined role, responsibility and area of operation.

Ministries of Defense play a vital role in protecting the nation's military networks and cyber infrastructure. Their task is not only to provide defense against cyber attacks on military systems and equipment, but also to guarantee secure and reliable communication between the various components of the army. In the digital age, where cyber attacks can threaten not only military effectiveness but also the very sovereignty of the state, this activity becomes existentially important. Ministries of Defense therefore do not operate in isolation; they work closely with alliance defense structures, particularly NATO Member States and other defense coalitions, to share information on current threats, coordinate defense operations and ensure a unified and effective response to crisis situations. This cooperation allows each state to not only effectively protect its military capabilities, but also to maintain compatibility and connectivity with partners' defense systems, which is critical to the functioning of collective defense. Thus, a key role of defense ministries is to maintain the state's ability to respond to cyber conflicts, prevent the destabilization of military and political structures, and at the same time contribute to the overall security of the democratic world through integrated linkages with other states and their defense mechanisms. In the context of the Central Cyber Shield, the role of the Ministries of Defense is significantly expanded, as the Shield provides a unified framework that enables the sharing of key data, the coordination of defense measures and the collective protection not only of military networks but also of the entire democratic infrastructure in physical and digital space.

Ministries of the Interior have a fundamental responsibility to protect public safety in cyberspace and to prevent cybercrime, which threatens the daily lives of citizens and the stability of society. Their activities include coordinating the state police and other security forces in detecting threats, investigating cyberattacks, and securing critical information flows. In the digital age, when disinformation, extremist ideologies and radicalization spread at an incredible speed through social networks and online platforms, interior ministries must not only respond to attacks already underway, but actively monitor and anticipate new threats. Their remit also includes monitoring disinformation campaigns and cyber activities that can destabilize public discourse, increase social tensions and threaten citizens' trust in state institutions and democratic processes. Ministries of the Interior therefore not only detect and neutralize digital threats, but also support the stabilization of public space and democratic discourse, thereby ensuring the protection of citizens and the integrity of state institutions.

Within the Central Cyber Shield, the role of the Ministries of the Interior is significantly strengthened, as the Shield enables coordinated interconnection with other state and international institutions, including the defense structures of NATO and other democratic states. The system provides a unified framework for monitoring, preventing and responding to hybrid threats and disinformation, creating an environment in which the Home Office can effectively protect public safety and the stability of digital and physical society. This ensures that citizens, institutions and democratic processes are protected not only from physical but also from cyber threats, which is essential for the long-term stability and security of the democratic world.

Ministries of Justice play a key role in creating and overseeing the digital laws and legal frameworks that are necessary to protect democratic infrastructure in cyberspace. Their remit includes not only the development of legislation governing digital statehood, but also the development of modern legal norms that incorporate the principles of ONLINE DEMOCRACY, including a digital constitution and rules for the legitimate functioning of political, security and value processes in the digital space.

The Ministries of Justice also provide legal support in the event of cyber-attacks, the spread of disinformation, the manipulation of public opinion or other forms of hybrid threats that may threaten the stability of the state and citizens' trust in democratic institutions. Their work ensures that the state's response to cyber threats is not only effective, but also consistent with the rule of law, human rights and respect for the dignity of the individual.

In the context of the Central Cyber Shield, the Ministries of Justice form the legal backbone of the entire structure. Through coordination with other ministries, defense institutions, security forces and international organizations, including NATO Member States and other democratic countries, they enable the uniform implementation of legal measures at national and international level. This ensures that the protection of democracy in cyberspace is not merely fragmented, localized or selective, but functions as a comprehensive, coordinated and legitimate system that protects more than five billion Internet and social network users while promoting long-term stability, security and trust in democratic processes.

Ministries of finance play a vital role in protecting the digital economy and ensuring the stability of a country's financial systems. Their work includes protecting digital payment systems, securing financial transactions and monitoring banking networks, which are increasingly exposed to sophisticated cyber-attacks and hybrid threats. In the digital age, where financial transactions are conducted in real time through online platforms and global networks, their activities are a fundamental pillar of protecting national and international economic stability.

At the same time, ministries of finance coordinate with international financial institutions, central banks and other national and international entities to ensure a unified defense against cyber fraud, financial manipulation and attempts to destabilize the economic system. Such cooperation enables rapid exchange of information on threats, coordination of preventive measures and effective response to crisis situations.

As part of the Central Cyber Shield, ministries of finance ensure that the economic and financial components of the digital democratic infrastructure are linked to the other pillars of the Shield. This integrated system not only enables the protection of financial flows, but also supports the stability of digital statehood and the overall security of the state. In this way, the Central Cyber Shield creates a coordinated and comprehensive defense that protects the financial system of democratic states – including EU Member States, other democratic countries and NATO Member States – and ensures that economic stability is not compromised by cyber attacks, manipulation or disinformation campaigns.

Thus, the key role of ministries of finance is to maintain the financial stability of states and protect the economic system, which is now inextricably linked to the protection of democracy and legitimate decision-making processes in the physical and digital world. The Central Cyber

Shield ensures that this stability is long-term, coordinated and resilient to complex hybrid threats, enabling democratic states to function effectively in a global digital civilization.

State security forces are a key element in protecting the digital and physical integrity of the democratic system and are an integral part of the Central Cyber Shield. The police ensure the security of public networks and protect citizens from cyber threats, detect online crime, monitor disinformation campaigns and radicalization, and thus stabilize public discourse. National counterintelligence specializes in preventing infiltration by foreign actors, hybrid threats, and sophisticated cyber operations that could threaten national security and public confidence in democratic institutions. Intelligence services provide a strategic overview of international cyber activities, detect high-risk threats and provide early warning to state authorities, enabling a coordinated defense against complex attacks. Cyber units have the capabilities to respond immediately to cyber attacks, take preventive measures and active defense, thus preventing the spread of destabilizing processes into the physical world.

Each of these components provides specialized expertise and specific tools for the area it covers. However, for the effective protection of democracy and the stability of the state, it is not enough to operate in isolation – that is why all security forces are fully interconnected through the Central Cyber Shield. This integrated system allows for coordinated action, immediate exchange of information, a unified defense strategy and effective response to hybrid threats, thus creating a real mechanism for collective protection of democratic infrastructure not only for EU and NATO Member States, but also for other democratic countries and international institutions.

Through this coordination, the Central Cyber Shield ensures that security forces are not just a tool to protect physical space, but that together they form a robust defense system that connects the cyber and real worlds, stabilizes decision-making processes, protects citizens and democratic infrastructure, while ensuring long-term resilience to sophisticated and global cyber threats.

Digital law legislative and expert teams are a fundamental pillar of the legal protection of democracy in cyberspace and act as a key tool of the Central Cyber Shield. These teams develop and update standards for digital laws, regulations and digital constitutions that form the legal framework for the functioning of ONLINE DEMOCRACY. They create legal structures that enable the state, institutions and citizens to operate safely in the digital space, protecting their rights, freedoms and democratic principles, while providing tools for effective defense against disinformation, manipulation and hybrid attacks.

The teams also contribute to the development and implementation of international agreements on digital statehood, coordinate with other democracies and international organizations, and ensure that legal frameworks respect the universal values of human rights, freedom of expression and the rule of law. This legal basis is essential for the operation of the Central Cyber Shield, because the protection of democracy cannot exist on the basis of technical measures, regulations or isolated tools alone – it requires a comprehensive, legally anchored system that links the digital and physical worlds.

A key role of these teams is to ensure that all processes of defense and protection of democratic infrastructure have a solid legal framework and that the collective protection of

democracy is not only technically but also legally assured. Without the existence of this legal pillar, cyber protection would be inadequate, as democratic processes, citizen trust and the legitimacy of national decision-making – including by EU and NATO Member States and other states – would remain vulnerable in cyberspace. Thanks to these teams, the Central Cyber Shield is able to provide the long-term, coordinated and legally anchored protection that is absolutely essential for the survival of democracy in both the physical and digital worlds.

The Central Cyber Shield is not just a national or regional initiative; it is a comprehensive international platform, with key multinational organizations, alliances and security structures working together to ensure coordinated protection of democracy in cyberspace. In this platform, the European Union is a key partner, coordinating digital legislation, cybersecurity standards and the protection of democratic processes between Member States. In this way, the EU ensures a single framework and harmonization of rules, which is essential for the effective protection of democratic infrastructure in all Member States.

The NATO Alliance engages through military and cyber strategies, providing the necessary support to defend Member States against hybrid and cyber threats. In this context, it is absolutely necessary to extend the existing Article 5 with a digital Article 5. At the same time, the Central Cyber Shield fills a crucial gap, because while NATO Member States have Article 5 for collective defense in the physical world, no similar coordinated collective defense in cyberspace exists to date. This platform thus enables the implementation of digital collective defense that includes not only EU and NATO Member States, but also other democratic countries and key international actors, thus ensuring the protection of democracy and the stability of states in virtual space.

The United Nations provides a global framework for respecting human rights, freedom of expression and international law, strengthening the legitimacy and legal integrity of digital democratic processes. The International Monetary Fund and the World Bank are focusing on protecting digital financial systems, coordinating economic resilience and preventing the destabilization of states through cyber threats, allowing economic infrastructure to remain secure and stable in the digital space. Interpol and Europol then provide international support in detecting cybercrime, monitoring disinformation networks and coordinating security operations across borders, thereby making a significant contribution to preventing the escalation of hybrid threats into the physical world.

Other international organizations, including regional defense alliances, regulatory and standard-setting bodies, human rights institutions and expert groups on hybrid threats, are an integral part of this system. Each organization has a clearly defined role and responsibility, ensuring the integrity of the platform and coordination at a global level. In this way, the Central Cyber Shield enables the interconnection of political, security, values and legal frameworks across states and organizations, creating the first truly collective defense of democracy in cyberspace, which is existentially necessary for the stability of digital civilization and the protection of democracy in the physical world.

The Central Cyber Shield integrates into its structure key technology and research institutions that provide the expertise and tools necessary to effectively protect the digital democratic infrastructure. Technology companies have a vital role to play in developing and operating tools for network monitoring, data analytics, cyber threat detection, and securing cloud

systems and digital identities. Their expertise enables them to predict attacks, identify security weaknesses and respond quickly to crisis situations, ensuring the continuity and security of digital statehood.

Research and academic institutions are focusing on predictive threat modelling methodologies, crisis management scenarios and tools for stabilizing public discourse. Their work is critically important, as it allows them to anticipate hybrid attacks and disinformation campaigns that can destabilize not only cyberspace but also the physical world. These institutions provide the analytical basis that enables state authorities, security forces and international organizations to address complex threats in a coordinated manner.

Analytical centers and cyber security experts ensure uniform standards of defense, monitor cyber attacks and provide rapid incident response. Their activities link technological expertise with the operational structures of national and international security, enabling effective information sharing, coordination of defense operations and immediate resolution of crisis situations.

Psychological and sociological experts complement this structure by analyzing the impact of disinformation on public opinion, assessing the risks of radicalization and supporting the so-called immunity system of democracy. Their role is essential for understanding the social and psychological impact of hybrid threats that spread through social networks and digital platforms, and for developing strategies that minimize the destabilization of society and undermine trust in democratic processes.

The existence of an international medical consilium directly in the operational center of the Central Cyber Shield is necessary because the current threats in cyberspace no longer attack only technical infrastructure, but target the biological and psychological integrity of the population. The presence of high-end medical capabilities at the point of command will enable the immediate identification and neutralization of bio-cyber attacks that can cripple healthcare systems through digital networks or directly threaten the lives of patients in cyberspace. This consilium also functions as a diagnostic and defensive body against sophisticated psychological operations that aim to cause mass stress and mental disintegration of society. The integration of medical expertise into digital national defense thus ensures that the protection of human health and the preservation of the psychological stability of the population are a priority part of collective security throughout the international order.

Together, these technological and research entities form an integral part of the Central Cyber Shield, which thus acquires multidisciplinary capabilities for prevention, detection, response and mitigation of threats in cyberspace. This integrated system is necessary to ensure the collective defense of democracy not only of NATO Member States, but also of the European Union and other countries. Without the coordination and cooperation of these technological and scientific institutions, it would be impossible to effectively protect democratic infrastructure and maintain citizen confidence in the safe and stable functioning of national and international systems.

Through this interconnected structure, the Central Cyber Shield thus creates a unified, functional and legitimate framework for the protection of democracy, replacing the

fragmented, uncoordinated and short-sighted approaches of individual states or organizations. The integration of technological and research institutions is therefore crucial to ensure the continuity of democratic processes in cyberspace and to protect democratic civilization, whose stability is existentially dependent on the reliable functioning of ONLINE DEMOCRACY.

The Central Cyber Shield integrates specialized teams focused on the creation of digital legislation and value systems that ensure the legal and value stability of ONLINE DEMOCRACY. The teams for the digital law create a comprehensive legal framework that enables the protection of cybersecurity, civil rights and national sovereignty. This framework replaces the fragmented and uncoordinated legislation that is often fragmented and ineffective across countries today. Thanks to the centralized structure of the Central Cyber Shield, all states, institutions and international organizations are able to draw on a unified and functional legal system that ensures legitimacy, coordination and effective defense against hybrid threats.

The teams for the digital constitution define the basic principles of digital statehood and the functioning of democratic processes in cyberspace. They are responsible for codifying the rights and obligations of all participants in the digital environment, ensuring the transparency of decision-making processes and protecting the integrity of democratic structures. The digital constitution creates a stable foundation for the collective defense of democracy in cyberspace, which is as critical as traditional military defense. Without such defined principles, NATO Member States, European Union Member States, as well as other countries, would not be able to effectively coordinate the protection of democratic processes or respond to sophisticated cyber attacks.

Experts on the protection of democratic values focus on maintaining and strengthening the so-called immunity system of democracy. Their task is to monitor public discourse, analyze the impact of disinformation campaigns and prevent destabilizing attacks that could undermine citizens' trust in democratic processes. These experts develop methodologies that link legal, security and value frameworks, thus enabling effective prevention of the destabilization of democracy. Their work is an integral part of the ten pillars of the Central Cyber Shield and contributes to the long-term stability and cohesion of digital and physical society.

The Central Cyber Shield, through these teams, thus provides integral support for the collective defense of democracy in cyberspace. It is not just about protecting individual states or alliances, but about ensuring the integrity of democratic processes globally, which are existentially dependent on a stable and coordinated legal and value system. This structure replaces ineffective directives, bans and local regulations, which alone cannot provide real security and stability for democratic states.

The integration of the teams for the digital law, the digital constitution and experts in the protection of democratic values creates a unified legal and values framework that supports a coordinated defense against hybrid threats, disinformation and cyber attacks. This framework enables states and international organizations to collaborate effectively, share information, develop prevention strategies and ensure a stable, legitimate and trusted digital space.

This robust interdisciplinary complex represents an unprecedented integration hub, with direct representation from all relevant ministries, expert teams and specialists across the spectrum of government. Its uniqueness lies in its global reach: the Central Cyber Shield includes not only EU and NATO Member States, but also partners from Africa, Asia and other regions who share a common interest in protecting digital statehood, sovereignty and state legitimacy in cyberspace.

Part of this apparatus is an international medical and professional consilium that, in addition to technological experts, ensures the protection of the biological and psychological integrity of the population. This broad international cooperation enables real-time sharing of data and defense protocols, creating a global digital alliance.

Overall, this Central Cyber Shield structure is the pillar on which the protection of democracy in cyberspace rests and on which the future of democracy in the physical world is existentially dependent. Without it, it would not be possible to ensure a coordinated and effective collective defense of democratic states or the stability of public discourse, making it an essential part of the ten pillars of the Central Cyber Shield.

Section 11

The building of the Bohemia: Central Cyber Shield gigacenter

The Central Cyber Shield, housed in an imposing building known as “Bohemia: Central Cyber Shield”, will be a truly unique project aimed at developing an innovative, comprehensive and integrated political, security, value and legal system – ONLINE DEMOCRACY – in cyberspace. This building will not just be an administrative headquarters, but will become a monumental, architecturally and functionally exceptional center of global significance, unparalleled in the world. It will be a structure of a unique format, designed to be a physical and symbolic pillar for the protection of democratic values in the digital age, where thousands of experts, analysts, security specialists, lawyers, technology leaders and government representatives from around the world will meet every day.

Within Bohemia: Central Cyber Shield all key components of the state and supranational structures will be represented – ministries of defense, interior, justice and finance, security and intelligence services, legislative and expert teams of digital law, technology and research institutions, international organizations and alliance partners. This highly complex ecosystem will be linked through a single infrastructure of data sharing, decision-making and operational coordination, enabling the emergence of a fully integrated mechanism for the collective defense of democracy in cyberspace.

The Bohemia: Central Cyber Shield building itself will be designed as a highly secure, autonomous and logistically self-sufficient unit. Its status will be that of a neutral international territory, administered by a global agreement of democratic states. The security of this area will be provided by specialized units composed of representatives of security structures from all over the world, thus guaranteeing the maximum degree of independence, credibility and protection from any external influences.

In terms of security architecture, Bohemia: Central Cyber Shield will represent the most advanced level of protection ever created. The facility will be equipped with multi-layered security systems, including physical protection, cyber defense, biometric access mechanisms, continuous surveillance and predictive analytics tools. All processes inside the building will be subject to 24-hour monitoring and real-time evaluation, using the latest artificial intelligence and data analytics technologies. This system will enable the immediate identification and neutralization of threats that could jeopardize the stability of democratic processes on a global scale.

Extensive logistical and infrastructural facilities will also be an essential element. As thousands of experts from different countries will be working in Bohemia: Central Cyber Shield, the complex will include a fully integrated system of housing, healthcare, administrative services, educational and research capacities and other support structures. These elements ensure not only high efficiency but also the long-term sustainability of the entire system. Employees and collaborators will have an environment that meets the highest standards of security, comfort

and professional support, which will be essential to meet the extreme challenges of protecting more than five billion users of the digital space.

Bohemia: Central Cyber Shield will also represent the first ever global center that will systematically protect the digital statehood, sovereignty and legitimacy of individual countries in cyberspace. In an environment where more and more political, social and economic processes will take place online, the protection of democracy in the digital dimension will become directly determinant for its survival in the physical world. It is in this context that it will be absolutely essential in the digital age that such a center exists, because without it it will be impossible to ensure the stability and security of democratic systems on a global scale.

A key lesson from the past will be that isolated regulations, directives or restrictive measures could never ensure stable and long-term functional protection of democratic values. The fragmentation of approaches between states has led to information chaos, weakened public trust and an increase in hybrid threats. Bohemia: Central Cyber Shield will overcome this fundamental deficiency by creating a single, value-based and legally consistent framework in which all activities are coordinated at a global level.

The fundamental importance of this center will also lie in the fact that for the first time in history a true equivalent of collective defense in cyberspace will be created. While traditional security alliances provide protection in the physical world, Bohemia: Central Cyber Shield will bring an analogous principle to the digital dimension. It will enable instantaneous information sharing, coordinated threat response and joint strategic planning, thereby fundamentally increasing the resilience of democratic systems to sophisticated attacks, disinformation and manipulation of public opinion. In the digital era, which will define how society functions for centuries to come, the world simply cannot do without this center.

The whole complex will function as a dynamic, constantly evolving organism that will link technology, law, security and the value framework of democracy into a single whole. Every decision, every operation and every strategic initiative will be based on a single system that ensures transparency, accountability and long-term stability. This approach will allow not only to respond to current threats, but also to prevent them systematically.

Bohemia: Central Cyber Shield will thus represent not only the technological peak of its time, but above all a new standard of protection for the democratic world. It will become a symbol of global cooperation, trust and shared responsibility for the future of democracy. In the digital age, when cyberspace will be the main battleground for the shape of public discourse, the legitimacy of institutions and the stability of states, the existence of this complex will be irreplaceable and its construction will be a necessity for at least the next century, at least for the horizon of five hundred years.

The creation of this center will prove that democratic states are capable of overcoming fragmentation, unifying their capacities and creating a system that will meet the challenges of the 21st century and the distant future. Bohemia: The Central Cyber Shield will not just be a building – it will become a symbol of the determination to protect democracy in its most vulnerable, yet most important dimension. It will be the place where the stability of the world, the trust of citizens and the future of freedom itself will be decided on a daily basis.

Section 12

Global Security Center for the Protection of Democracy

Current and future societal development is characterized by the full coexistence of the physical and digital spheres in which citizens live, communicate and make decisions simultaneously. This duality fundamentally affects the stability of democratic systems, with cyberspace being the dominant source of hybrid threats that are subsequently transmitted to the real world. In response to this systemic imbalance, the establishment of the Global Security Center for the Protection of Democracy is a key tool for ensuring comprehensive security in both these dimensions.

The Global Security Center for the Protection of Democracy is the world's foremost authority on the protection of democratic principles. It will not be a superior body to the states in the sense of direct exercise of power, but will act as the ultimate reference and decision-making framework from which states, governments and citizens will draw binding principles, standards and strategic direction.

Decisions taken at the level of the Global Security Center for the Protection of Democracy will subsequently be implemented through national legislation, security measures, economic instruments and institutional mechanisms, thus ensuring their consistent application in practice. As a consequence of this systemic set-up, it will be essential that all policy activities at national and international level are conceived and implemented from the moment of the establishment of the Center in direct relation to its strategic framework.

Political decision-making will now take place in an environment where every single step – be it in security, economic, social, health, legal or environmental policy – will be inextricably linked to the protection of democratic processes. Therefore, political leaders will need to take into account the principles, recommendations and direction defined by the Global Security Center for the Protection of Democracy and actively align their actions with this framework. This approach will not be a limitation of their work, but rather a major streamlining, simplification and acceleration of their work, providing a unified, expert-based and long-term stable basis for decision-making.

At the same time, this model will require ongoing coordination and consultation between national policy structures and the Global Security Center to ensure that individual measures are fully compatible and consistent with the global framework for democracy protection. This coordination will become a key element of governance to eliminate inconsistencies, increase the effectiveness of public policies and ensure that the protection of democracy is integrated into all decision-making processes, regardless of their sectoral focus.

Ensuring this principle will be a top security priority for current and future developments. In an environment where democratic systems face complex threats in both physical and cyber space, there is no alternative way to effectively protect them other than through systematically linking national decision-making to a global governance framework. The

integration of these levels will thus become a prerequisite for the stability, resilience and long-term sustainability of democracy.

The Global Security Center for the Protection of Democracy must not base its activities on restrictive instruments such as blanket bans, directive commands, regulation of digital space or restrictive interference in the free functioning of democratic processes. Such an approach would be in direct contradiction to its core mission and principles. The protection of democracy must not be achieved by restricting freedom, but by building an integrated political, security, values and legal system. It is based on the principle of ONLINE DEMOCRACY, which opens up a new space for transparent, open and accountable functioning of democratic processes in the digital age.

A key role in this process will be played by the expert and organizational structure of the Global Security Center for the Protection of Democracy, which will ensure the preparation of strategic agendas, conceptual materials and decision-making documents. This specialized apparatus will perform a crucial function not only in relation to the Global Center itself, but also in relation to the Central Cyber Shield of Democracy, for which it will provide the necessary analytical, conceptual and organizational background. The staff of this structure will have to be provided with the highest security protection and functional immunity necessary for the performance of their activities, and will be deployed on a 24-hour standby basis, corresponding to the highest security priority. This must be matched by the creation of the most effective institutional, staffing and technological facilities to enable them to act quickly, flexibly and professionally in real time.

This staff and professional structure will bear an extremely high level of responsibility, as its activities will directly affect the quality of decision-making at the global level and the effectiveness of democracy protection as a whole. Its position will be crucial for the functioning of the whole system, as it will provide the link between strategic management, expertise and practical implementation of individual measures in the global and national context.

A fundamental principle of the Center's operation will be its direct accountability to the world community. The Global Security Center will systematically, transparently and fully inform citizens about its decisions, activities and long-term strategies. The world public has an unquestionable right to access this information, as citizens are the bearers of democratic legitimacy. This principle will not only ensure control over the Center's activities, but also strengthen trust in democratic processes and active citizen participation in their protection.

The Global Security Center for the Protection of Democracy will include the Central Cyber Shield of Democracy, which will form its key pillar in the digital space. These two pillar institutions will be housed in a single, comprehensive and highly secure institutional building that will constitute a global hub for the management of democracy protection. This physical and functional integration will ensure maximum efficiency, coordination and continuity between strategic decision-making and expertise.

The Central Cyber Shield of Democracy will act as an expert, advisory and design pillar that will systematically provide the Global Security Center with suggestions, proposals, recommendations and strategic materials necessary for decision-making on the protection

and development of democracy. Based on these outputs, the Global Security Center will make key decisions, define rules and set long-term direction. At the same time, it will provide this Shield with all the necessary background across the political, security, legislative, economic and value levels, thus creating a unified and coherent management system.

National Security Centers for the Protection of Democracy will gradually be established in each country, where the relevant competences, agendas, institutional capacities, professional services and staffing of the existing institutions and authorities working in the field of democracy protection, security and related policies will be systematically integrated and transferred. This process of centralization and unification of management will lead to a substantial streamlining of the state's activities, elimination of duplication, acceleration of decision-making processes and an increase in overall security resilience.

This model will not only increase the effectiveness of the protection of democratic processes and the security of citizens, but will also lead to significant economic savings. Member States, including those of the European Union and NATO, will be able to save significant amounts of money in their national budgets, in the billions each year, while improving the quality of governance and the protection of democracy.

At the same time, the Global Security Center for the Protection of Democracy will organize regular Global Democracy Summits where national leaders will assess progress, identify weaknesses and take further strategic decisions. This will ensure the continuous adaptation of the system to new challenges and the dynamic development of the security environment.

The whole concept will create a unified, long-term sustainable and systemically coherent framework capable of responding to current and future threats. The Global Security Center for the Protection of Democracy will thus become a key pillar for the protection of democratic values and their stable development, ensuring that democracy is effectively protected both in the physical world and in cyberspace.[29, 30, 31, 32, 33]

10 ALLIANCE SECURITY PILLARS OF THE CENTRAL CYBER SHIELD

The Central Cyber Shield is built on 10 Alliance security pillars that form an integrated system and a comprehensive security and governance architecture for cyberspace, complementing and harmonizing existing digital regulatory and security frameworks, including fragmented national approaches. This system represents a key coordination and protective framework for cybersecurity, on whose functional integrity the strategic stability, trust and defense capability of member states depend fundamentally. European Union and The North Atlantic Treaty Organization . In a broader context, its stability is of fundamental importance for the security balance in both digital and physical space, on which the resilience of the current international security environment is built.

---

1. **ONLINE DEMOCRACY**
   The first political system operating in cyberspace, enabling the active involvement of citizens in democratic processes in the digital environment.

2. **Digital Democratic Infrastructure**
   A unified platform ensuring collective defense and stable functioning of democratic institutions in cyberspace.

3. **Politinn**
   social network The first European platform of the new generation focused on the protection and development of democracy in cyberspace.

4. **Cyber Strategy 2026 – Combating Disinfocracy**
   A strategic framework for countering “ disinfocracy ,” one of the most destructive hybrid threats of the 21st century that threatens democratic processes and public trust.

5. **Central cyber shield for NATO.**
   Extension of the principle of collective defense to the cyberspace dimension through the implementation of digital Article 5.

6. **Digital World Organization (DWO)**
   An international institution ensuring the protection and development of digital civilization, consisting of more than five billion users of the Internet and social networks, with the aim of protecting the physical world.

7. **Cyber Strategy 2026 – Fighting "digital cancer"**
   An initiative aimed at protecting the physical and mental health of citizens of EU

and NATO member states from the negative impacts of the digital environment.

8. **Cyber Strategy 2026 – Cyber Rearmament of EU and NATO Member States**

Strengthening the technological, security and defence capacities of EU and NATO Member States. The aim is to effectively protect and ensure the integrity of digital statehood, sovereignty, national identity and legitimacy of states in the online environment. It also includes the protection of critical infrastructure and key state institutions from targeted and coordinated hybrid attacks.

9. **Cyber Strategy 2026 – Combating social terrorism**

Measures aimed at preventing radicalization, hatred and violence spread through social networks.

10. **Building a security, legal and especially value system in cyberspace:** A key


part of protecting democratic values is the systematic building of a value framework based on the principles of democracy, not only in the physical world, but especially in the digital space, where the global hybrid war of the 21st century is taking place. Trust in democratic principles, institutions and allied relations represents one of the fundamental pillars of the security, social, economic, environmental and legal stability of democratic states. For this reason, the international initiative "Democratic Personality of the Year" is being created, the mission of which will be to build and develop a value system that protects and strengthens trust not only between allies, but also within democratic societies, and thus contribute to increasing the defense capability of alliance structures, strengthening information resilience and reducing the vulnerability of member states to destabilizing influences.

    The first ever edition of the prestigious “Democratic Personality of the Year” award will be officially launched on September 15th, on the occasion of the International Day of Democracy, in the form of a press conference in the Czech Republic. This moment marks the beginning of a new global tradition of the “celebration of democracy”, which aims to create the most important international platform for the celebration of democratic principles, shared values, civic responsibility and the public good in the modern era. The Czech Republic thus becomes the founding country of this new democratic tradition of the digital age, which has the ambition to gradually connect democratic states and citizens across the world through the sharing of common values.

    The actual ceremony of announcing the nominees and presenting the prestigious award "Democratic Personality of the Year" will take place in 2027, again symbolically on September 15. The award will be presented in twelve categories reflecting key areas of the functioning of a democratic society and the protection of the public good, including education, healthcare, social care, politics and public administration, security and rescue services, business, media and new forms of communication, culture and art, sports, science and innovation, law and justice, philanthropy and the environment and animal protection. The aim is to

systematically recognize personalities and citizens whose activities bring demonstrable benefits to society and strengthen trust in democratic values.

The “Democratic Person of the Year” initiative is the first international project of its kind that connects democratic education with the digital environment and modern technologies. At a time when there is no comparable global platform connecting democratic states, citizens of the European Union, NATO and the wider international community through a positive value framework, a new space is being created for sharing inspiration, civic responsibility and mutual respect between people. This concept responds to the growing influence of information chaos, disinformation, hatred, polarization and radicalization in the public space, which are being transferred from cyberspace to the physical world and affecting social cohesion and security.

A key part of the entire initiative is the social network Politinn , which allows citizens to nominate personalities from various areas of public life, but also to mutually recognize ordinary citizens for their concrete contribution to society, civic bravery and performing public good for society and the state. This mechanism creates a new space for highlighting positive role models, sharing experiences and strengthening trust in democratic processes.

The international initiative "Democratic Person of the Year" is emerging in the context of growing hybrid threats. The "Celebration of Democracy" therefore represents a new majestic symbol of democratic culture, applied not only in the physical but also in the digital world. Its basis is civic responsibility, doing public good, respect for one another, mutual support, sharing values and public recognition of those who, within their capabilities and abilities, protect democratic principles and contribute to the development of society and the state.

List of references – sources and literature

[1] https://niss.gov.ua/sites/default/files/2017-01/GW_engl_site.pdf

[2] https://www.demdigest.org/inside-putins-hybrid-war-western-democracy/#:~:text=%E2%80%9CThey've%20got%20the%20vehicle%20to%20do%20this,Western%20democracy%20itself%2C%20he%20writes%20for%20Reuters .

[3] https://report.az/en/other-countries/macron-accuses-russia-of-unleashing-world-hybrid-war

[4] https://www.novinky.cz/clanek/zahranicni-evropa-ruske-hybridni-operace-jsou-predehrou-valky-uvadi-nemecky-armadni-dokument-40556312

[5] https://www.forum24.cz/rusko-zaseva-rozkol-jsme-v-hybridni-valce-prohlasila-von-der-leyenova-evropa-potrebuje-dronovou-zed

[6] https://www.techzpravy.cz/hybridni-valka-uz-zacala-macron-varuje-pred-nebezpecnou-strategii-ruska/

[7] https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

[8] https://www.seznamzpravy.cz/clanek/domaci-politika-ai-uz-ted-meni-prubeh-boje-rika-muz-ktery-nato-

pripravye-na-moderni valceni-302405#dop_ab_variant=0&dop_source_zone_name=zpravy.sznhp.box&source=hp&seq_no=1&utm_campaign=abtest305_podcasty_v_boxiku_varB&utm_medium=z-boxiku&utm_source=www.seznam.cz

[9] https://www.theguardian.com/world/2026/apr/01/trump-says-he-is-absolutely-considering-withdrawing-us-from-nato?utm_source=chatgpt.com

[10] https://ct24.ceskatelevize.cz/clanek/svet/usa-by-nemusely-prijit-nato-v-pripade-potreby-na-pomoc-prohlasil-trump-371802

[11] https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

[12] https://www.ceskenoviny.cz/zpravy/sef-nato-vyzval-staty-aby-letos-presvedcili-ze-zvysuji-vydaje-na-obranu/2804662

[13] https://www.nato-pa.int/document/2025-cybersecurity-report-kairidis-010-cds?utm_source=chatgpt.com

[14] https://www.consilium.europa.eu/en/press/press-releases/2023/12/07/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-the-protection-of-democratic-processes-against-malicious-cyber-activities/?utm_source=chatgpt.com

[15] https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/?utm_source=chatgpt.com

[16] https://www.hybridcoe.fi/publications/countering-disinformation-in-the-euro-atlantic-strengths-and-gaps/?utm_source=chatgpt.com

[17] https://www.consilium.europa.eu/cs/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners/?utm_source=chatgpt.com

[18] https://reference-global.com/article/10.2478/kbo-2025-0014?utm_source=chatgpt.com

[19] https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2026.1790164/full?utm_source=chatgpt.com

[20] https://www.seznamzpravy.cz/clanek/domaci-politika-ai-uz-ted-meni-prubeh-boje-rika-muz-ktery-nato-pripravuje-na-moderni-valceni-302405#dop_ab_variant=0&dop_source_zone_name=zpravy.sznhp.box&source=hp&seq_no=1&utm_campaign=abtest305_podcasty_v_boxiku_varB&utm_medium=z-boxiku&utm_source=www.seznam.cz

[21] https://www.atlanticcouncil.org/dispatches/to-adapt-to-todays-security-threats-nato-should-prioritize-the-basics-of-defense-innovation/?utm_source=chatgpt.com

[22] https://www.researchgate.net/publication/394754993_NATO'S_MECHANISMS_FOR_THE_GOVERNANCE_OF_CYBERSECURITY

[23] https://commission.europa.eu/news-and-media/news/stronger-measures-protect-our-democracy-and-civil-society-2025-11-12_en?utm_source=chatgpt.com

[24] https://chinamediaproject.org/2026/04/01/ai-for-human-propaganda/

[25] https://en.wikipedia.org/wiki/Xinhua%E2%80%93Sogou_AI_news_anchor?utm_source=chatgpt.com

[26] https://ny1.com/nyc/all-boroughs/ap-top-news/2024/05/24/chinas-latest-ai-chatbot-is-trained-on-president-xi-jinpings-political-ideology?utm_source=chatgpt.com

[27] https://www.idnes.cz/technet/vojenstvi/putin-na-ukrajina-nacvicuje-nova-valka-online-maskirovka.A140703_163345_vojenstvi_kuz

[28] https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats#:~:text=Malign%20actors%20routinely%20conduct%20hostile%20information%20operations,and%20build%20resilience%20against%20these%20information%20threats

[29] https://ct24.ceskatelevize.cz/clanek/svet/porota-v-usa-shledala-google-a-metu-odpovednymi-v-pripadu-zavislosti-na-sitich-371703

[30] https://ct24.ceskatelevize.cz/clanek/veda/proti-sireni-dezinformaci-selhava-vetsina-znamych-strategii-upozornuje-studie-7229

[31] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en?prefLang=uk&utm_source=chatgpt.com

[32] https://www.oecd.org/en/topics/disinformation-and-misinformation.html

[33] https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/?utm_source=chatgpt.com