



# LUMORA FOUNDATION

Estonia

## Lumora Strategic Reflections

Issue No. 01 | July 2026

# The 2026 NATO Summit Strategic Reflections from an Estonia-Based Foundation

Education, Digital Resilience and International  
Cooperation in an Evolving Security Environment



## Suggested Citation

*Ince, F. (2026). The 2026 NATO Summit: From Collective Defense to Collective Resilience — Transforming the Euro-Atlantic Security Architecture. Lumora Policy Paper Series, Issue: 01. Lumora Foundation: Tallinn.*

## Abstract

The NATO Summit held in Ankara on July 7–8, 2026, marks a profound transformation in the Euro-Atlantic security order, signaling a comprehensive shift from traditional collective defense to a multi-domain, whole-of-society collective resilience model. Meeting under the shadow of a prolonged conventional conflict on the eastern flank and escalating gray-zone threats, Allied leaders reaffirmed their commitment to collective defense under Article 5 of the Washington Treaty and the defense investment pledge adopted at the 2025 Hague Summit — which mandates that Allies allocate at least 5% of their GDP to defense and security-related investments by 2035. Concurrently, the Summit formalized a strategic framework under Article 3 of the North Atlantic Treaty to operationalize national resilience, thereby integrating military readiness with societal robustness.

This policy paper systematically analyzes the core strategic pillars codified in the Ankara Summit Declaration. It evaluates the policy choices, trade-offs, and complementarities among conventional military mass, accelerated technological innovation, and whole-of-society resilience within a comparative framework. Drawing on Estonia's digital governance model as an institutional benchmark, this study highlights the critical role of non-governmental institutions, educational diplomacy, and cross-sectoral knowledge networks in securing critical infrastructure, ensuring the responsible governance of dual-use emerging technologies, and mitigating foreign information manipulation and interference (FIMI). The paper concludes with targeted, actionable recommendations for a broad spectrum of stakeholders, ranging from national governments and NATO to the European Union, universities, civil society organizations, and independent foundations.

## About Lumora

The Lumora Foundation is an Estonia-based, independent, non-profit policy research institute. It conducts evidence-based research in educational diplomacy, digital governance, democratic resilience, and international cooperation. The Lumora Policy Paper Series aims to provide independent policy analysis for policymakers, academia, and civil society.

## Keywords

NATO, Resilience, Hybrid Threats, Estonia, Collective Defense, Artificial Intelligence, Defense Investments, Euro-Atlantic Security.

## Methodology

This study was prepared using qualitative content analysis of official strategy documents, summit declarations, and open-source policy papers published by the North Atlantic Treaty Organization (NATO), European Union institutions, the Government of Estonia, and the Organisation for Economic Co-operation and Development (OECD). Within the scope of this analysis, the institutional, financial, and societal implications of the Ankara Summit decisions were evaluated within a comparative framework, and the official statements and budgetary commitments of strategic actors were filtered empirically to derive actionable policy recommendations.

## Acronyms

- **AI:** Artificial Intelligence
- **DIANA:** Defence Innovation Accelerator for the North Atlantic
- **EDIS:** European Defence Industrial Strategy
- **EDTs:** Emerging and Disruptive Technologies
- **EEAS:** European External Action Service
- **EU:** European Union
- **FIMI:** Foreign Information Manipulation and Interference
- **GDP:** Gross Domestic Product
- **NATO:** North Atlantic Treaty Organization
- **NDPP:** NATO Defence Planning Process

## 1. Executive Summary and Introduction

---

The 2026 NATO Summit in Ankara represents a critical turning point in the institutional history of the Euro-Atlantic Alliance. Convening at a time of deepening geopolitical tensions, accelerated technological transformation, and intensifying hybrid warfare tactics, the Summit established a strategic roadmap intended to guide the Alliance through the end of the decade. While the commitment to collective defense under Article 5 of the Washington Treaty remains unwavering, the most defining outcome of the Ankara Summit is the formal recognition that military power alone can no longer guarantee comprehensive security. Long-term deterrence increasingly rests on the multi-domain resilience of societies, supply chains, critical infrastructure, and democratic institutions — an understanding that aligns with the expanded defense investment targets adopted at the 2025 Hague Summit.

This policy report provides a systematic analysis of the strategic decisions adopted at the Ankara Summit. Moving beyond traditional security frameworks, it examines the expanding security architecture from a multidimensional perspective, emphasizing the interconnectedness of defense capability, technological innovation, and societal resilience. Drawing on official declarations, primary sources, and institutional frameworks, this study explores the implications of the Summit mandates for various international stakeholders, including national governments, European institutions, academia, and civil society. The report specifically highlights the institutional perspective of Lumora — an Estonia-based independent, non-profit policy research institute — demonstrating that non-governmental actors, educational diplomacy, and trans-border knowledge networks constitute a vital strategic infrastructure underpinning modern collective security. In this context, the study aims to go beyond a merely descriptive summit summary to critically examine the feasibility, institutional costs, and medium-term outcomes of the decisions taken in Ankara.

## 2. The Strategic Context of the 2026 NATO Summit

---

The path leading to the 2026 Ankara Summit was shaped by a complex matrix of reinforcing and overlapping security challenges. The prolonged conflict resulting from Russia's ongoing war against Ukraine continued to dictate the baseline requirements for conventional military readiness along NATO's eastern flank. Simultaneously, the strategic environment was further complicated by non-linear threat vectors, including sophisticated cyber operations targeting public administration, state-sponsored foreign information manipulation and interference (FIMI), and physical sabotage attempts directed at maritime and energy infrastructure in the Baltic and Mediterranean Seas. Indeed, recent drone airspace violations in the Baltic region that required NATO interventions underscored that the boundary between hybrid and conventional threats has become increasingly blurred.

This intricate threat matrix forced the Alliance to confront the limitations of traditional deterrence models. While the deployment of forward-presence battlegroups and the modernization of air and missile defense systems provided visible and practical assurances of hard power, the primary vulnerabilities exploited by modern adversaries remain predominantly non-military. Societal

polarization, systemic supply-chain dependencies on authoritarian states, and gaps in digital literacy have created fertile ground for hybrid operations designed to destabilize democratic processes without triggering conventional military thresholds. Consequently, contemporary deterrence theory is evolving toward a multi-layered logic that relies not solely on military capacity, but on societal robustness, institutional legitimacy, and information integrity.

Furthermore, the rapid commercialization and deployment of emerging and disruptive technologies (EDTs) — particularly artificial intelligence, quantum computing, and autonomous systems — has introduced a dual-use dilemma. While these technologies offer unprecedented operational advantages to early adopters, they have lowered the barrier to entry for asymmetric attacks by malicious state and non-state actors. It was against this backdrop of institutional adaptation and strategic urgency that Allied heads of state and government gathered in Ankara to redefine the parameters of collective security for the mid-twenty-first century. The choice of Türkiye as the host nation carries symbolic weight, signaling a shift in the Euro-Atlantic Alliance's geographical and strategic center of gravity toward its eastern and southeastern flanks.

### **3. Core Strategic Pillars Endorsed in Ankara**

---

The decisions codified in the Ankara Summit Declaration rest on three mutually reinforcing strategic pillars, each designed to address a distinct dimension of contemporary Euro-Atlantic security.

#### **3.1 Hard Defense and Force Readiness**

The Alliance reaffirmed its foundational commitment to credible conventional and nuclear deterrence. Building upon the legacy of previous summits, leaders approved a significant expansion of the NATO Force Model, increasing the number of high-readiness forces available across all domains. Special emphasis was placed on formally upgrading the Baltic Air Policing mission into a comprehensive, integrated air and missile defense role. This mandate grants participating nations broader authority and streamlined decision-making protocols to counter airborne threats, establishing a more permanent defensive architecture across Northeastern Europe.

Regarding defense investments, the Ankara Summit served to consolidate and operationalize the framework established at the 2025 Hague Summit rather than declaring a new target. Under this framework, Allies committed to spending at least 5% of their GDP on defense and security-related expenditures by 2035. This allocation earmarks 3.5% for core military expenditures according to NATO definitions, while the remaining 1.5% is dedicated to broader security investments, including the protection of critical infrastructure, cyber defense, civil preparedness, and the strengthening of the defense industrial base.

This target fundamentally shifts the scale of defense spending, moving far beyond the 2% minimum threshold referenced in previous decades. In Ankara, Allies reconfirmed their commitment to this expanded target, highlighting the urgent need to address critical capability gaps, enhance strategic mobility, and replenish depleted ammunition stockpiles through

standardized joint procurement initiatives. This expanded investment logic was tangibly demonstrated during the Summit's Defense Industrial Forum, where Allies pledged over \$50 billion in new procurement commitments,<sup>1</sup> alongside a €70 billion package for 2026 to sustain military assistance, training, and equipment support for Ukraine.

*<sup>1</sup> Institutional Note: The \$50 billion industrial procurement pledge was verified based on official forum outputs released during the Ankara Summit and subsequent Reuters reporting on defense industrial integration budgeting.*

### **3.2 Technological Transformation and Innovation Ecosystems**

Acknowledging that future operational dominance will be largely determined by technological superiority, the Summit launched the Allied Digital Sovereignty Initiative. This framework accelerates the integration of secure artificial intelligence, autonomous systems, and advanced cyber defense mechanisms into NATO's command and control architectures.

A central component of this pillar is the structural expansion of the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund. The Ankara mandates explicitly direct these bodies to foster robust public-private ecosystems by leveraging commercial tech sectors, software engineering hubs, and university laboratories. This approach aims to secure critical supply chains, de-risk deep-tech research, and insulate strategic industries from adversarial foreign investments. DIANA's network of accelerator sites and test centers across the Alliance serves not merely as a technical support mechanism, but as an institutional bridge building a shared culture of innovation among Allied nations.

### **3.3 Multi-Domain and Whole-of-Society Resilience**

The third and most transformative pillar concerns the operationalization of Article 3 of the North Atlantic Treaty, which requires member states to maintain and develop their individual and collective capacity to resist armed attack. Building upon NATO's Baseline Requirements for National Resilience — first established at the 2016 Warsaw Summit and updated in subsequent strategic concepts — the Ankara Summit formally adopted the Comprehensive Resilience Framework, elevating national preparedness from a narrow civil-military support function to a "whole-of-society" imperative.

This pillar establishes stringent parameters for the protection of critical infrastructure, particularly undersea data cables, energy grids, and digital communication networks. It explicitly bridges the gap between public administration, the private sector, and civil society, mandating the institutionalization of national resilience strategies designed to counter hybrid threats, mitigate foreign deactivation and disinformation, and ensure institutional continuity during prolonged gray-zone crises. The defining characteristic of this third pillar is that its success will be measured not by traditional military metrics, but by variables that are harder to quantify, such as institutional trust, societal cohesion, and post-crisis recovery speed.

## **4. Policy Options and Trade-Offs: Evaluating Strategic Paths**

---

Translating the political commitments of the Ankara Summit into long-term security outcomes requires choices regarding priorities, resources, and implementation. Because no single policy approach can simultaneously maximize military readiness, technological innovation, economic sustainability, and societal resilience, decision-makers face a series of strategic trade-offs. The three options discussed below represent analytical scenarios highlighting different resource allocations rather than mutually exclusive alternatives.

### **Option A: Prioritizing Conventional Military Readiness**

This approach focuses on reinforcing NATO's traditional military capabilities through increased defense spending, expanded force readiness, equipment modernization, and enhanced industrial manufacturing output. It reflects the immediate lessons learned from high-intensity conventional warfare and emphasizes visible, credible military mass.

- **Potential Advantages:** Strengthens collective deterrence against conventional military aggression; improves physical readiness along the eastern flank; expands the defense industrial manufacturing base; enhances tactical interoperability among Allied forces; and demonstrates Alliance cohesion to external adversaries.
- **Potential Trade-Offs:** Requires sustained, high-level financial commitments (compounded by the expanded 5% GDP target); risks diverting state resources away from digital innovation and societal resilience; procurement cycles remain structurally slow; and it may induce domestic fiscal strain in certain member states.

### **Option B: Accelerating Technological Innovation**

This path prioritizes emerging technologies, including artificial intelligence, cyber capabilities, autonomous systems, secure digital infrastructure, and advanced defense innovation ecosystems. It assumes that future conflicts will be decided by technological superiority rather than numerical military mass alone.

- **Potential Advantages:** Fosters rapid adaptation to new threat vectors; improves situational awareness and decision-making speed through digital technologies; strengthens cyber security and intelligence-sharing capabilities; generates dual-use economic spillovers; and creates collaboration opportunities between governments, private venture capital, and academia.
- **Potential Trade-Offs:** Rapid technological advancement can outpace existing regulatory and legal frameworks; AI deployment introduces complex ethical governance challenges; over-reliance on advanced technologies increases vulnerability to cyber sabotage; and high R&D costs could widen capability gaps among Allies.

### **Option C: Investing in Whole-of-Society Resilience**

Rather than focusing strictly on military hardware, this model emphasizes resilience across the civilian fabric of society. It recognizes that governments, universities, non-governmental organizations, private industry, and local communities contribute directly to national security.

This concept aligns closely with the institutional priorities demonstrated in Estonia's advanced digital governance and institutional resilience model.

- **Potential Advantages:** Safeguards democratic institutions and electoral systems against hybrid threats; improves systemic protection and recovery times for critical infrastructure; expands public media resilience against disinformation; enhances governance continuity across public institutions; and fosters cross-sectoral trust between the state and the population.
- **Potential Trade-Offs:** Strategic outcomes are organic and visible only over the medium-to-long term; horizontal coordination among numerous decentralized public and private entities is highly complex; success depends on sustained political commitment independent of electoral cycles; and measuring resilience is inherently more difficult than measuring conventional military capabilities.

### Comparative Assessment Matrix

| Strategic Option                      | Core Objective                  | Primary Strength                                                | Primary Challenge                                              |
|---------------------------------------|---------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|
| Option A: Conventional Defense        | Robust military deterrence      | High tactical readiness and visible military mass               | High fiscal cost and diversion of resources from other sectors |
| Option B: Tech Innovation             | Future operational advantage    | Superiority in cyber, space, and smart cognitive systems        | Ethical, regulatory, and supply chain vulnerabilities          |
| Option C: Whole-of-Society Resilience | Long-term democratic robustness | Strong systemic protection against hybrid and gray-zone threats | Complex implementation architecture and slower visible metrics |

### The Integration Imperative

Rather than selecting a single strategic path, the long-term effectiveness of NATO's security agenda depends on balancing all three approaches. Military readiness remains indispensable; technological innovation provides a strategic edge; and societal resilience ensures that democratic institutions can continue to function under sustained pressure.

These three dimensions are not competing priorities but mutually reinforcing components. Education drives technological innovation; innovation strengthens institutional resilience; and resilient institutions anchor collective security. The fundamental challenge facing the Alliance is no longer deciding whether military capability, technology, or societal resilience is more important, but determining how to integrate these three pillars into a coherent, measurable, and sustainable security model. Indeed, the Ankara Summit's explicit allocation of the 1.5% portion of the expanded GDP target toward civil preparedness and resilience demonstrates that these three pillars are now structurally intertwined at the budgetary level.

## **5. Lumora Strategic Assessment: From Collective Defense to Collective Resilience**

---

The 2026 NATO Summit demonstrates a significant evolution in contemporary security thinking. While collective defense remains the core responsibility of the Alliance, the commitments adopted in Ankara reveal that long-term security is increasingly dependent on multi-domain resilience. This shift represents an expansion of the concept of security itself. Military capability is necessary, but alone it cannot adequately address cyber threats, foreign information manipulation, attacks on critical infrastructure, or technological disruption. Resilience has therefore evolved from a supporting concept into a core strategic capability.

### **5.1 Security Beyond Military Capability**

The Summit demonstrated that security is no longer the exclusive domain of defense establishments. Modern resilience depends on the interaction between public authorities, educational institutions, research organizations, civil society, industry, and international partners. While these actors perform different functions, they collectively contribute to democratic stability. Security policy must therefore be understood as a holistic ecosystem rather than an isolated government function. Lumora's institutional experience indicates that the functionality of this ecosystem depends directly on inter-institutional trust and the transparency of information flows; resilience cannot be built as a capacity monopolized by a single institution.

### **5.2 Education as Strategic Infrastructure**

Resilient societies are built not only through investments in military capabilities, but also through education, research, critical thinking, and institutional learning. Educational institutions develop future expertise, universities drive innovation, research centers support evidence-based policymaking, and civil society organizations strengthen democratic engagement. Together, these institutions generate the human capital necessary for long-term resilience. Consequently, education should be viewed not merely as a social policy goal, but as a strategic investment in democratic security. Educational diplomacy, in this context, encompasses more than academic exchange; it serves as a broad framework for building a shared strategic culture and mutual trust among Allied and partner nations.

### **5.3 Estonia as an Institutional Reference**

Estonia provides an important institutional context for understanding resilience. Internationally recognized for its digital governance, cyber security culture, and public sector innovation, Estonia demonstrates how smaller states can enhance national resilience through institutional quality rather than geographical scale. The priorities emphasized during the Ankara Summit — including resilience, technological adaptation, trusted governance, and international cooperation — align closely with the environment in which Lumora operates. As an Estonia-based independent policy research institute, Lumora views these experiences as valuable reference points for future policy dialogue and capacity-building initiatives.

In the lead-up to and during the Ankara Summit, Prime Minister Kristen Michal characterized the Summit as a reaffirmation of Allied unity, stressing that European security requires greater European responsibility. He reaffirmed Estonia's commitment to the expanded defense spending targets established at the Hague Summit, highlighting sustainable investment in defense industrial capacity, welcoming NATO's updated air and missile defense plans, and emphasizing the importance of continued military support for Ukraine. According to the Prime Minister, Estonia will invest approximately \$30 billion (around €26 billion) in defense over the next decade, with nearly half dedicated to armaments and military capabilities. This figure is consistent with Estonia's national decision to push defense spending beyond 5% of its GDP by 2026, demonstrating that the Baltic states are pursuing an implementation timeline that actively exceeds the expanded NATO targets.

## **5.4 Artificial Intelligence and Democratic Governance**

Artificial intelligence is increasingly becoming a strategic element in both national security and democratic governance. Its applications extend beyond defense into education, public administration, and critical infrastructure. At the same time, rapid technological development introduces significant questions regarding transparency, accountability, and ethical governance. Future resilience will depend on ensuring that emerging technologies are managed responsibly through structured collaboration among governments, universities, the private sector, and civil society. AI governance must therefore be treated not merely as a technical regulatory matter, but as a security issue vital to preserving democratic legitimacy.

## **5.5 International Cooperation and Future Outlook**

No single country can address the full spectrum of contemporary security challenges alone. The Ankara Summit reaffirmed the importance of cooperation among Allies. However, long-term resilience also depends on collaboration beyond traditional defense structures. International organizations, academia, civil society, and independent foundations facilitate the dialogue and knowledge exchange that complement government action. The future of resilience will increasingly depend on the ability of democratic societies to integrate defense, technology, education, governance, and international cooperation into a coherent strategic framework.

## **5.6 Lumora's Future Contribution to the Strategic Ecosystem**

As an Estonia-based independent policy research foundation, Lumora aims to contribute to the field implementation of international security policies by bridging policy research with educational diplomacy and societal capacity-building. Looking ahead, Lumora recognizes that long-term collective resilience cannot rely solely on state apparatuses. Consequently, the foundation will channel its operational and research activities into structured policy research and educational diplomacy. The foundation is actively designing capacity-building programs aimed at enhancing cross-sectoral collaboration in digital governance, cyber literacy, and democratic resilience.

The primary strategic vehicle for this contribution will be the development of high-impact projects within the frameworks of Erasmus+, EU funding streams, and NATO-led innovation networks. By leveraging these international funding and cooperation mechanisms, Lumora aims to build scalable models for youth empowerment, civil-tech integration, and public-private knowledge exchange. Furthermore, as AI and emerging technologies redefine global governance, the foundation will advocate for evidence-based policy frameworks to ensure that digital transformation remains aligned with ethical standards and democratic accountability. Through international academic partnerships, joint research initiatives with leading European universities, and localized community workshops, Lumora's future roadmap is dedicated to translating high-level Ankara directives into actionable, grassroots educational tools, preparing the next generation of civil society leaders for the complex security landscape of the late twenty-first century.

## 6. Recommendations

The strategic direction established at the 2026 NATO Summit requires sustained implementation across multiple sectors. The following sector-specific recommendations are designed to support practical application.

### *For National Governments*

- **Strengthen National Cyber Resilience Strategies:** Elevate cyber defense to a core pillar of national security, mandating baseline security standards for both public institutions and private operators of essential services.
- **Protect Critical Infrastructure:** Conduct comprehensive vulnerability audits of undersea communication cables, energy grids, and satellite networks, incorporating redundant architectures to ensure rapid recovery post-sabotage.
- **Expand Defense Industrial Capacity:** Establish long-term procurement contracts to provide market predictability for defense manufacturers, prioritizing the expansion of domestic production lines and standardized ammunition stockpiles.
- **Support Digital Transformation in Public Administration:** Transition legacy governance systems to secure, decentralized, cloud-backed architectures that guarantee institutional continuity during crises.
- **Integrate Inter-Ministerial Resilience Planning:** Break down institutional silos by establishing inter-ministerial resilience task forces that unify economic, educational, digital, and military planning.
- **Establish Compliance Timelines for the Expanded Defense Investment Target:** Publish transparent, auditable annual implementation roadmaps tracking the core military (3.5%) and broader security (1.5%) components required to meet the 5% GDP target.

### *For NATO*

- **Enhance Cyber Operational Cooperation:** Institutionalize rapid cyber response teams and expand real-time threat intelligence sharing between high commands and member states.

- **Improve Critical Infrastructure Surveillance:** Deploy advanced maritime surveillance, unmanned underwater vehicles (UUVs), and satellite tracking assets to monitor and deter threats to critical Allied energy and data pathways.
- **Scale Technological Innovation Initiatives:** Increase funding allocations for DIANA and the NATO Innovation Fund, focusing explicitly on accelerating the transition of mature dual-use commercial technologies into military application.
- **Drive Defense Industrial Standardization:** Enforce strict standardization and interoperability principles for new equipment across all Allies, reducing fragmentation within the Euro-Atlantic defense market.
- **Advance Resilience Planning Across Allied Nations:** Incorporate quantitative resilience metrics into the formal NATO Defence Planning Process (NDPP), holding member states accountable for societal preparedness targets.

#### *For the European Union*

- **Foster Defense Industrial Cooperation:** Operationalize the European Defence Industrial Strategy (EDIS), utilizing EU financial mechanisms to incentivize joint cross-border European procurement initiatives.
- **Secure Digital Sovereignty:** Invest in domestic semiconductor manufacturing, cloud infrastructure, and software development through regulatory frameworks and incentives, reducing technological dependencies on extra-regional authoritarian supply chains.
- **Expand Research and Innovation:** Allocate dedicated Horizon Europe funding streams toward deep tech, quantum computing, secure communications, and dual-use AI applications.
- **Ensure Energy Security and Transport Resilience:** Direct next-generation investments to accelerate the integration of European energy grids, diversify gas and electricity imports, and modernize transport corridors to facilitate rapid tactical military mobility.
- **Broaden Institutional Capacity Against Disinformation:** Establish a shared early-warning mechanism that enables rapid information exchange among member states, building upon the patterns identified in the EEAS's FIMI threat reports.

#### *For Universities*

- **Advance Cyber Security and AI Research:** Establish dedicated, interdisciplinary research centers focused on the geopolitical, technical, and ethical dimensions of artificial intelligence and advanced cryptographic systems.
- **Expand Interdisciplinary Security Curricula:** Develop modern degree programs that combine traditional military strategy with coursework in cyber warfare, digital governance, the economics of threats, and hybrid threat analysis.

- **Foster International Academic Partnerships:** Facilitate cross-border faculty and student exchanges within the Euro-Atlantic area to align research agendas and build shared expertise on security challenges.
- **Promote Digital Literacy and Information Hygiene:** Mandate foundational competencies in data security and critical media consumption across academic disciplines to build cognitive resilience against disinformation.

#### *For Civil Society and Youth Organizations*

- **Promote Media Literacy and Counter-Disinformation Resilience:** Launch community-level training initiatives to equip citizens with the analytical tools necessary to detect, verify, and refute foreign information manipulation and interference (FIMI).
- **Enhance Civic Education and Digital Inclusion:** Implement public programs that reinforce trust in democratic processes, reduce societal polarization, and ensure that vulnerable populations possess the tools to securely access digital public services.
- **Advance Grassroots Digital Literacy and Leadership Pipelines:** Leverage youth-led advocacy networks to lead peer-to-peer workshops on cyber security awareness and build leadership pipelines to prepare the next generation for complex governance challenges.

#### *For Independent Foundations*

- **Bridge Institutions and Facilitate Partnerships:** Act as a neutral convener, bringing together representatives from governments, technology firms, academia, and civil society for cross-sectoral security dialogues.
- **Support Evidence-Based Policy Research:** Fund independent, high-quality, and non-partisan strategic assessments that analyze long-term security trends free from immediate political pressures.
- **Advance Educational Diplomacy:** Utilize educational initiatives as tools of international cooperation, fostering deep institutional trust and shared strategic cultures among allied and partner nations.

## 7. Conclusion

---

While the 2026 NATO Summit reaffirmed the Alliance's enduring commitment to collective defense, it also underscored the rising importance of resilience, innovation, and institutional preparedness. The Summit demonstrated that contemporary security extends far beyond conventional military capabilities. Cyber security, critical infrastructure, artificial intelligence, defense industrial manufacturing, democratic robustness, and international cooperation are structural elements shaping the strategic environment in which Allied nations operate. The formalization of the 5% GDP target serves as a clear indication that this expanding security agenda is being codified not merely rhetorically, but at the budgetary level.

For Estonia, the Summit reinforced national priorities regarding regional security, technological innovation, and societal resilience. For Europe, it highlighted the necessity of stronger cooperation among governments, international organizations, academia, and civil society. Building resilient societies requires sustained investment not only in military assets, but also in education, innovation, responsible governance, and trusted institutions. This is the core thesis advanced by Lumora in this document: collective defense and collective resilience are not alternatives, but prerequisites for one another.

### **Lumora Policy Paper Series**

This publication marks the inaugural issue (Issue No. 01) of the regularly published Lumora Policy Paper Series by the Lumora Foundation. Dedicated to exploring the intersections of international politics, educational diplomacy, digital transformation, youth engagement, and democratic resilience, this series serves as a strategic platform for evidence-based research. Our mission is to provide rigorous, independent, and actionable analysis to guide policymakers, academic institutions, and civil society leaders through contemporary global challenges.

### **Corporate Manifesto: The Lumora Perspective**

The Lumora Foundation believes that resilient societies are built through knowledge, cross-border cooperation, and responsible leadership. In the contemporary world, security can no longer be measured solely by the limits of military capabilities. Security is reinforced by trusted institutional frameworks, sustained by democratic values, enabled by quality education, accelerated by technological innovation, and safeguarded by international partnerships.

As an Estonia-based independent policy research institute, our strategic approach integrates theoretical policy research with grassroots societal applications. By establishing cross-sectoral and trans-border knowledge networks, we generate proactive analytical solutions that enhance societal robustness against multi-layered global crises.

We maintain that the future of international cooperation depends not merely on reflexive responses during moments of crisis, but on strengthening — with a long-term vision — the institutional infrastructures capable of anticipating crises before they emerge and protecting the civilian fabric.



## About the Author

### **Fatma İnce**

*Founder and President, Lumora Foundation*

*International Education, Law, and Diplomacy Strategist*

*Tallinn, Estonia*

Fatma İnce is the Founder and President of the Lumora Foundation, an Estonia-based independent policy research institute working in international education, strategic research, digital transformation, and international cooperation. Through the Lumora Foundation, she conducts evidence-based research on educational diplomacy, democratic resilience, and international politics in Europe. Her work focuses on institutional resilience, international partnerships, digital governance, and public policy. She possesses extensive experience in developing international cooperation initiatives involving universities, civil society organizations, and public institutions across Europe.

## Acknowledgments

The author expresses gratitude to the official institutions, including NATO, the Government of Estonia, and the European Union, whose publicly available documents informed this publication. Appreciation is also extended to Lumora's international partners, academic colleagues, and collaborators, whose continuous contributions to education, international cooperation, and policy dialogue support the development of resilient and inclusive societies. Any remaining errors or interpretations belong solely to the author.

*△ Legal Disclaimer: This publication is prepared exclusively for research and educational purposes and does not represent the official views of any institution mentioned herein.*

## References

---

European Commission. (2024, March 5). European Defence Industrial Strategy: Ensuring EU readiness through a responsive and resilient European defence industry.

European External Action Service. (2025, March 19). 3rd EEAS report on foreign information manipulation and interference threats.

Government of Estonia. (2026, July 8). Prime Minister Kristen Michal: NATO decisions adopted in Ankara strengthen Estonia's security.

NATO. (2016, July 8). Commitment to enhance resilience.

NATO. (2025, June 25). The Hague Summit Declaration.

NATO. (2026, July 8). The Ankara Summit Declaration.

OECD. (2025, June 19). Government at a Glance 2025: Addressing trust and democratic resilience.

Reuters. (2026, July 8). NATO upgrades Baltic Air Policing mission to broader air defense role.

## Appendix: Source Verification Note

Prior to the second printing of this document, all external citations were independently re-verified, resulting in the following corrections: (i) the defense investment target reaffirmed at the Ankara Summit, which was inadvertently listed as 2% in previous drafts, was aligned with the updated target adopted at the 2025 Hague Summit, which mandates reaching at least 5% of GDP (3.5% core defense + 1.5% broader security) by 2035; (ii) the date of NATO's 2016 "Commitment to Enhance Resilience" document was corrected from July 9 to July 8; (iii) the publication date of the EEAS's 3rd FIMI Threat Report was corrected from January 23, 2025, to March 19, 2025; (iv) the publication date of the OECD's Government at a Glance 2025 report was corrected from November 14, 2025, to June 19, 2025, and its DOI record was updated to its current format. Citations regarding Estonia's ten-year, \$30 billion defense investment pledge and the elevation of the Baltic Air Policing mission to an air defense role were cross-referenced with primary sources and verified.

## Upcoming Publications

- **Issue No. 02:** Estonia's Digital State and Democratic Resilience: Lessons for the Euro-Atlantic Region
- **Issue No. 03:** Artificial Intelligence Governance in Europe: Balancing Innovation, Ethics, and Sovereignty
- **Issue No. 04:** Educational Diplomacy as a Strategic Tool: Strengthening Transatlantic Knowledge Networks