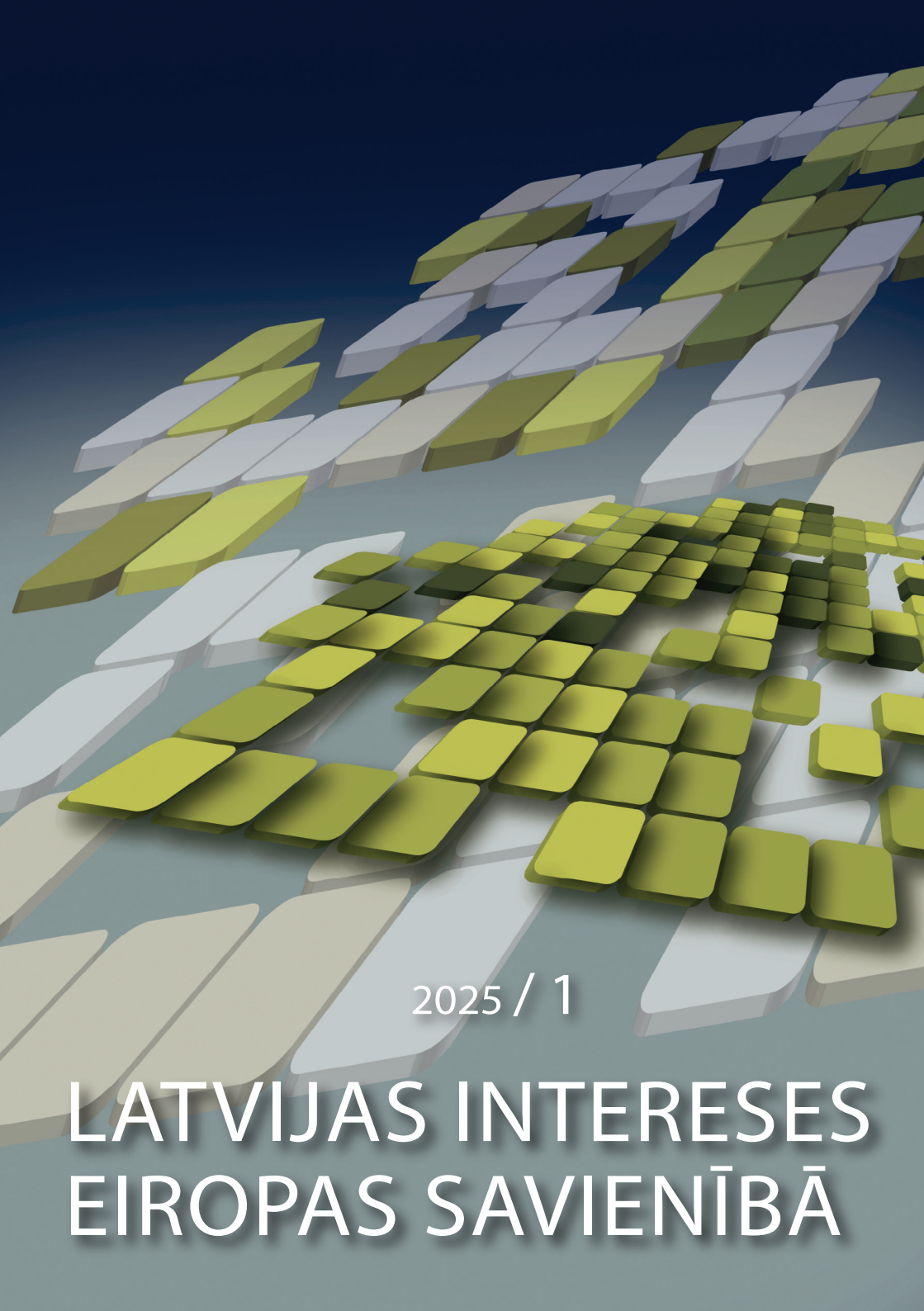

2025 / 1

LATVIJAS INTERESES EIROPAS SAVIENĪBĀ

2025/1

LATVIJAS INTERESES EIROPAS SAVIENĪBĀ

Zinātniskie redaktori **Iveta Reinholde, Žaneta Ozoliņa, Elizabete Klēra Bože**
Projekta vadības grupa **Iveta Reinholde, Žaneta Ozoliņa**
Literārie redaktori **Ingūna Patmalniece, Elizabete Klēra Bože**
Maketētāja **Inese Siliniece**
Māksliniece **Kristīne Plūksna**

Par rakstos atspoguļotajiem faktiem un viedokļiem atbild autori.

Redakcijas kolēģijas adrese:

Latvijas Politologu biedrība
Lomonosova iela 1A, Rīga, LV-1019
Tālrunis: 67140533
e-pasts: info@politologubiedriba.lv
www.politologubiedriba.lv

ISSN 2243-6049

Contents

Editorial

One of the editorial board's long-standing priorities for the journal *"Latvijas intereses Eiropas Savienībā"* has been to include voices from the younger generation of researchers, providing them with a platform to express their views while also supporting their professional development. In cooperation with the Latvian Transatlantic Organisation, we publish the best articles written by participants of the Future Leaders Forum, which reflect the younger generation's perspectives on international affairs and offer solutions and recommendations for policymakers. In the shadow of escalating geopolitical uncertainties, the articles about the future of collective security, the role of leadership, and the resilience of democratic alliances, form a coherent mosaic of contemporary international relations – marked by the resurgence of great power politics, institutional strain, and the need for renewed strategic clarity.

Salma Rhilane's analysis of the "Trump Effect" offers a sobering look at the fragility of the transatlantic alliance. Her assertion that Europe must now move from aspirational strategic autonomy to actionable sovereignty is both timely and necessary. Trump's transactional foreign policy has undermined trust in NATO, exposing Europe's overdependence on U.S. defense guarantees. Yet, as Rhilane outlines, this challenge may also catalyze a long-overdue integration of EU defense capabilities. The EU's policy strides in 2025 – ranging from the ReArm Europe plan to the Preparedness Union Strategy – signal a tectonic shift in mindset. But these measures are not immune to internal divisions. Eastern European states remain skeptical of any EU-led defense framework, clinging tightly to U.S. guarantees in the face of Russian aggression. This east-west divide within the EU is the greatest obstacle to strategic coherence.

David Shakarishvili's contribution masterfully complements this perspective by examining how NATO, in the wake of Ukraine, has evolved from a Cold War relic into a dynamic fusion of deterrence and diplomacy. His depiction of NATO's dual-track strategy – blending forward defense with

strategic dialogue – is particularly insightful. NATO's capacity to deter aggression while engaging diplomatically, even amidst internal divergence, speaks to its institutional resilience. As the author notes, deterrence today involves not only tanks and troops but cyber resilience, information integrity, and societal cohesion.

What emerges across both analyses is the centrality of adaptability. Whether it is the EU recalibrating for autonomy or NATO modernizing its deterrence posture, flexibility in strategy and leadership is paramount. Shakarishvili's call for harmonization – described aptly as a "symphony of strength" – is not merely poetic, but strategic. In a security environment where threats are hybrid and systemic, the synchronization of hard and soft power is essential.

A striking theme that bridges both articles is the role of leadership. Whether it is Emmanuel Macron advocating for a sovereign Europe or NATO generals recalibrating doctrine on the fly, the future of international security hinges on individuals who can balance vision with pragmatism. This insight is expanded in Alberto Messeri's essay on the importance of leadership in international relations. Messeri argues convincingly that 21st-century leaders must possess more than charisma or ideological resolve – they need long-term vision, institutional literacy, and the moral courage to make unpopular decisions for the greater good.

The inclusion of young leaders and intergenerational thinking also deserves attention. Messeri points out that legitimacy today is tied not only to results but to inclusion. Youth, as both inheritors and drivers of global change, must be brought into the institutional fold – not just symbolically, but structurally. In an era when institutions face a trust deficit, this is not only desirable but necessary for democratic resilience.

As a whole, the articles form a powerful narrative: the global order is undergoing a transformation, and both institutions and leaders must evolve in step. Europe's pursuit of autonomy, NATO's strategic balancing, and the emergence of adaptive leadership are not separate threads but parts of the same fabric. They signal a world that is less anchored in past certainties and more shaped by pluralism, agility, and strategic depth.

The collection of articles addressing security issues is effectively complemented by a timely and insightful contribution on a topic that has gained increasing prominence in EU political debates: the role and recognition of

informal caregivers. While social policy is becoming a central pillar of national agendas across EU member states, legal protections in this area remain uneven, and certain vulnerable groups – such as informal caregivers – are often inadequately safeguarded. In his article, Rachid Al Bitar offers a valuable analysis of existing practices across member states, highlighting both gaps in legal frameworks and promising policy developments. His recommendations are not only relevant but also actionable, contributing meaningfully to the ongoing discourse on harmonizing social rights and protections within the EU.

This edition of the journal concludes with two interviews that serve as a call to action: Europe must invest not only in defense spending, but also in political unity and global engagement. Rihards Kols, a Latvian Member of the European Parliament, emphasizes that the EU must be well-prepared to defend itself and respond effectively in times of crisis or potential military conflict. Meanwhile, Stein Verschelden, EU Policy Officer for the Asia-Europe Meeting, highlights the EU's multifaceted role in building bridges and fostering networks with partners in Asia – efforts that ultimately contribute to a more stable and predictable international environment.

Iveta Reinholde,
Žaneta Ozoliņa,
Elizabete Klēra Bože

I

OPINIONS

The Trump Effect: A Catalyst for European Strategic Autonomy or Disintegration?

Salma Rhilane
Analyst, Youth Policy Center

"*If NATO countries don't pay for their own defense, the United States will not defend them.*"

President Donald Trump

The resurgence of Donald Trump's "America First" policy poses critical challenges for European security and transatlantic unity. Trump's potential disengagement from NATO and reduced support for Ukraine compel the European Union (EU) to reconsider its defense strategy urgently. This article evaluates whether Trump's isolationist stance will catalyze Europe's pursuit of strategic autonomy, fostering deeper EU defense integration, or exacerbate internal divisions, jeopardizing collective security. It further explores implications for EU-US relations, NATO's future, and global geopolitical dynamics, providing strategic recommendations to enhance European defense capabilities amidst rising international uncertainty.

Key words: defense integration, Donald Trump, European Union, geopolitical security, NATO, Strategic autonomy, Transatlantic relations.

Donalda Trampa politikas "Amerika vispirms" atdzimšana rada izaicinājumus Eiropas drošībai un transatlantiskajai vienotībai. Trampa iespējamā izstāšanās no NATO un atbalsta samazināšana Ukrainai mudina Eiropas Savienību (ES) steidzami pārskatīt savu aizsardzības stratēģiju. Šajā rakstā

tiek izvērtēts, vai Trampa izolacionistiskā nostāja veicinās Eiropas stratēģiskās autonomijas attīstību un padziļinās ES aizsardzības integrāciju, vai arī saasinās iekšējās domstarpības, apdraudot spēju kolektīvi rīkoties. Rakstā tiek analizētas iespējamās sekas ES un ASV attiecībām, NATO nākotnei un globālajai ģeopolitiskajai situācijai. Autore piedāvā stratēģiskus ieteikumus Eiropas aizsardzības spēju stiprināšanai pieaugošas starptautiskās nedrošības apstākļos.

Atslēgvārdi: aizsardzības integrācija, Donalds Tramps, Eiropas Savienība, ģeopolitiskā drošība, NATO, stratēģiskā autonomija, transatlantiskās attiecības.

Introduction

Donald Trump's renewed ascent to the U.S. presidency, underpinned by a reinvigorated "America First" doctrine, has profoundly unsettled the architecture of transatlantic security and the international system. His administration's skeptical stance toward NATO, combined with threats of economic disengagement and reduced defense commitments, has rekindled existential questions for European policymakers. At the heart of this dilemma lies a pivotal question: Will the EU finally realize its long-debated vision of strategic autonomy, or will internal divisions leave the continent vulnerable to an unpredictable global order?

Historically, NATO has been the linchpin of European security, shielding the continent through collective defense and anchoring the transatlantic alliance. Yet Trump's transactional approach, epitomized by his most recent remarks that NATO allies must "*pay for their own defense*" or risk losing U.S. protection, has triggered widespread anxiety. These statements, paired with economic policies such as revived tariffs on European goods, highlight a multidimensional shift in U.S. foreign policy that extends beyond defense.

This article explores the implications of this shift by analyzing three interconnected dimensions: (1) the EU's readiness to assume greater responsibility for its own security, (2) the consequences for NATO and the global balance of power, and (3) actionable pathways toward resilient and autonomous European defense. Drawing from recent policy developments, expert analyses, and geopolitical trends, the article aims to inform decision-makers navigating a volatile transatlantic landscape.

Strategic context

Since its establishment in 1949, NATO has served as the backbone of European defense and the cornerstone of transatlantic unity. Anchored in Article 5's mutual defense clause, the alliance provided a robust deterrent during the Cold War and helped shape a stable postwar order. The U.S. military umbrella, bolstered by nuclear capabilities and global reach, allowed European nations to underinvest in defense while focusing on economic reconstruction and integration.

Donald Trump's first term challenged this foundational arrangement. He criticized NATO as "obsolete," accused allies of free-riding, and raised the specter of U.S. withdrawal unless burden-sharing targets were met.[1] His return to power in 2025 has revived these concerns. Trump's public declaration – "If NATO countries don't pay for their own defense, the United States will not defend them" – has reinforced European anxieties. This rhetoric, compounded by actions such as exclusion of EU representatives from Ukraine-related negotiations,[2] and the imposition of a 20% tariff on EU goods in early April 2025 (suspended 90 days later), has introduced significant uncertainty into transatlantic relations, signaling a transactional and unpredictable U.S. approach that undermines alliance cohesion.[3]

In response to rising global tensions and the renewed uncertainty in transatlantic relations, the European Union has accelerated its defense agenda through a series of ambitious 2025 initiatives. The European Commission's 2025 Work Programme introduced a White Paper on the Future of European Defence and the first-ever European Defence Industrial Strategy, aimed at consolidating procurement, boosting innovation, and reducing dependency on non-EU suppliers.[4] These measures seek to pave the way

[1] Sperling, J. & Webber, M. (2019). Trump's Foreign Policy and NATO: Deterrence and Reassurance under Uncertainty. International Affairs, 95(2), 301–325.

[2] Messari, N. (2025). Framing U.S.–Russia Relations: A New International Architecture? Policy Brief N°18/25. Policy Center for the New South.

[3] AP News, April 10, 2025 https://www.nytimes.com/2025/04/10/world/europe/european-union-trump-tariffs-pause.html

[4] White & Case (2025). Big Bang: European Commission Unveils Proposals to Support a Surge in Defence Spending and Reduce Reliance on Non-EU Suppliers. April 2025. https://www.whitecase.com/insight-alert/big-bang-european-commission-unveils-proposals-support-surge-defence-spending-reduce

toward a unified European defense market and institutionalize the long-debated strategic autonomy. In March 2025, the Commission also unveiled the "ReArm Europe" plan and the SAFE Facility, a proposed €150 billion loan framework allowing member states to increase defense spending up to 1.5% of GDP between 2025 and 2029, with relaxed EU budgetary constraints. Complementing these measures is the new Preparedness Union Strategy, which introduces stockpiling mandates and rapid response tools to enhance EU resilience against hybrid threats such as cyberattacks and public health emergencies.[5] These efforts are part of a broader paradigm shift: the EU is actively embedding strategic autonomy into its economic, technological, and public health domains. Initiatives such as the Digital Decade targets and industrial repatriation plans aim to reduce Europe's dependency not only on the United States, but increasingly on China, particularly in areas like semiconductors, AI, and critical infrastructure.[6]

Building upon these policy initiatives, EU defense spending has experienced a significant surge. In 2024, total defense expenditure reached an estimated €326 billion, accounting for 1.9% of the EU's GDP, a more than 30% increase since 2021. Notably, 31% of this spending was allocated to defense investments, primarily for new equipment procurement.[7] Despite this overall growth, disparities persist among member states. For instance, Estonia and Latvia have announced commitments to spend 5.0% of GDP, and Poland plans to reach 4.7% in 2025.[8]

Public opinion across the EU reflects strong support for enhanced defense cooperation. According to a 2025 Eurobarometer survey, 79% of EU citizens favor increased EU-level defense collaboration, and 65% support higher defense spending.[9] However, there is less clarity on the preferred

[5] European Commission (2025). ReArm Europe Plan and SAFE Facility – March 2025 Press Briefing.

[6] Eurasia Review (2025). Trump's Second Term: How It's Shaking NATO, the EU, and Ukraine's Future. https://www.eurasiareview.com/21012025-trumps-second-term-how-its-shaking-nato-the-eu-and-ukraines-future-oped/

[7] Council of the European Union. (2025). EU Defence in Numbers. https://www.consilium.europa.eu/en/policies/defence-numbers/

[8] McKinsey & Company. (2025). A Different Lens on Europe's Defense Budgets. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-different-lens-on-europes-defense-budgets

[9] Bruegel. (2025). Stronger Together: Public Preferences for Different European Defence Cooperation Designs. https://www.bruegel.org/first-glance/stronger-together-public-preferences-different-european-defence-cooperation-designs

design of cooperation, whether through joint military forces or looser intergovernmental coordination. France and Germany remain key drivers of integration efforts, while Central and Eastern European countries continue to rely heavily on U.S. guarantees, revealing persistent divisions in strategic culture across the bloc.

Shifting global dynamics further complicate the landscape. China's growing economic footprint in Europe, Russia's ongoing war in Ukraine, and Brexit's disruption of pan-European security cooperation all demand a reassessment of Europe's strategic role. Notably, the absence of a unified EU response to Trump's latest tariff threats reflects deep-seated fragmentation in both economic and security policy.

In this context, the EU's longstanding aspiration for strategic autonomy has evolved from a normative ambition into a strategic necessity. Whether it can be realized – and at what cost – depends on the Union's ability to reconcile internal divisions, respond flexibly to global shifts, and assert a coherent geopolitical posture.

European responses: Strategic autonomy or internal divisions?

The 2nd term of President Donald Trump has reignited longstanding debates within the EU over its capacity to act independently in matters of defense and foreign policy. For key member states – notably France and Germany – Trump's renewed skepticism toward NATO has been interpreted as a geopolitical shock, accelerating calls for a sovereign European defense architecture. President Emmanuel Macron has repeatedly stated that Europe must "*learn to depend on itself for security,*" especially in light of shifting global power dynamics and the risk of being sidelined in U.S.-China rivalry.[10]

France, leveraging its nuclear capabilities and historical emphasis on military independence, has long championed strategic autonomy. Germany, traditionally more cautious, has adopted a more assertive posture since the launch of its Zeitenwende doctrine in 2022, increasing defense spending and prioritizing military modernization.[11] Together, both countries support

[10] Biscop, S. (2020). No Peace from America: Trump, Biden, and Europe's Strategic Autonomy. Egmont Royal Institute for International Relations.

[11] Barigazzi, J. (2023). "Germany's Zeitenwende and Europe's Defense Future." Politico Europe. https://www.politico.eu/article/germany-defense-budget-zeitenwende-eu/

key EU defense initiatives such as the Permanent Structured Cooperation (PESCO) and the Strategic Compass, positioning themselves as leaders in the EU's pursuit of a more coherent security strategy.[12]

However, internal divisions continue to constrain progress. Central and Eastern European countries, including Poland, the Czech Republic, and the Baltic states, maintain a firm preference for NATO and bilateral ties with the United States. These countries view the U.S. presence as a more credible deterrent against Russian aggression, shaped by historical memory and geographic proximity.[13] For them, EU-led defense remains unproven, both politically and operationally. These discrepancies reinforce deeper structural divides regarding strategic autonomy. Some nations may pursue a 'Steep and Strong' rearmament path, while others might adopt 'Pump and Dump' or 'Slow and Low' approaches, reflecting varying levels of commitment and capability.[14]

Public opinion reflects this east-west divergence. A 2025 Eurobarometer survey showed that while 68% of French and 64% of German respondents supported increasing the EU's role in defense, only 42% of Poles and 39% of Estonians shared this view. Citizens in Eastern Europe continue to prioritize NATO's protection and express skepticism toward strategic autonomy initiatives, fearing that such efforts might undermine American support. By contrast, respondents in Southern Europe (e.g., Spain and Italy) supported EU defense integration but cited economic constraints as the main obstacle.[15]

Moreover, the legitimacy of strategic autonomy hinges on public trust and democratic buy-in. A recent study by the European Council on Foreign

[12] European Parliament. Permanent Structured Cooperation (PESCO): Developments and Challenges. December 2021. Available at: https://www.eeas.europa.eu/sites/default/files/pesco_factsheet_2021-12.pdf ; European External Action Service (EEAS). A Strategic Compass for a Stronger EU Security and Defence. March 2022.Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[13] Menon, A. (2022). Europe as a Power: Strategic Autonomy and the New Global Order. Oxford University Press.

[14] Bellais, R., Maślanka, Ł., & Schütz, T. (2025). Three Trajectories for Defence Spending in the EU and Their Consequences for the European Industry and Capabilities. ARES Group Policy Paper No. 111, April 2025. IRIS. Available at: https://www.iris-france.org/wp-content/uploads/2025/04/ARES_2025_04_111_Trajectories_Defence_Spendings_PolicyPaper.pdf

[15] European Commission. (2025). Attitudes of European Citizens Towards Security and Defence. Special Eurobarometer 535. March 2025. Available at: https://europa.eu/eurobarometer/surveys/detail/3492

Relations found that while support for "more Europe" in defense is growing, there is little public consensus on what this should mean in practice, especially when it comes to military interventions or joint procurement.[16] Without broader civic engagement and communication strategies, strategic autonomy risks remaining an elite-driven vision disconnected from public concerns.[17]

Finally, uneven defense capabilities continue to limit operational readiness. As of early 2025, only a minority of EU member states meet the NATO 2% defense spending benchmark. The European Defence Agency reported that defense spending across the bloc reached 1.9% of GDP in 2024, with major disparities between countries.[18] Some states, like Greece and Poland, meet or exceed the target, while others, such as Belgium and Spain, remain well below. In this context, the path toward strategic autonomy remains fragmented. While momentum exists among core EU members, translating ambition into a united and credible defense posture requires addressing political divisions, engaging public sentiment, and investing in shared capabilities.

Implications for NATO and the global order

The European Union's pursuit of strategic autonomy unfolds in a geopolitical environment marked by uncertainty and fragmentation. Its trajectory is tightly interwoven with the future of NATO and the evolving global security architecture. Donald Trump's return to the U.S. presidency has reignited longstanding concerns about the durability of American security guarantees, which serve as the foundation of NATO's deterrence framework. His transactional approach to alliances – reflected in threats to withdraw from NATO or condition U.S. support on financial contributions and economic advantages from Ukraine – has eroded trust and cohesion within the Alliance.[19]

[16] Dennison, S., & Zerka, P. (2024). Europe's Strategic Dissonance. European Council on Foreign Relations. https://ecfr.eu/publication/europes-strategic-dissonance/

[17] Steiner, N., et al. (2023). A Unified Autonomous Europe? Public Opinion of the EU's Foreign and Security Policy in the Wake of the War. Journal of European Public Policy, 30(7), 1045–1064. Available at: https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2217230

[18] European Defence Agency (2024). EU Defence Spending Hits New Records in 2023–2024. https://eda.europa.eu/news-and-events/news/2024/12/04/eu-defence-spending-hits-new-records-in-2023-2024

[19] Sperling, J., & Webber, M. (2019). Trump's Foreign Policy and NATO: Deterrence and Reassurance under Uncertainty. International Affairs, 95(2), 301–325.

These anxieties have been reinforced in 2025 by credible reports of potential U.S. troop reductions in Germany and other NATO member states, triggering renewed debate about the alliance's long-term deterrence posture. Analysts warn that such moves, if enacted, could severely undermine NATO's readiness and signal waning American commitment to Europe's frontline security.[20] However, this rhetorical hardline is somewhat tempered by continued operational engagement. The United States has remained active in joint deterrence efforts, most notably through the DEFENDER 25 exercise, a large-scale deployment involving 25,000 troops across 18 European nations. This demonstrates that while Washington's approach under Trump remains transactional and politically volatile, military cooperation and interoperability with NATO allies have not ceased. Rather, they now coexist with strategic ambiguity, highlighting the dual-track nature of current U.S. policy: deterrence through presence, but reassurance increasingly conditioned on financial burden-sharing.[21] The upcoming NATO Summit, scheduled for June 2025 in The Hague, is expected to be a critical test of alliance cohesion. President Trump's renewed push for NATO members to commit 5% of GDP to defense – an escalation from the previous 2% threshold – has generated significant intra-alliance tension. European leaders fear that setting such an ambitious target risks deepening rifts between high- and low-spending members while reinforcing perceptions of U.S. conditionality.[22]

This transactionalism now extends into the economic domain. Trump's imposition of tariffs on both adversaries and traditional allies has strained transatlantic economic ties and highlighted the volatility of U.S. policy. In 2018, the Trump administration levied 25% tariffs on steel and 10% on aluminum imports from the EU, disproportionately impacting industrial

[20] EconoTimes (2025). How Donald Trump is Reshaping NATO Policies in 2025. April 2025. https://econotimes.com/How-Donald-Trump-is-reshaping-NATO-policies-in-2025-1694434

[21] U.S. European Command (2025). DEFENDER 25 Press Release. https://www.eucom.mil/article/43163/press-release---us-assets-depart-for-defender-25-exercise-alongside-allies-and-partners

[22] Eurasia Review (2025). Trump's Second Term: How It's Shaking NATO, the EU, and Ukraine's Future. https://www.eurasiareview.com/21012025-trumps-second-term-how-its-shaking-nato-the-eu-and-ukraines-future-oped/

exporters in Germany, France, and Italy.[23] These policies resurfaced in 2025, with proposals for a 10% blanket tariff on EU goods and renewed threats to impose 25% tariffs on European cars. Germany, whose automotive exports to the U.S. exceeded €28 billion in 2018, remains particularly exposed.[24] French wine, Spanish olive oil, and Italian cheeses were also targeted in earlier tariff rounds, with European agricultural exporters again bracing for renewed losses.[25] The recent tariff fluctuations further complicate the global economic landscape, potentially shaking the economic foundations that support NATO's collective defense commitments.[26]

Internally, NATO's cohesion is further challenged by diverging strategic priorities among its members. Eastern European countries continue to prioritize conventional deterrence against Russia, while Southern and Western European states are increasingly focused on hybrid threats, terrorism, and instability in the Sahel and Mediterranean regions. Compounding these differences is Trump's foreign policy pivot toward the Indo-Pacific, with China framed as the United States' primary strategic competitor – leaving core European security concerns at risk of marginalization.[27] In parallel, the European Union is beginning to recalibrate its strategic geography. Recognizing that U.S. security priorities may increasingly tilt toward the Indo-Pacific, the EU has launched a more coherent engagement strategy in the region. The 2025 review of the EU Indo-Pacific Strategy underscores the need for diversified partnerships with countries such as Japan, India, South Korea, and Australia. While Europe's capabilities in the region remain limited compared to the United States, this shift reflects an evolving understanding that strategic autonomy must include a global dimension.

[23] Euronews (2024). Why Trump's Tariffs Could Push Europe to Target US Tech Services. https://www.euronews.com/business/2025/02/10/why-trumps-tariffs-could-push-europe-to-target-us-tech-services

[24] Fortune (2024). Germany Faces 'Tariff Man': How Europe's Biggest Economy Could Lose Out Under Trump Plan. https://fortune.com/europe/2024/11/07/germany-crisis-tariffs-trump-2025/

[25] BBC News (2025). US Tariffs: Is Donald Trump Looking for a Trade War with Europe?. https://www.bbc.com/news/business-67758395

[26] Reuters. (2025). EU Leaders Warn of Economic Fallout from Renewed US Tariffs. April 10, 2025. Available at: https://www.reuters.com/world/europe/eu-leaders-react-trump-tariff-fluctuations-2025-04-10/

[27] Messari, N. (2025). Framing U.S.–Russia Relations: A New International Architecture? Policy Center for the New South.

Engagement in the Indo-Pacific is no longer merely economic, it now includes joint naval exercises, maritime security dialogues, and cyber cooperation, aimed at safeguarding supply chains and reinforcing a rules-based international order.[28]

At the global level, the international order is becoming increasingly contested. The relative decline of U.S. leadership, the assertiveness of revisionist powers such as Russia and China, and the emergence of middle powers have led to a more fragmented, multipolar system. Trump's open skepticism of multilateralism and weakening of institutional norms have further accelerated this shift.[29]

In this geopolitical vacuum, authoritarian regimes have expanded their influence. Russia, despite sanctions and military setbacks, continues to disrupt the European security architecture. China, meanwhile, has advanced its global reach through the Belt and Road Initiative and the BRICS+ platform, now joined by several emerging economies.[30] The perceived weakening of NATO – the world's most institutionalized defense alliance – risks emboldening these actors and contributing to systemic instability. The lack of a unified EU approach to defense investment has led to industrial fragmentation. National producers often compete rather than collabrate, undermining Europe's ability to project force and respond effectively during crises.[31]

For Europe, the implications are clear: the Atlantic alliance can no longer be taken for granted. A decline in U.S. reliability would not only reduce deterrence but also limit the EU's capacity to influence global security agendas. As great-power competition intensifies, Europe's ability to act with strategic coherence and autonomy will be essential to safeguarding its interests and values on the world stage.

---

[28] Bena, L. & Druláková, R. (2024). Transatlantic Transitions: STRATEGIES FOR 2025 AND BEYOND. Transatlantic Policy Forum Paper, Europeum Institute for European Policy. https://www.europeum.org/wp-content/uploads/TAPF_2024_ppfinal.pdf

[29] Martill, B., & Sus, M. (Eds.). (2018). Europe and the Trump Presidency: The Transatlantic Relationship in Turbulent Times. Palgrave Macmillan.

[30] Reuters (2025). As BRICS Expands, China and Russia Push Alternative World Order. https://www.reuters.com/world/brics-expansion-china-russia-influence-2025/

[31] Bellais, R., Maślanka, Ł., & Schütz, T. (2025). Three Trajectories for Defence Spending in the EU and Their Consequences for the European Industry and Capabilities. ARES Group Policy Paper No. 111, April 2025. IRIS. Available at: https://www.iris-france.org/wp-content/uploads/2025/04/ARES_2025_04_111_Trajectories_Defence_Spendings_PolicyPaper.pdf

Pathways toward resilient and autonomous European defense: policy recommendations

To navigate the transatlantic uncertainty and reinforce its security posture, the EU must not only set ambitious defense objectives but also confront the practical and political challenges of implementation. The following recommendations aim to deepen strategic autonomy while ensuring their feasibility in a fragmented EU context.

1. Develop an enforceable strategic autonomy roadmap

The EU should formalize a common roadmap with agreed milestones for strategic autonomy in defense, cyber, and supply chain resilience. This must include mechanisms for annual review, peer pressure, and conditional access to EU defense funding (e.g., from the European Defence Fund) based on tangible progress.[32] This scenario indicates that a consistent funding trajectory is essential to transition from fragmented procurement to a resilient and scalable European Defence Technological and Industrial Base (EDTIB). Planning must account for how short-term budget surges ('Pump and Dump') can lead to long-term vulnerabilities.

2. Introduce incentives and penalties for defense spending compliance

To address disparities in national defense contributions, the EU should explore introducing financial incentives (such as co-financing) for states meeting agreed benchmarks, alongside reputational costs or access limitations for those who consistently underperform.[33] This could mirror the fiscal rules model used in the Stability and Growth Pact. As highlighted in recent policy assessments, incentive mechanisms are critical to overcoming the mismatch between national defense spending trends and EU-wide capability goals.

---

[32] European Defence Agency (2024). Annual Report on Defence Data 2023–2024. https://eda.europa.eu/news-and-events/news/2024/12/04/eu-defence-spending

[33] Biscop, S. (2020). No Peace from America: Trump, Biden, and Europe's Strategic Autonomy. Egmont Royal Institute

3. Build internal consensus with a tiered approach

Recognizing that not all member states share the same level of ambition, the EU should operationalize a tiered model of defense cooperation. A core group – led by France, Germany, and Poland – could pioneer integration, while others gradually align based on political will and capabilities.[34]

4. Strengthen EU–NATO institutional ties

To avoid duplication and reduce political friction, the EU should intensify structured dialogues with NATO on crisis planning, threat assessments, and military mobility. A permanent coordination mechanism at the Brussels level would improve complementarity.[35]

5. Engage civil society to build political legitimacy

Strategic autonomy cannot succeed without public understanding and support. The EU should fund national-level citizen assemblies and public consultations to debate defense priorities, address fears of militarization, and increase transparency around spending.[36]

6. Operationalize partnerships beyond the U.S.

Deepen security cooperation with partners like Japan, Canada, and Australia by establishing joint exercises, shared early-warning mechanisms, and technology-sharing agreements. However, attention must be paid to different regional threat perceptions and capacity limitations.[37]

7. Embed economic security in defense strategy

Trump's 2025 tariff threats highlight the importance of economic resilience. Defense policy must be linked to trade diversification, industrial repatriation (e.g., critical technologies), and collective tools for countering economic coercion.[38]

---

[34] Menon, A. (2022). Europe as a Power: Strategic Autonomy and the New Global Order. Oxford University Press.

[35] EEAS (2022). EU–NATO Joint Declaration on Cooperation. https://www.eeas.europa.eu

[36] European Commission (2024). Conference on the Future of Europe – Final Report. https://futureu.europa.eu

[37] ECFR (2023). The Limits of Strategic Partnerships: Europe's Indo-Pacific Challenge. https://ecfr.eu/publication

[38] Fortune (2024). Trump Tariffs Threaten European Industrial Recovery. https://fortune.com/europe/2024/11/07/germany-crisis-tariffs-trump-2025

Conclusions

The Trump effect is in full display, since his return, strategic fault lines in transatlantic relations have resurfaced, forcing the EU to confront a fundamental question: can it rely on the continuity of U.S. security guarantees, or must it finally invest in genuine strategic autonomy? The article has shown that Europe no longer has the luxury of assuming stable American leadership. Trump's unpredictable stance on NATO and coercive economic policies has exposed the vulnerabilities of Europe's overdependence.

This moment presents a challenge and an opportunity. While the divisions between Eastern and Western member states remain sharp, the case for collective action has never been more compelling. Public opinion is split, with enthusiasm for autonomy in some capitals and apprehension in others, highlighting the need for inclusive dialogue and citizen engagement. Without domestic legitimacy, even the best-laid defense strategies risk political fragility.

Moreover, implementation hurdles – from defense spending disparities to institutional inertia – cannot be ignored. The EU must take a pragmatic approach: incentivize contributions, accommodate varying levels of ambition, and maintain coherence with NATO. Simultaneously, the bloc must deepen partnerships beyond the United States and integrate economic resilience as a pillar of its security doctrine.

Strategic autonomy is not a rejection of NATO or the transatlantic alliance. Rather, it is an affirmation of Europe's responsibility to act where others may retreat. It is the cornerstone of a balanced, multipolar, and rules-based order that reflects Europe's interests and values. To seize this moment, Europe must not only dream of sovereignty – it must deliver on it.

A Symphony of Strength: NATO's Harmonization of Diplomacy and Deterrence in the Wake of Ukraine

David Shakarishvili
Lecturer, Klaipėda University

In the aftermath of Russia's invasion of Ukraine in 2022, NATO has had to recalibrate its strategic posture, blending military deterrence with diplomatic engagement to maintain regional stability and defend collective security. This paper explores NATO's evolving response to the crisis, focusing on how the alliance has synchronized its military and diplomatic tools, harmonizing power projection with peace-building efforts. NATO's dual approach reflects a sophisticated understanding of modern conflict, where deterrence and diplomacy are not mutually exclusive but rather complementary elements of the same strategy.

Initially, NATO's military response was swift and resolute, with enhanced deployments along the alliance's eastern borders. The activation of defense plans and the bolstering of forward defense in Eastern Europe underscored NATO's commitment to collective security and deterrence by denial. These moves were intended to prevent any further Russian expansion into NATO territory, sending a clear signal of solidarity among member states.

This article argues that NATO's ability to balance military might with diplomatic finesse in the context of the Ukraine crisis demonstrates the alliance's adaptability in the face of modern geopolitical challenges. The synergy between NATO's deterrence and diplomatic outreach has been instrumental in navigating the complex dynamics of the conflict, ensuring a comprehensive response to the evolving threats posed by Russia.

Key words: conflict,deterrence, diplomacy, NATO, Ukraine.

Pēc Krievijas iebrukuma Ukrainā 2022. gadā NATO bija spiesta pārskatīt savu stratēģisko nostāju, apvienojot militāro atturēšanu ar diplomātisku iesaisti, lai saglabātu reģionālo stabilitāti un kolektīvo drošību. Šajā rakstā

tiek analizēta NATO reakcija uz krīzi, īpaši pievēršoties tam, kā alianse ir sinhronizējusi savus militāros un diplomātiskos instrumentus, līdzsvarojot spēka projicēšanu ar miera veidošanas centieniem. NATO divpusējā pieeja atspoguļo alianses izpratni par mūsdienu konfliktiem, kuros atturēšana un diplomātija nav savstarpēji izslēdzoši, bet gan papildinoši vienas stratēģijas elementi.

Sākotnēji NATO militārā reakcija bija ātra un izlēmīga, palielinot izvietojumu pie alianses austrumu robežas. Aizsardzības plānu aktivizēšana un pastiprināta aizsardzība Austrumeiropā apliecināja NATO apņēmību nodrošināt kolektīvo drošību un atturēšanu, liedzot pretiniekam iespēju gūt panākumus. Šie soļi bija vērsti uz turpmākas Krievijas ekspansijas NATO teritorijā novēršanu, vienlaikus skaidri demonstrējot dalībvalstu solidaritāti.

Rakstā tiek argumentēts, ka NATO spēja līdzsvarot militāro spēku ar diplomātisko prasmi Ukrainas krīzes kontekstā apliecina alianses spēju pielāgoties mūsdienu ģeopolitiskajiem izaicinājumiem. Sinerģija starp NATO atturēšanas pasākumiem un diplomātisko aktivitāti ir bijusi būtiska sarežģītā konflikta pārvaldībā, nodrošinot visaptverošu reakciju uz Krievijas radītajiem draudiem.

Atslēgvārdi: atturēšana, diplomātija, konflikts, NATO, Ukraina

"In the shifting sands of global order, NATO endures not because it commands force, but because it cultivates faith – in principles, in partners, and in the promise that security without values is merely silence before the storm."

Introduction

The Russian Federation's full-scale invasion of Ukraine in February 2022 catalyzed a profound reassessment of Euro-Atlantic security structures. NATO, as the principal framework for collective defense in the transatlantic space, found itself confronting not only a dramatic escalation in conventional warfare on its periphery but also a strategic inflection point demanding rapid and multidimensional adaptation. The crisis has underscored the evolving nature of international conflict – where military threats are no longer isolated from diplomatic, informational, and hybrid pressures – and it has tested the alliance's capacity to respond with both unity and sophistication.

This article examines how NATO has sought to harmonize deterrence and diplomacy in response to the Ukraine crisis. The central aim is to investigate the alliance's strategic balancing act: maintaining credible military deterrence while simultaneously engaging in diplomatic efforts to prevent escalation and sustain regional dialogue. In doing so, the paper positions NATO not merely as a reactive military bloc, but as a complex political institution capable of orchestrating a multi-layered security strategy in real time.

Three core analytical tasks structure the article. First, it explores the theoretical and doctrinal underpinnings of NATO's dual-track approach, tracing the alliance's historical evolution in managing the tension – and potential synergy – between deterrence and diplomacy. This involves situating NATO's current posture within broader debates in security studies, particularly the interplay between hard and soft power in alliance behavior. Second, the article analyzes the specific military measures taken by NATO in the wake of the Ukraine invasion, including forward defense initiatives, force posture enhancements, and the activation of collective defense mechanisms under Article 5. These developments are examined not in isolation, but as part of a larger strategic vision intended to deter further aggression and assure member states. Third, the article investigates NATO's diplomatic engagements both internally – through alliance cohesion and consensus-building – and externally, via partnerships, high-level dialogue, and normative signaling to adversaries and third parties.

In bridging these dimensions, the article argues that NATO's approach reflects an increasingly integrated model of security governance, where deterrence and diplomacy operate not as opposing forces but as complementary instruments of strategic communication. This harmonization is not without challenges; tensions between member states, differing threat perceptions, and the unpredictability of Russian behavior complicate the formulation of a coherent response. Nevertheless, the capacity of NATO to act simultaneously as a military shield and a diplomatic platform marks a significant evolution in its institutional identity and operational logic.

Ultimately, this study contributes to a deeper understanding of NATO's adaptive strategy in the face of renewed geopolitical confrontation. It offers insights not only into the alliance's actions but also into the conceptual recalibration necessary for managing conflict in the twenty-first century, where credibility, cohesion, and coordination are as vital as capability. Through

this lens, the article sheds light on the broader implications of NATO's post-2022 trajectory for the future of collective defense and international order.

To carry out this analysis, the article employs a qualitative content-based approach, drawing on official NATO communiqués, strategic concepts, summit declarations, and statements by key political and military leaders. Deterrence indicators are identified through observable shifts in force posture, military deployments, exercises, defense spending, and institutional readiness measures such as the activation of defense plans or the reinforcement of the NATO Response Force. Conversely, diplomatic indicators are discerned through alliance-level initiatives aimed at dialogue, de-escalation, and international norm-setting – such as the use of NATO's consultative mechanisms, outreach to partners, engagement with international organizations and public diplomacy efforts. The distinction is analytical rather than absolute: many actions have both deterrent and diplomatic dimensions. However, by disaggregating NATO's tools into these categories, the article seeks to reveal how the alliance strategically sequences and synchronizes them in response to evolving security dynamics. This dual coding allows for a clearer examination of NATO's comprehensive strategy, as well as its broader implications for alliance politics and international security architecture.

Dimensional approaches – defense and deterrence

Reinforcing unity through diplomacy

NATO's response to the full-scale Russian invasion of Ukraine in 2022 has been shaped not only by military recalibration but by a sustained effort to reinforce political cohesion through dialogue. This dual-track strategy – combining deterrence with diplomacy – reflects the Alliance's ongoing effort to maintain unity among its diverse members while projecting credibility to both adversaries and partners. In this context, strategic dialogue has served as both a mechanism for internal alliance management and an instrument of external signaling, reinforcing NATO's role as a diplomatic actor within an increasingly adversarial global environment.

The theoretical foundation for NATO's dual approach lies in liberal institutionalist thought, which underscores the role of multilateral institutions in reducing uncertainty, fostering cooperation, and facilitating collective

security (Auerswald & Saidemen, 2014). NATO has long operated as more than a military alliance; it has served as a forum for political consultation and strategic alignment among its members. As Article 4 of the North Atlantic Treaty affirms, member states have the right to convene discussions when their territorial integrity, political independence, or security is threatened. Since the onset of the Ukraine war, Article 4 consultations have increased significantly, illustrating the Alliance's renewed reliance on dialogue as a tool for strategic consensus-building (CAMPBELL & Mazrui, 2013).

Dialogue within NATO serves several interconnected purposes. First, it provides a structured space for aligning national threat perceptions and policy preferences. While the invasion of Ukraine created a shared sense of urgency, member states entered the crisis with differing historical experiences, geographic vulnerabilities, and domestic political contexts (Czosseck, Ottis, & Talihärm, 2011). Dialogue helps mitigate these asymmetries by fostering common understanding and shared purpose. For example, the 2022 Madrid Summit produced a revised Strategic Concept that explicitly named Russia as "the most significant and direct threat" to Allied security – an outcome of intensive internal deliberation. This clarity helped align political messaging and operational planning across the Alliance.

Second, internal dialogue strengthens alliance resilience by managing tensions and avoiding fragmentation. Previous crises – such as the U.S.-led invasion of Iraq in 2003 or debates over burden-sharing – exposed the fragility of NATO's political unity (Iversen, 2012). The Ukraine war, by contrast, has catalyzed an unusually high degree of consensus, in part due to regular consultation and transparent communication among members. Countries with historically divergent views on Russia, including Germany, Hungary, and the Baltic states, have engaged in continuous dialogue to coordinate responses, sanctions, and military support for Ukraine (Goldgeier & Shifrinson, 2023). These conversations have not eliminated disagreement but have helped ensure that internal frictions do not undermine the Alliance's collective posture.

From an external standpoint, NATO's diplomatic engagement reinforces its legitimacy as a global security actor. Strategic dialogue with partners – such as the European Union, Australia, Japan, and Ukraine itself – has expanded in scope and frequency. These engagements serve to harmonize defense and humanitarian efforts, share intelligence, and build interoperable

capabilities. NATO's open-door policy remains a symbolically powerful form of diplomatic signaling. Finland's accession in 2023, and Sweden's pending membership, not only reflect a shift in national security calculations but also demonstrate NATO's continued ability to adapt and integrate new members without compromising internal cohesion (Kott, 2018).

Reinforcing unity through dialogue does not imply the absence of deterrence. On the contrary, diplomacy and deterrence are mutually reinforcing when effectively coordinated. Dialogue reduces misperceptions and enhances predictability, which are essential for maintaining credible deterrence without escalating conflict. In this sense, NATO's dual-track approach mirrors Cold War-era strategies, where dialogue with adversaries – through mechanisms like the NATO-Russia Council or arms control treaties – coexisted with robust military preparedness.

The success of dialogue in reinforcing unity depends on its inclusiveness and strategic clarity. Dialogue must be more than a procedural exercise; it must reflect genuine efforts to bridge national interests, accommodate differing levels of risk tolerance, and project a coherent vision. In an age of complex threats – including cyberattacks, disinformation, and energy insecurity – dialogue must also extend beyond traditional military elites to include policymakers, civil society, and private sector actors involved in critical infrastructure and information ecosystems (Anderson, 2016).

Reinforcing unity through dialogue is essential to NATO's strategic harmony. As the Alliance confronts an increasingly contested security environment, its ability to maintain internal cohesion while engaging diplomatically with external partners will shape its future relevance. Dialogue, when embedded within a broader framework of credible deterrence and strategic foresight, is not a sign of weakness but a necessary component of collective strength in the 21st century.

Modernizing deterrence in practice

A core element of this modernization has been the shift from deterrence-by-punishment to deterrence-by-denial. Rather than relying solely on the promise of overwhelming retaliation, NATO has sought to deny adversaries the ability to achieve their objectives in the first place. This transition is visible in the restructuring of NATO's force posture, particularly along

the eastern flank. The enhanced forward presence in the Baltic states and Poland – once symbolic tripwire deployments – has matured into a scalable and fully integrated deterrence network (Ingram, 2011). The move toward brigade-sized units, coupled with prepositioned equipment and streamlined logistics, ensures that NATO can respond rapidly and credibly to any hostile act.

Equally significant is the integration of advanced technologies into NATO's defense architecture. The modern deterrence toolkit includes not only tanks and aircraft but also real-time intelligence, surveillance, and reconnaissance capabilities, cyber defenses, and artificial intelligence-enabled decision systems. The Defence Innovation Accelerator for the North Atlantic, launched in 2021, plays a critical role in fostering transatlantic cooperation on emerging technologies, ensuring interoperability and closing capability gaps among member states (Auerswald & Saidemen, 2014). Through DIANA and the NATO Innovation Fund, the Alliance is positioning itself to deter not only conventional threats but also those emanating from hybrid, cyber, and space domains (Rynning, 2024).

Cybersecurity has become a central pillar of NATO's deterrence doctrine. Recognizing that future conflicts may begin – or unfold primarily – in cyberspace, NATO has declared cyber as a domain of operations alongside land, sea, air, and space (Daehnhardt, 2011). The Alliance has strengthened its capacity to detect, attribute, and respond to cyberattacks, including through rapid reaction teams and coordinated exercises such as Locked Shields and Cyber Coalition. These initiatives are aimed not merely at protecting digital infrastructure but at reinforcing credibility: signaling to adversaries that cyber aggression against any member state will trigger collective consequences (Ringsmose, 2020).

The war in Ukraine has underscored the importance of resilience as a component of deterrence. NATO has broadened its strategic understanding of what constitutes security, encompassing energy networks, supply chains, civil preparedness, and societal cohesion. Deterrence today is as much about maintaining the continuity of government, protecting information ecosystems, and countering disinformation as it is about deploying troops (Rynning, 2024). This integrated approach was emphasized at the 2023 Vilnius Summit, where member states reaffirmed their commitment to enhance

national resilience under Article 3 of the North Atlantic Treaty, recognizing that a robust home front is indispensable to effective forward defense (Rynning, 2024).

Another innovation in NATO's deterrence posture is the refinement of nuclear signaling. While the Alliance remains committed to arms control and non-proliferation, it has also reiterated the centrality of nuclear deterrence in its strategic concept. The United States' rotational deployment of nuclear-capable aircraft and NATO's continued nuclear sharing arrangements send a calculated message of readiness without escalating tensions unnecessarily (Marrone, 2022). This balance – between deterrence and reassurance – is vital in preventing miscalculation while maintaining strategic stability in the Euro-Atlantic area.

NATO and shifting diplomacy landscape

The conductor's dilemma – strategic unity amid divergent voices

NATO's credibility rests on its capacity to present a unified strategic posture while accommodating the diverse political, military, and historical perspectives of its member states. This tension defines the alliance's internal dynamics, particularly during moments of acute geopolitical stress. The Russian invasion of Ukraine exposed long-standing divergences among NATO members, raising questions about the alliance's ability to harmonize threat perceptions, resource commitments, and foreign policy orientations. The challenge of unity begins with geography (Auerswald & Saidemen, 2014). Frontline states in Eastern Europe interpret Russian actions as existential threats demanding robust deterrence measures, including permanent deployments and accelerated integration of non-member partners. In contrast, some Western and Southern European members tend to prioritize diplomatic resolution, energy stability, or Mediterranean security. These asymmetries reflect not only strategic calculations but also national identities, post-colonial legacies, and differing degrees of historical entanglement with Moscow (Czosseck, Ottis, & Talihärm, 2011). Institutional decision-making within NATO is based on consensus, a model that prioritizes cohesion over speed. This structure often slows policy responses,

particularly during crises that demand swift action. Yet the consensus rule also reinforces legitimacy, as it obliges even dominant powers within the alliance to seek alignment with smaller members (Allison, 2017). The enlargement process illustrates this dynamic. Finland and Sweden's applications, widely supported across the alliance, required extensive negotiation to address Turkish and Hungarian objections. These intra-alliance frictions reveal both the procedural complexity and the underlying political tensions within the alliance. Resource commitments remain a contested issue (Drylie, 2024). The 2% GDP defense spending target, introduced in 2014, continues to divide member states. While some have met or exceeded the threshold, others face domestic resistance or prioritize social spending. The uneven implementation of this target fuels perceptions of burden-shifting, particularly among the United States and Central European allies (Ringsmose, 2020). This debate affects the credibility of collective defense and complicates efforts to standardize force readiness across the alliance. Strategic messaging presents another site of divergence. Public discourse on nuclear policy, arms transfers, and escalation risks varies significantly among members. Differences in communication strategies reflect national political cultures, media landscapes, and electoral dynamics. These variations complicate NATO's deterrence posture, as adversaries may interpret mixed signals as evidence of disunity or hesitation (Kott, 2018). Despite these challenges, the alliance has demonstrated a high degree of political resilience. Coordinated support for Ukraine, adjustments to force posture on the eastern flank, and sustained military exercises reflect an operational convergence, even in the absence of complete political agreement. Much of this coordination occurs through quiet diplomacy, informal networks, and bilateral initiatives nested within the NATO framework (Stephen G. Brooks, 2016). The alliance's capacity to maintain unity amid diversity depends on its ability to manage internal asymmetries through institutional flexibility, shared strategic narratives, and ongoing political consultation. As NATO faces a more contested international order, its effectiveness will continue to rely on reconciling national interests with collective purpose. Strategic unity does not require unanimity of worldview but demands sustained commitment to shared deterrence and the credibility of collective defense (Smith, Kollars, & Schechter, 2024).

The diplomatic score – dialogue, de-escalation, and backchannels

Following Russia's invasion of Ukraine in 2022, NATO recalibrated its diplomatic strategy within a rapidly shifting security environment. Although deterrence and force posture have dominated alliance discourse, diplomacy remains an integral component of NATO's comprehensive approach. Diplomatic engagement does not operate in isolation from military planning but functions as a stabilizing mechanism, reducing misperceptions and preserving lines of communication.

The traditional dual-track strategy – deterrence combined with dialogue – continues to inform NATO's engagement with external actors. This approach was reaffirmed in the 2022 Strategic Concept, which designated Russia as the primary threat while maintaining a framework for political contact. The deterioration of formal dialogue mechanisms, such as the NATO-Russia Council, reflects the deep erosion of trust and the limited effectiveness of institutionalized formats under conditions of high-intensity conflict. As formal diplomacy retreats, informal and discreet channels have become more salient (Sorooshian, 2024).

Backchannels and bilateral contacts, particularly between key NATO members and the Russian Federation, serve as instruments for crisis management. These communications mitigate risks of escalation by maintaining a basic level of strategic transparency (CAMPBELL & Mazrui, 2013). While not publicized, these channels enable a degree of predictability and provide space for negotiation outside rigid institutional parameters. Their role becomes more critical in scenarios where official diplomatic formats are suspended or discredited.

NATO's engagement with partner countries, including Ukraine, Moldova, and Georgia, has acquired greater diplomatic depth (Ingram, 2011). Political consultations, joint coordination platforms, and capacity-building missions constitute an expanding architecture of engagement beyond formal alliance membership. These efforts reinforce political solidarity and support institutional resilience in frontline states, without extending security guarantees. They also contribute to NATO's broader regional influence by strengthening norms of political cooperation and civil-military integration (Dragan, Arfi, Tiberius, Ammari, & Ferasso, 2024).

Within the alliance, internal diplomacy plays a decisive role in policy formation and cohesion maintenance. Member states differ in strategic priorities, military capabilities, and historical legacies. Diplomacy among allies ensures policy alignment on military assistance, threat assessments, and engagement thresholds. The maintenance of consensus requires sustained political negotiation, often shaped by domestic pressures and regional interests. Disagreements on arms deliveries, energy dependencies, or enlargement policies are addressed through continuous diplomatic engagement, reinforcing alliance unity.

NATO's diplomatic activity also intersects with the European Union and other multilateral bodies. Joint initiatives on cybersecurity, disinformation, and sanctions illustrate the expanding interface between NATO and civilian institutions. This cooperative dynamic reflects a shift toward multi-layered security governance, where military alliances and political unions coordinate responses to hybrid threats. Institutional convergence enhances NATO's ability to operate across domains that transcend conventional warfare.

Diplomacy within NATO's strategy remains both functional and symbolic. It enables de-escalation, affirms political commitment, and provides channels for crisis communication. The current security context does not permit the full restoration of formal diplomatic dialogue with adversaries. Nonetheless, the presence of informal channels, internal consensus-building, and external coordination reflects a layered diplomatic practice. NATO's capacity to balance coercive credibility with political engagement will shape its strategic relevance in the years ahead.

The last movement – toward a future-ready NATO

NATO stands at a pivotal juncture defined by systemic transformation, strategic ambiguity, and evolving threats that transcend the traditional boundaries of military engagement. The Russian invasion of Ukraine has reaffirmed the alliance's core purpose while exposing the complexity of its operational environment. As geopolitical rivalries intensify and multipolarity gains traction, NATO must transition from reactive posture to anticipatory strategy, integrating deterrence, diplomacy, and adaptability within a coherent framework. Strategic unity remains essential but must be reimagined

through dynamic coordination mechanisms capable of accommodating internal diversity without diluting collective resolve. Defense modernization, including digital infrastructure, cyber resilience, and space-based capabilities, demands sustained investment and innovation, not as adjuncts but as integral components of deterrence credibility. The emergence of hybrid warfare, information manipulation, and non-state influence campaigns requires a broadened security lexicon that includes cognitive, technological, and societal dimensions. NATO's engagement with partners beyond the Euro-Atlantic area signals a recognition that regional security cannot be disentangled from global interdependencies. Relations with Indo-Pacific democracies, responses to authoritarian assertiveness, and the strategic implications of China's rise necessitate a more outward-looking strategic vision. The institutional relationship between NATO and the European Union also requires further consolidation, built on complementarity rather than redundancy, to address overlapping mandates and coordinate responses to transnational crises. Climate change, demographic shifts, and resource competition will increasingly intersect with security imperatives, challenging NATO to develop multidomain readiness that is both environmentally conscious and socially sustainable. Cohesion must be cultivated through strategic narratives that articulate shared values without erasing national particularities, reinforcing legitimacy through democratic accountability and transparent burden-sharing. The alliance's deterrence posture must remain flexible, capable of scaling responses across the spectrum of conflict while maintaining a threshold that deters aggression without accelerating escalation. Strategic communication must be sharpened to counter disinformation and reinforce public trust, as the credibility of NATO's commitments rests not only on military capability but also on political coherence. Enlargement policy, while symbolically powerful, must be approached with clarity regarding strategic consequences and institutional capacity. NATO's success will hinge less on static doctrines than on its institutional agility, its ability to respond to crises without fragmentation, and its commitment to renewal in both conceptual and material terms. As the alliance moves forward, the balance between continuity and innovation will define its relevance. The symphonic metaphor that frames NATO's evolution captures the need for harmonization across multiple registers – military, diplomatic, economic, and normative.

A future-ready NATO must sound neither discordant nor monolithic, but cohesive, responsive, and attuned to the realities of a rapidly transforming international order. The task ahead is not the preservation of past structures but the orchestration of a strategic future that integrates complexity without sacrificing purpose.

Conclusions

The conflict in Ukraine has served as both a crucible and a catalyst for NATO, forcing the organization to examine, reaffirm, and refine its strategic posture in the face of a renewed threat environment. This paper argues that NATO's response to Russia's full-scale invasion has been marked by a deliberate and calibrated harmonization of deterrence and diplomacy – two instruments that were previously viewed as antagonistic but are now increasingly recognized as mutually reinforcing elements of collective security. NATO has displayed strategic dexterity commensurate with the complexity of today's conflict by updating its deterrence infrastructure while deepening diplomatic engagement.

From the quick development of advanced defense capabilities to the formation of the NATO-Ukraine Council, the Alliance has demonstrated both military strength and political resolve. The shift toward deterrence-by-denial, aided by technology innovation and resilience-building, represents a pragmatic realization that credible deterrent must be effective across conventional, cyber, and informational domains. Meanwhile, NATO's diplomatic approach, which includes internal consultations, external collaborations, and open-door enlargement, has strengthened the Alliance's political unity and global importance.

NATO's agility in this crisis has been not only reactive, but productive. The integration of Finland, the projected accession of Sweden, and the increase in defense spending among member states all indicate a collective acknowledgment of the changing geopolitical realities confronting the Euro-Atlantic region. These developments highlight NATO's ongoing transition from a Cold War-era military bloc to a dynamic, multifaceted security entity capable of navigating hybrid threats, great power competition, and normative challenges to democratic order.

However, as the immediate urgency of the Ukraine war grows, the strength of NATO's cohesion will be tested by internal difference, shifting global alignments, and growing dangers outside Europe's boundaries. The Alliance's future significance will be determined by its ability to institutionalize strategic foresight, foster unity amidst political variety, and explain its mission to new generations of citizens. In this setting, NATO's symphony of strength – the combination of hard might and principled diplomacy – must be more than just a verbal construct. It must be the driving spirit of a reinvigorated Alliance, ready not just to deter aggression, but also to construct a more secure, cooperative, and resilient international order in the decades ahead.

References

Allison, G. (2017). Destined for War: Can America and China Escape Thucydides's Trap? Houghton Mifflin Harcourt.

Anderson, M. P. (2016). NATO Nuclear Deterrence: The Warsaw Summit and Beyond. Connections: The Quarterly Journal, 15(4), pp.5-30. https://www.jstor.org/stable/26326457

Auerswald, D. P., & Saidemen, S. M. (2014). NATO in Afghanistan: Fighting Together, Fighting Alone. Princeton: Princeton University Press.

Burns, N., & Lute, D. (2019). NATO at Seventy: An Alliance in Crisis. Belfer Center for Science and International Affairs.

Campbell, H., & Mazrui, A. A. (2013). Global NATO and the Catastrophic Failure in Libya. NYU Press. http://www.jstor.org/stable/j.ctt9qfrnd

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism, 1(1), pp.24-34.

Daehnhardt, P. (2011). The Masdrid Summit and NATO'S New Strtegic Concept. IDN Brief | The Madrid Summit and NATO's New Strategic Concept

Dagdelen, S. (2024). NATO: A Reckoning with the Atlantic Alliance. LeftWord Books.

Dragan, G. B., Arfi, B., Tiberius, V., Ammari, A., & Ferasso, M. (2024). Acceptance of circular entrepreneurship: Employees' perceptions on organizations' transition to the circular economy. Journal of Business Research, 173, pp.114-461.

Drylie, J. (2024). Intelligence Studies: Politicization of Intelligence. Politicization of Intelligence – Intelligence Studies – LibGuides at Naval War College

Goldgeier, J., & Shifrinson, J. R. (2023). Evaluating NATO Enlargement: From Cold War Victory to the Russia-Ukraine War. Brookings Institution.

Habeeb, A. R. (2024). Evaluating the Scandinavian economy's transition to a sustainable environment. Fresh evidence from newly developed CS-ARDL approach. Resources Policy, pp.104-566.

Hof, T. v. (2025). The End of NATO? Trump, Ukraine and the Fracturing of the West: How America's Shift, Europe's Divide, and Cultural Clashes Are Threatening Global Security. The End of NATO? Trump, Ukraine and the Fracturing of the West: How America's Shift, Europe's Divide, and Cultural Clashes Are Threatening Global Security – Kindle edition by van 't Hof, Tat. Politics & Social Sciences Kindle eBooks @ Amazon.com.

Ingram, P. (2011). NATO's Nuclear Deterrence Posture and Baltic Security. British American Security Council.

Iversen, K. B. (2012). Danish Perspective on Baltic Security. Copenhagen: Biblioscholar.

Kott, A. &.-G. (2018). Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop. doi:10.48550/arXiv.1804.07651

Larsen, H. (2022). NATO's Adaptation to the Russia Threat. CSS Analyses in Security Policy, pp.1-4. CSSAnalyse306-EN.pdf

Marrone, A. (2022). NATO's New Strategic Concept: Novelties and Priorities. Istituto Affari Internazionali.

Ringsmose, J. &. (2020). Hedging their bets? The case for a European pillar in NATO. Defence Studies, 20(4), pp.295-317.

Rynning, S. (2024). NATO: From Cold War to Ukraine, a History of the World's Most Powerful Alliance. Yale University Press.

Smith, F. L., Kollars, N. A., & Schechter, B. H. (2024). Cyber Wargaming: Research and Education for Security in a Dangerous Digital World. Washington: Tantor Audio.

Sorooshian, S. (2024). The sustainable development goals of the United Nations: A comparative midterm research review. Journal of Cleaner Production, 453(10), pp. 142-272. doi:https://doi.org/10.1016/j.jclepro.2024.142272

Stephen G. Brooks, W. C. (2016). The Rise and Fall of the Great Powers in the Twenty-first Century: China's Rise and the Fate of America's Global Position. International Security, 40(3), pp.1-53.

The Importance of Leadership in International Relations

Alberto Messeri
Student, University of Palermo

In an era marked by complex global threats, leadership is pivotal in ensuring international security and resilience. Machiavelli, in "The Prince", aptly noted: "The lion cannot protect himself from traps, and the fox cannot defend himself from wolves. One must therefore be a fox to recognize traps, and a lion to frighten wolves." This quote highlights the necessity for leaders to possess both strategic wisdom and determination, as well as the adaptability to navigate diverse challenges.

Equally important is the leader's role in fostering resilience – the ability to absorb, adapt, and recover from shocks. It is imperative for leaders to consider the long-term impacts of their actions, as neglecting resilience can lead to detrimental outcomes. This article examines the dual faces of effective leadership and how young leaders should be, in theory, more indicated to take over in the global equilibrium.

Key words: game theory, global equilibrium, international relations, leadership, young leaders.

Laikmetā, kurā pastāv sarežģīti globāli draudi, līderībai ir izšķiroša nozīme starptautiskās drošības un noturības nodrošināšanā. Makiavelli savā darbā **"**Valdnieks**"** trāpīgi rakstīja: *"Lauva nespēj pasargāt sevi no slazdiem, un lapsa nespēj aizsargāties pret vilkiem. Tāpēc jābūt lapsai, lai atpazītu slazdus, un lauvai, lai iebiedētu vilkus."* Šis citāts uzsver, cik svarīgi ir, lai līderiem būtu abas kvalitātes – gan stratēģiska gudrība un apņēmība, gan spēja pielāgoties dažādiem izaicinājumiem.

Tikpat svarīga ir arī līdera loma noturības veicināšanā – spējā absorbēt, pielāgoties un atgūties pēc satricinājumiem. Ir būtiski, lai līderi ņemtu vērā savu rīcību ilgtermiņa sekas, jo noturības ignorēšana var novest pie nopietnām negatīvām sekām. Šajā rakstā tiek aplūkotas efektīvas līderības

divas puses un tas, kāpēc jaunajiem līderiem būtu lielāka piemērotība pārņemt vadību globālā līdzsvara uzturēšanā.

Atslēgvārdi: globālais līdzsvars, jaunie līderi, spēļu teorija, starptautiskās attiecības, līderība.

Introduction

In an age defined by multiple crisis – an overlapping of military, environmental, economic, and social challenges – the importance of leadership in international relations has become central to global stability. While leadership has always been a factor in diplomacy and conflict resolution, today it plays a more complex and nuanced role. Modern leaders must respond to a variety of stakeholders, act within institutional and legal constraints, navigate transnational crises, and communicate effectively in a hyper-connected world. In this context, leadership cannot be reduced to charisma or decisiveness alone. It must include strategic foresight, emotional intelligence, institutional awareness, and moral clarity.

The study of leadership has always been central to political science. As early as the 4th century B.C., Plato, in his dialogues Statesman (*Politicus*) and Republic, reflected deeply on the nature of leadership and the ideal structure of the state. Another great example is represented, during the 16th century, by Machiavelli, that would continue this inquiry in his political treatises, particularly The Prince. Historically, leadership was often associated with authoritarian command, territorial ambition, or dynastic power. However, in modern international relations, especially in liberal democracies and multilateral systems, effective leadership is rooted in legitimacy, long-term vision, and capacity for coordination across actors and borders. From global health governance to security alliances, leaders today must perform on a multilevel stage: local, national, regional, and international. Failure at any of these levels can produce cascading consequences that destabilize entire regions.

The central aim of this article is to explore what makes leadership effective in international relations, and to argue that leaders that possess also the quality of long-term vision – when supported by strong institutions – can play a transformative role in shaping a more resilient, equitable, and cooperative world order. The following sections examine how leadership functions

in international contexts, what qualities are needed in the 21st century, the role of institutions, and why empowering youth may offer one of the best responses to contemporary global governance challenges.

Leadership in historical and institutional context

Leadership in international affairs has not always been understood in the same way. In the early modern period, sovereign rulers wielded unchecked power in a relatively anarchic international system. Diplomacy was secretive and personalized, often conducted by monarchs or their closest confidants. Treaties, alliances, and wars were all direct extensions of personal leadership decisions.

The Peace of Westphalia (1648) marked a turning point in international politics by establishing the legal principle of state sovereignty and codifying a new diplomatic order (Osiander, 2001). Later, the formation of institutions like the League of Nations and, more effectively, the United Nations, formalized the idea that leadership must operate within shared norms and frameworks. This institutional shift altered both the style and substance of global leadership. Leaders became accountable not only to domestic audiences but also to multilateral agreements and international scrutiny (Guterres, 2021).

Today, leaders do not act in a vacuum. Their choices are constrained – and sometimes enabled – by institutions such as the United Nations, NATO, the European Union, and the African Union. The actions of national leaders are scrutinized by international courts, media networks, NGOs, and their own constituencies. International leadership has become as much about managing complexity as it is about asserting authority.

Legal and political frameworks shaping modern leadership

Modern leadership functions within a complex web of legal and institutional frameworks that simultaneously empower and constrain its exercise. In democratic systems, these frameworks include constitutions, parliaments, independent judiciaries, and a free press. At the international level, they encompass treaty obligations, customary international law, and participation in multilateral organizations. For instance, Article 78 of the Italian

Constitution explicitly reserves the authority to declare war to Parliament, thereby restricting the executive's discretion in matters traditionally considered the prerogative of the head of state. Comparable provisions are found in many other democratic systems, where leaders are required to obtain legislative approval before committing to military action or binding international agreements. In this way, decision-making is no longer the domain of a single individual but is mediated through collective and institutional processes.

This reality prompts an important question: if leadership is increasingly embedded in collective governance, why does the study of individual leadership still matter? The answer lies in two critical observations. First, not all states are democratic, and thus not all leaders are subject to the same institutional checks and balances. In authoritarian or hybrid regimes, individual leaders may retain extensive discretionary power over foreign and military policy. Second, even within democracies, representative mechanisms mean that elected officials – often a single individual such as a president or prime minister – are entrusted with embodying the will of the people and are expected to act on their behalf in moments of crisis. These individuals, operating within institutional systems, still wield significant influence in shaping the strategic direction of their states. Hence, the analysis of leadership remains central to understanding both domestic and international political behaviour.

Moreover, global governance is increasingly shaped by legal norms that define acceptable leadership conduct. International humanitarian law, human rights conventions, and environmental accords impose clear expectations on state behaviour. Leaders who violate these norms face reputational damage, economic sanctions, or even legal accountability through mechanisms such as the International Criminal Court (ICC). Rather than limiting leadership, this evolving legal architecture provides a framework through which leaders can act with legitimacy and navigate crises with greater clarity and cooperation.

Ultimately, effective leadership in today's international system is not about bypassing constraints but about working constructively within them. It is defined by the ability to coordinate institutional actors, persuade international partners, and reconcile national interests with global responsibilities. In this sense, leadership becomes not an act of domination, but an exercise in integration and strategic stewardship.

In the next paragraphs will try to identify which are the essential qualities that a contemporary leader must possess.

The Essential qualities of contemporary leadership

Effective leadership in the international arena hinges on a set of interrelated traits: strategic foresight, resilience, moral legitimacy, and communication skills. Nowadays leadership needs to be inspired by a balance between national interest and global responsibility.

Strategic foresight and long-term thinking

Leaders in the 21st century must transcend the narrow confines of electoral cycles and engage with systemic, long-term challenges that threaten global stability. Issues such as climate change, technological disruption, and widening global inequality are not episodic concerns – they require strategic continuity, institutional innovation, and cross-border collaboration. As Sternberg (2007) suggests, wisdom in leadership involves the capacity to foresee future consequences and make ethically grounded decisions that serve both present and future generations. Strategic foresight enables leaders to design preventive policies, foster resilience, and establish international initiatives before emerging risks develop into full-blown crises.

One of the most illustrative examples of long-term leadership in recent history is Angela Merkel's role during the Eurozone crisis. Rather than opting for politically expedient solutions, Merkel engaged in sustained, often unpopular negotiations that emphasized fiscal stability and European unity, prioritizing long-term structural reform over short-term national gain (Carbone, 2021). This approach exemplifies a core quality of contemporary global leadership: the ability to navigate immediate political pressure while maintaining a focus on broader, intergenerational goals.

Historical precedents further demonstrate the power of long-term strategic thinking. Figures such as Robert Schuman and Jean Monnet, architects of the post-war European project, envisioned supranational institutions that would make future conflicts not only unthinkable but materially impossible. Their proposal for the European Coal and Steel Community laid the foundation for what would become the European Union – arguably one of the most

successful peace-building initiatives of the modern era (Guterres, 2021). This contrasts sharply with the short-sighted rivalries of the Cold War era, where superpowers prioritized competition over cooperation. The absence of a shared long-term vision in that context contributed to proxy wars, arms races, and enduring instability – highlighting the profound consequences of leadership driven by immediate political or ideological gains rather than collaborative, future-oriented strategy.

Resilience, crisis management and capacity of adaptability

The COVID-19 pandemic served as a profound litmus test for global leadership, revealing stark differences in how political leaders respond to crisis under conditions of uncertainty, fear, and institutional stress. Countries that succeeded in mitigating the health and economic impacts of the pandemic were often led by individuals who demonstrated clarity of purpose, empathy in communication, and the adaptability to revise policies as new information emerged. A widely cited example is Jacinda Ardern's leadership in New Zealand: her government's swift implementation of lockdown measures, coupled with transparent and emotionally intelligent public messaging, not only saved lives but also reinforced public trust and social cohesion (UN Youth Envoy, 2022).

Resilient leadership, however, is not defined solely by personal traits – it is fundamentally about building and leveraging institutional capacity. Effective leaders must coordinate across sectors and levels of government, mobilize both technical expertise and financial resources, and maintain public confidence during prolonged periods of disruption. According to Guterres (2021), resilience in governance involves not just the ability to endure shocks, but to transform institutions in ways that reduce future vulnerabilities. This includes investing in healthcare infrastructure, improving crisis communication systems, and fostering international collaboration for resource sharing and innovation.

Closely related to resilience is the quality of adaptability, which has become an essential trait for leaders in an era characterized by rapid technological change, global interdependence, and socio-political volatility. While adaptability has long been valued – famously captured by Machiavelli's metaphor of the lion and the fox in The Prince – its significance is amplified

in today's fast-evolving world. As Machiavelli observed, a leader must be "a lion to frighten wolves and a fox to recognize traps" (Machiavelli, 1998). This metaphor continues to resonate, but modern circumstances demand an even more dynamic and iterative form of adaptation.

In contemporary governance, adaptability means more than adjusting tactics; it entails rethinking frameworks, experimenting with new forms of diplomacy, and embracing innovation. Leaders must be open to scientific advice, capable of pivoting policy when evidence shifts, and agile enough to navigate both digital and geopolitical transformations. During the pandemic, for instance, governments that integrated real-time epidemiological data into their decision-making, updated regulations to support remote work, and employed digital platforms for public health messaging demonstrated a much higher degree of policy flexibility and effectiveness.

In this sense, the ability to adapt is no longer a supplementary asset – it is a foundational leadership skill. Those who fail to recognize shifting dynamics or cling to rigid strategies risk exacerbating crises and losing both legitimacy and control. By contrast, leaders who embody adaptive resilience – who combine institutional robustness with strategic flexibility – are better positioned to protect their societies and strengthen global cooperation in the face of unpredictable challenges.

Resist to political and personal incentives

Political incentives often diverge from both personal interest and purely rational models of decision-making, leading to outcomes that reflect complex political calculations rather than objective utility. Leaders frequently make decisions not solely based on strategic necessity but also to maintain domestic popularity, respond to shifting public sentiment, or enhance their prospects for re-election. A well-known example of this phenomenon is the Falklands War in 1982, during which British Prime Minister Margaret Thatcher's decision to launch a military response was widely interpreted as influenced by internal political pressures. The conflict, though costly, significantly bolstered her domestic support and helped secure her electoral victory the following year.

In contrast, more ethically grounded leadership can be observed in the context of the European sovereign debt crisis. Faced with rising debt levels

and pressure from international markets, several European leaders – includ ing those in Greece, Italy, and Germany – were compelled to implement highly unpopular austerity measures and structural reforms. These decisions, often met with fierce public opposition and exploited by populist movements, demonstrated a willingness to prioritize long-term national and European stability over short-term political gain. Despite the immediate electoral risks, such choices reflect a more virtuous dimension of leadership: acting in the broader public interest, even at the cost of personal or party popularity.

Institutions as catalysts for responsible leadership

A big role in the expression of this characteristic, that a today's leader should have, is played by Institutions such as the United Nations, the European Union, and regional organizations. They amplify a leader's capacity to act while simultaneously imposing constraints to protect collective interests.

Multilateral institutions reduce the transaction costs of diplomacy, create shared norms, and enable burden-sharing in addressing complex problems. For example, the European Union's governance structure requires leaders to engage in constant dialogue, compromise, and joint decision-making – skills essential for modern global leadership (Panke, 2012).

However, institutions can also be weakened by poor leadership. The delayed international response to the 1994 Rwandan genocide, due to bureaucratic inertia and political cowardice, illustrates how the absence of leadership within institutions can lead to catastrophic outcomes (UN Youth Envoy, 2022). Even when international institutions operate with the intention of preserving peace, enforcing agreements, or managing global challenges, tensions can arise between their decisions and the preferences of national leaders. It is not uncommon for heads of state to publicly oppose or undermine the rulings of international bodies, even when those decisions are based on legal frameworks or shared commitments. These conflicts reveal a deeper structural problem: when international obligations collide with domestic political interests, some leaders may choose to defend their national popularity or political standing rather than uphold international norms. In such cases, the personal or electoral interests of a leader can

override the rational and cooperative path proposed by international institutions. This dynamic illustrates how the effectiveness of global governance depends not only on institutional design but also on the integrity and orientation of national leadership. Where leadership is short-sighted or self-interested, even the most well-constructed international mechanisms can be weakened or delegitimised.

To enhance the quality of leadership, institutions must promote transparency, provide training, and ensure inclusive representation. Bodies such as the World Trade Organization and the UN Security Council must evolve to reflect demographic and geopolitical realities, giving more voice to underrepresented nations and emerging leaders.

However, institutions are not infallible. When they fail to adapt, when they are co-opted by special interests, or when they lack enforcement mechanisms, they can become complicit in leadership failures. The 1994 Rwandan genocide, for example, revealed the devastating consequences of institutional paralysis and inadequate leadership at the United Nations. Similarly, the inability of the World Trade Organization to manage new digital trade conflicts, or the failures of the international community to prevent Russia's 2022 invasion of Ukraine, highlight the limits of institutional influence when not backed by decisive and coordinated leadership.

This interdependence means that reforming institutions is part of enabling better leadership. Democratizing representation within global organizations, enhancing transparency, and ensuring enforceability of rules can help foster a new generation of accountable, strategic, and responsive leaders. By embedding states within frameworks of norms, rules, and enforcement mechanisms, these institutions help align short-term political incentives with longer-term cooperative outcomes. They provide platforms for dialogue, reduce transaction costs in diplomacy, and impose reputational and material costs on states that defect from cooperative agreements.

Toward a new model of leadership incentives

The preceding discussion highlights several important conclusions: leaders decisions arise from complex considerations, shaped by evolving perceptions of payoffs and political incentives. Within this complexity leaders – owing to their longer time horizons and greater personal investment in

future outcomes – may be more naturally inclined toward strategies that emphasize cooperation, stability, and multilateralism. Furthermore, despite the anarchic nature of the international system, collective mechanisms of sanction and enforcement exist that can reinforce cooperative behaviours and deter opportunistic defection.

Recognising these dynamics suggests the need for a new perspective in evaluating and selecting leaders. Traditional criteria – such as experience, military credentials, or ideological commitment – should be complemented by a careful assessment of a leader's future orientation and long-term strategic incentives. A leader's capacity to internalise the future consequences of present actions, to prioritise sustainable peace over short-term victories, and to perceive cooperation as a strategic asset rather than a vulnerability, should become central to political theory and practice. Particularly in an international environment increasingly defined by complex interdependence, the ability to think and act with a long-term horizon may prove to be among the most critical leadership qualities.

Therefore, the promotion of future-oriented leadership must go hand in hand with strong institutional frameworks that educate, constrain, and channel leaders' actions. Robust democratic systems, transparent decision-making processes, and a resilient international order are indispensable complements to individual leadership qualities. As Machiavelli wisely advised, success requires not only *virtù* – the internal qualities of the leader – but also the wisdom to adapt to *fortuna* – the unpredictable circumstances of the world. In this sense, fostering leaders who embody strategic patience, adaptability, and long-term rationality is not simply an ideal but a practical necessity for ensuring stability and cooperation in the 21st century.

The prospective of young people

An increasingly relevant dimension of leadership today – though not necessarily a new criterion – is the ability to recognize the importance of engaging younger generations in the decision-making process. In recent years, many democratic societies and international institutions have faced a significant erosion of public trust (OECD, Survey on Drivers of Trust in Public Institutions – 2024 Results). This crisis of legitimacy is particularly pronounced among youth, who often perceive political systems as

unresponsive, opaque, or dominated by self-interested elites (Cammaerts et al., 2014). As trust in institutions declines, the effectiveness of leadership is also undermined, making it more difficult for national governments and global organizations to implement coherent and inclusive policies.

One potential remedy to this legitimacy deficit is greater inclusion of youth – not merely as symbolic participants, but as active contributors and, ultimately, as leaders themselves. Involving young people in policy design, strategic planning, and institutional governance not only broadens representation but injects fresh perspectives into systems that can otherwise become stagnant or detached from societal realities. Leadership, in this sense, is not only about authority but about listening, empowering, and incorporating diverse generational experiences.

Recent years have witnessed numerous examples of young individuals playing transformative roles in international affairs. Greta Thunberg, though not an elected official, has become one of the most influential voices in global climate advocacy. Through the Fridays for Future movement, she has mobilized millions of young people worldwide, directly challenged political elites, and helped reframe the climate crisis as a moral and intergenerational issue (Fridays for Future, 2025). Her impact demonstrates that leadership is not confined to formal office – it can emerge wherever individuals are able to influence global agendas, mobilize collective action, and hold power accountable.

Historically, young leadership has also played a decisive role in shaping the world. Alexander the Great ascended to power in his early twenties and radically transformed the geopolitical landscape of his time. In modern contexts, the world of technology offers striking examples of youth-driven transformation. Founders such as Bill Gates and Mark Zuckerberg launched ventures in their early twenties that not only created vast economic value but redefined communication, commerce, and information access. While business leadership and political governance are distinct domains, both demonstrate the capacity of young individuals to lead, innovate, and reshape their environments.

Thus, a key leadership competency in today's world may be the ability to engage with and learn from younger generations. This involves not only selecting young people for leadership roles, but fostering intergenerational dialogue, mentorship, and institutional mechanisms that ensure their voices

are heard and respected. Youth are not only future leaders – they are already shaping the world through activism, entrepreneurship, diplomacy, and digital innovation. The task of contemporary leadership is to recognize this reality and act accordingly, integrating youth participation into the heart of global governance and some steps in this direction have been done, in fact we have programs like the UN Youth Envoy or EU Youth Strategy 2019–2027. It will be interesting to see if there will be further initiatives of this kind internal in the countries.

Conclusion

In addressing the role of leadership in international relations, this article has engaged with one of the most persistent and complex challenges of political analysis: how to understand, predict, and guide the behaviour of those entrusted with the power to act on behalf of the state. From classical reflections by Plato and Machiavelli to modern frameworks such as game theory, the question of leadership has been examined across time, cultures, and ideologies. While contexts have changed dramatically, the core dilemma remains: how can leaders make decisions that safeguard not only their immediate interests but also the long-term well-being of their societies and the international order?

The increasing complexity of leadership in a world characterized by overlapping crises – security threats, institutional fragility, and interdependence on a global scale. It was highlighted how the modern state, far from being an absolutist entity under the control of a single individual, is now embedded in legal, political, and bureaucratic frameworks that both constrain and support leadership action. This transformation has opened the door for rational, deliberate decision-making, which in turn makes analytical tools like game theory more relevant for understanding political behaviour.

At the same time, leadership remains deeply personal. It is shaped not only by structural factors but also by internal political dynamics, ambition, ideology, and the desire for legacy or survival. These subjective dimensions often influence decision-making as much as, or more than, purely strategic calculations. As this article has shown, personal and political incentives, as well as time horizons, play a critical role in determining the quality of

leadership behaviour. Leaders focused solely on short-term gains – whether electoral or reputational – are less likely to invest in cooperative or sustainable strategies. Conversely, those who consider the broader implications of their actions, and who act with intergenerational responsibility, are better positioned to contribute to a stable and just international system.

This led to the second key pillar: the role of institutions in reinforcing or constraining leadership behaviour. Institutions such as the European Union, the United Nations, the World Trade Organization, and various regional bodies create frameworks that encourage cooperation, penalize defection, and reduce the volatility of state interactions. These structures do not eliminate the importance of individual leadership but instead serve as necessary complements. They embed leaders within a system of shared expectations and accountability, altering the cost-benefit calculation of strategic choices. Institutions, when properly designed and enforced, enable prudent leadership to flourish.

Finally in the decades ahead, the quality of leadership will become more important – not less – as global interdependence increases. The challenges we face today are no longer confined by borders: climate change, technological disruption, pandemics, and economic fragility require a kind of leadership that is cooperative, future-oriented, and institutionally grounded. Leaders who think only in electoral terms, or who view diplomacy through the narrow lens of personal power, will not be equipped to manage these risks. What is needed are individuals – and leadership cultures – that recognize the value of strategic patience, adaptability, and intergenerational responsibility.

In this sense, the most vital trait of leadership in the 21st century may not be charisma or force, but vision: the ability to see beyond the immediate game, to understand that the outcomes of today's choices shape not only political careers but the viability of global order itself. Leadership must be rooted in a deeper understanding of systems, incentives, and time – a Machiavellian realism coupled with a renewed commitment to cooperation and collective survival. This is not an idealistic aspiration, but a pragmatic necessity for a world increasingly defined by shared fate.

References

Burns, J. M. (1978). *Leadership. New York*: Harper & Row.

Carbone, M. (2021). EU Development Policy and the Global South: New Leadership, Old Challenges. *Third World Quarterly*, 42(1), pp. 23-39.

Fearon, J. D. (1995). Rationalist Explanations for War. *International Organization*, 49(3), pp. 379-414.

Guterres, A. (2021). *Our Common Agenda: Report of the Secretary-General*. New York: United Nations.

Hall, T. H. and Ross, A. A. G. (2015). Affective Politics after 9/11. *International Organization*, 69(4), pp. 847-879.

Italian Republic. (1948): Constitution of the Italian Republic. https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf

Machiavelli, N. (1998). *The Prince*. Oxford: Oxford University Press.

Nye, J. S. (2008). *The Powers to Lead*. Oxford: Oxford University Press.

OECD (2024): Survey on Drivers of Trust in Public Institutions – 2024 Results. OECD Survey on Drivers of Trust in Public Institutions – 2024 Results (EN)

Panke, D. (2012). Leadership in the European Union: An Empirical Assessment of the Role of the Council Presidency. *Journal of Common Market Studies*, 50(2), pp. 258-275.

Plato (2008). *Republic and Statesman*. Indianapolis: Hackett Publishing Company.

Snyder, G. H. (1971). "Prisoner's Dilemma" and "Chicken" Models in International Politics. *International Studies Quarterly*, 15(1), pp. 66-103.

Sternberg, R. J. (2007). *Wisdom, Intelligence, and Creativity Synthesized*. Cambridge: Cambridge University Press.

Societal Cyber Resilience

Žaneta Ozoliņa
Senior researcher, University of Latvia

Sigita Struberga
Lecturer, University of Latvia

Societal cyber resilience forms an integral component of national security, epitomizing the collective capacity of a community or society to proactively prepare for, respond to, and recuperate from cyber threats and incidents, all the while preserving its functionality and overall well-being. The overarching objective of this article is to systematically examine the endeavors undertaken by individuals, groups, and non-governmental organizations aimed at fortifying cybersecurity practices, fostering heightened awareness, and constructing a robust foundation capable of withstanding and rebounding from cyber-attacks, such as resource constraints, rapid technological changes, and the evolving nature of cyber threats.

This exploration of societal cyber resilience will meticulously scrutinize pivotal elements, including education and awareness, training and skill development, collaborations and information sharing, community engagement, public-private partnerships, and adaptive strategies. The synthesis of these critical components is poised to empower societies, augmenting their resilience to effectively endure and rebound from diverse cyber threats. This comprehensive approach presented in the article seeks to establish a more secure and resilient environment, not only safeguarding the interests of individuals and businesses but also fortifying the critical infrastructure that underpins societal functionality.

Given Latvia's societal exposure to a myriad of cyber threats emanating from neighbouring countries, particularly Russia and Belarus, a focused analysis of potential challenges and corresponding resilience-building strategies becomes imperative. Through a nuanced examination of these dynamics, this article aims to contribute to the discourse surrounding cybersecurity preparedness and resilience, offering insights that are particularly relevant in the context of Latvia's unique geopolitical landscape.

Key words: cyber resilience, societal security, cybersecurity, adaptation strategies.

Sabiedrības kiberdrošības noturība ir neatņemama nacionālās drošības sastāvdaļa, kas atspoguļo kopējo sabiedrības vai kopienas spēju sagatavoties kiberdraudiem un incidentiem, reaģēt un atgūties no tiem, vienlaikus saglabājot spēju darboties un vispārējo labklājības līmeni. Šī raksta mērķis ir analizēt indivīdu, grupu un nevalstisko organizāciju centienus stiprināt kiberdrošības praksi, kas veicinātu lielāku informētību un izveidotu nosacījumus spējai atgūties no kiberuzbrukumiem, ņemot vērā tādus izaicinājumus kā resursu ierobežojumi, straujās tehnoloģiju pārmaiņas un kiberdraudu mainīgais raksturs.

Sabiedrības kiberdrošības noturības izpētē uzmanība veltīta tādiem elelmentiem kā izglītībai un informētībai, apmācībām un prasmju attīstībai, sadarbībai un informācijas apmaiņai, publiskā un privātā sektora partnerībai un pielāgošanās stratēģijām. Šo būtisko komponentu sintēze ir vērsta uz sabiedrības iespējošanu, lai efektīvi pārvarētu un atgūtos no dažāda veida kiberdraudiem. Ņemot vērā Latvijas sabiedrības pakļautību dažādiem kiberdraudiem, jo īpaši Krievijas un Baltkrievijas izraisītos, ir būtiski koncentrēties uz iespējamo izaicinājumu analīzi un atbilstošu noturības stiprināšanas stratēģiju izstrādi. Šo elementu izpēte saturiski papildinās diskusijas par kiberdrošības noturību, piedāvājot atziņas, kas īpaši nozīmīgas Latvijas unikālās ģeopolitiskās situācijas kontekstā.

Atslēgvārdi: kiberdrošības noturība, sabiedrības drošība, kiberdrošība, adaptēšanās stratēģijas.

Introduction

In the digital age, cyber security has become a critical component of societal stability and national security. As technology integrates deeper into the fabric of daily life, the threats posed by cyber-attacks have evolved, affecting not just individuals and corporations but society at large. This article explores the broad spectrum of societal cyber security, highlighting the emerging threats and discussing strategies to mitigate their impact leading to societal resilience.

The concept of societal cyber resilience is fundamental due to the relevance to national security, but not sufficiently explored. As Joinson, et al (Joinson et al., 2023, p.1) argue "There is a distinct lack of research on

what would constitute cyber resilience in individual users of technology who may encounter cybersecurity incidents in a domestic or non-work setting." Necessity to introduce societal perspectives in cyber security domain is underlined and argued in Joe Burton's and Clare Lain's study (Burton & Lain, 2020). They (Burton & Lain, 2020, p. 454) also emphasize the relevance of cognitive perspectives in cyber attacks: "The latest research on societal influences on cybersecurity supplement these theoretical assumptions by elevating the cognitive influence of cyberattacks and the cognitive effects generated within target populations. Fear, uncertainty and the sense of anxiety that cyber intrusions engender may shape responses in irrational ways, including in a national security context". Societal cyber security reflects a community's capacity to confront, respond to, and recover from cyber threats. In an era where digital infrastructure underpins many aspects of everyday life, from personal communications to critical national services, maintaining robust cyber defences is essential. This article delves into the multifaceted nature of societal cyber resilience, examining its key components and the proactive measures adopted by individuals, organizations, and governments.

The increasing frequency and sophistication of cyber threats have necessitated a shift from traditional defensive cyber security measures to a more resilient approach. This involves not only preventing attacks but also developing the capacity to absorb impacts, maintain essential functions, and swiftly recover. Societal cyber resilience encompasses various domains, including technical infrastructure, public awareness, policy frameworks, and collaborative efforts across different sectors.

A critical aspect of societal cyber resilience is the role of non-governmental organizations (NGOs), private sector entities, and community groups in enhancing cyber security practices. These actors contribute significantly to promoting awareness, education, and proactive defence measures. By fostering a culture of cyber hygiene and encouraging the adoption of best practices, they help build a more resilient society capable of withstanding and recovering from cyber incidents.

This article further illustrates and analyses these efforts through the case study of Latvia, a country that has made notable strides in enhancing its societal cyber resilience. Latvia's experience provides valuable insights into the practical implementation of cyber resilience strategies. The analysis

draws on empirical evidence collected from interviews with specialists across various sectors, including governmental, non-governmental, and business entities. Additionally, secondary data from public opinion polls and an examination of policy documents provide a comprehensive background.

Latvia's proactive stance in cyber security is highlighted by its multifaceted approach. The government has implemented robust policies and frameworks aimed at strengthening national cyber defences. These measures are complemented by initiatives from the private sector and NGOs, which focus on raising awareness, educating the public, and fostering collaboration. The collective efforts of these stakeholders create a resilient foundation, capable of responding to and recovering from cyber threats.

The analysis of Latvia's case also demonstrates the importance of public-private partnerships in building societal cyber resilience. Such collaborations leverage the strengths and resources of different sectors, creating a more comprehensive and effective defence against cyber threats. By integrating efforts across various levels of society, Latvia exemplifies how a coordinated approach can enhance national security and societal stability.

Societal cyber resilience is a critical aspect of todays and tomorrow's national security. As cyber threats continue to evolve, it is imperative for societies to adopt a resilient approach, encompassing prevention, response, and recovery. Through the examination of Latvia's case, this article highlights the importance of a collective effort involving individuals, organizations, and governments in building a robust and resilient cyber infrastructure. By fostering awareness, education, and collaboration, societies can better withstand and recover from cyber-attacks, ensuring stability and security in the digital age.

Understanding societal cyber resilience

This chapter delves into the theoretical underpinnings of societal cyber resilience, highlighting the decisive factors that influence resilience levels and showcasing empirical evidence of effective strategies. It aims to provide a comprehensive understanding of how societies can build and sustain resilience in the face of evolving cyber threats.

The theory of societal cyber resilience is an increasingly critical aspect of both contemporary and future national security. As cyber threats continue to evolve in complexity and scope, it is imperative for governments, IT businesses, and societies at large to adopt a resilient and holistic approach. The

development of cyber-resilient societies necessitates the establishment of a robust theoretical framework that thoroughly examines and delineates the multifaceted components of cyber resilience. This framework is essential for assessing the level of resilience within a society and for monitoring progress over time.

Identifying key components that determine societal resilience is vital to understanding how societies can withstand and recover from cyber incidents. Empirical studies play a crucial role in this context, offering a wealth of best practices that can be adopted and adapted. These studies also provide valuable lessons learned, which can help mitigate potential vulnerabilities and prevent failures. By integrating empirical insights with a solid theoretical foundation, societies can better prepare for and respond to cyber threats, thereby enhancing their overall resilience.

There are several reasons motivating necessity to apply the concept of societal cyber resilience in theory and practice. Daily life of individuals is substantially depending on access and functionality of **critical infrastructure**. Such services, which are essential for societies – power grids (for instance, attacks on power grids can cause widespread blackouts, disrupting daily life and economic activities; blackouts can affect everything from household heating to industrial operations, leading to financial losses and jeopardizing public safety), healthcare (as example, hospitals and healthcare providers are prime targets for ransomware attacks, where malicious actors encrypt critical data and demand ransom for its release, thus delaying medical treatments and endangering patient lives. The financial burden of paying ransoms and recovering from these attacks also strains healthcare resources. The theft of sensitive patient data can lead to identity theft and loss of privacy, undermining public trust in healthcare institutions, leading to a loss of confidence among patients and stakeholders), transportation, and financial systems, are increasingly reliant on digital technologies. A cyberattack on any of these sectors can lead to catastrophic consequences, affecting millions of people. Societal cyber resilience ensures that these infrastructures can withstand, quickly recover from cyber incidents and individuals are aware of actions to be taken in order to minimize risks and threats to their lives and ensure basic needs.

Cyberattacks can have severe economic impacts, from direct financial losses to indirect costs associated with downtime and recovery efforts. For

instance, phishing, malware, and social engineering to gain unauthorized access to banking systems, resulting in financial losses for individuals and institutions. These fraudulent activities can drain bank accounts, damage credit ratings, and lead to a loss of trust in financial institutions. The ripple effects of banking fraud can impact the broader economy, eroding consumer confidence and increasing the cost of banking services. Cyber espionage targeting corporations can lead to the theft of trade secrets, compromising competitive advantage and economic stability. Supply chain attacks can lead to the distribution of compromised goods, posing risks to consumer safety and damaging the reputation of affected companies. Ensuring the integrity of the supply chain is essential to maintain the trust and safety of products and services in the market.

In the era of cyber warfare, national security is closely tied to cyber resilience. State-sponsored cyberattacks can disrupt military operations, compromise sensitive data, destabilize national governance and even provoke societal distrust, polarization and unrest. Advanced technologies also increased the spread of disinformation and its impact on societies and national security. State and non-state actors use cyber tools to spread disinformation and influence elections, undermining democratic processes and trust in electoral outcomes. By manipulating information and public perception, these actors can sway election results, leading to political instability and eroding the legitimacy of elected officials. False information propagated through social media can incite violence, spread panic, and polarize communities, impacting societal cohesion. Disinformation can amplify divisions within society, leading to conflict and undermining social harmony. The rapid spread of false information on social media platforms makes it challenging to contain its impact and protect public discourse.

Besides, public trust in digital systems is crucial for the adoption of new technologies, the functioning of a digital economy and utilization of digital public services. When citizens are confident in the security and reliability of digital services, they are more likely to engage with and benefit from technological advancements and in the end become contributors to national economy and national security.

Understanding societal cyber resilience begins with the foundational concepts of classical resilience and cyber resilience. Classical resilience pertains to the ability of any system, organization, or community to withstand,

adapt, and recover from adverse conditions or disruptions. This broad definition lays the groundwork for more specific applications, such as cyber resilience. Cyber resilience, in turn, specifically addresses an organization's capability to prepare for, respond to, and recover from cyberattacks and incidents. It is a holistic approach that goes beyond traditional cybersecurity measures, which primarily aim to protect systems and data from attacks. Instead, cyber resilience emphasizes the ability to maintain critical operations and services despite these disruptions.

Expanding this concept further, societal cyber resilience refers to the collective efforts required by governments, businesses, and citizens to ensure the integrity and functionality of critical infrastructure and services in the face of cyber threats. This broader perspective acknowledges that the interconnected nature of modern societies means that cyber incidents can have far-reaching impacts beyond individual organizations. Therefore, societal cyber resilience involves a comprehensive strategy that integrates various stakeholders and sectors.

Moran Bodas et al. (Bodas et al., 2020) state that there is a consensus among scholars that better-prepared civilian populations are more capable of effectively responding to various emergencies, thereby increasing their overall resilience. According to them (Bodas et al., 2020, p. 2), "in contrast to national resilience, which deals with national infrastructure capacities to withstand and cope with hardships, societal resilience represents the ability of the members of the public to continue to function despite adversities". Elran Meir (Elran, 2017, p. 301) defines societal resilience as "the capacity of communities to flexibly contain major disruptions and to rapidly bounce back and forward following the unavoidable decline of their core functionalities". This distinction emphasizes the importance of individual and community preparedness in maintaining societal stability amidst crises. Research has shown that communities with higher levels of social capital, such as trust, networks, and norms, tend to recover more swiftly from disasters. Thus, fostering societal resilience not only involves preparing infrastructure and providing top-down approach for continuity of system function but also strengthening the social fabric and empowering individuals to act effectively in times of crisis.

Cyber resilience is generally defined as the ability of a system, organization, or society to withstand, adapt to, and recover from cyber-attacks and

incidents. Research literature emphasizes that cyber resilience is not just about defence but also about maintaining operational continuity in the face of cyber disruptions. As authors of the comprehensive overview of cyber resilience argue (Björck et al., 2015, p. 312): "Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. This ability can be considered at different levels". Such authors as Linkov (2013) and Chang & Shinozuka (2014) emphasize the necessity to use holistic approach to cyber resilience including also society, which as an integral part of cyber security landscape and is exposed to cyber threats and risks caused by humans or nature. Besides, societal cyber security includes also pro-active aspects of resilience, namely, undertaking actions by individuals and groups aimed at mitigating potential threats.

What are key components of societal cyber resilience?

Societal cyber security rests on several components, which derive from the concepts of resilience, cyber resilience and societal security. Cyber resilience hinges on a multifaceted concept of preparedness, encompassing technology, IT systems, states, and societies. Preparedness is an all-encompassing idea, yet specific areas indicate whether societies can confront cyber challenges and mitigate their impacts on individuals' lives.

A pivotal aspect of preparedness is risk assessment. This process demonstrates the ability to identify, evaluate, and withstand cyber threats and vulnerabilities. Effective societal cyber resilience begins with assessing potential threats, which requires a certain level of awareness, knowledge, and skills. Hence, the level of preparedness is a collective effort involving individuals, IT companies, and governments.

Preventive measures demonstrate existing capabilities to avert potential risks and vulnerabilities, as well as ability to apply those capabilities aimed at strengthening cyber and national security. Preventive measures should be applied on different levels. Individuals must cultivate a basic understanding of cybersecurity principles to protect personal information and recognize potential threats. This knowledge forms the foundation upon which broader societal resilience is built. Educational initiatives and public awareness campaigns can play a crucial role in this regard, equipping individuals with the tools they need to navigate the digital landscape safely.

IT companies, on the other hand, bear the responsibility of developing robust security measures and continuously updating their systems to counter emerging threats. These companies must prioritize the implementation of advanced cybersecurity protocols and technologies designed to mitigate identified risks. Regular security audits, vulnerability assessments, and penetration testing are essential practices that help organizations stay ahead of potential cyber adversaries.

Governments also play a critical role in fostering cyber resilience. By elaborating and enforcing comprehensive cybersecurity policies and regulations, governments can establish a secure digital environment for all citizens. This includes setting up national cyber response teams, promoting international collaboration to combat cybercrime, and supporting research and development in cybersecurity technologies.

To ensure the effectiveness of preventive measures, it is crucial to address existing, rather than imagined, threats. This realistic approach enables the development of targeted strategies that can effectively mitigate potential challenges. By collaborating and sharing information, individuals, IT companies, and governments can create a resilient cyber ecosystem capable of withstanding the ever-evolving landscape of cyber threats.

The level of societal cyber resilience depends not only on the ability to identify and mitigate risks but also on well-designed incident response plans, which are regularly updated and adapted to the constantly advancing technologies and changing cyber threats and risks. Analysing existing response plans allows for evaluating their efficiency and flexibility, ensuring they remain effective under various scenarios. Moreover, implementing these plans relies on robust coordination mechanisms and communication channels among stakeholders, including individuals, IT companies, and government agencies. This collaborative approach ensures that all parties can respond swiftly and effectively to cyber incidents, thereby enhancing overall cyber resilience.

Resilience presupposes the capacity to recover from experienced risks and threats and return to normalcy. In the context of cyber resilience, both human and technological components are involved. The IT sector must restore critical services that have suffered from the incident rapidly, working in close cooperation with governmental agencies to conduct thorough investigations. These investigations are crucial for understanding attack vectors,

learning from them, and enhancing future resilience. Meanwhile, society also learns from such incidents, using the experience to bolster its overall cyber resilience. When cyber incidents affect large groups within society or impact sectors of significant relevance to the wider public, it becomes imperative for the government to take action. This action often involves introducing new policy approaches designed to prevent similar incidents in the future and to protect public interest.

Such an example in Latvian history is the "Neo case," involving University of Latvia researcher Ilmārs Poikāns, also known as Neo. He was acquitted by the court for downloading data from the State Revenue Service's (SRS) Electronic Declaration System. Poikāns was charged with unauthorized acquisition of trade secrets and illegal activities with personal data after discovering a vulnerability in the SRS system in 2009, leading to the download of over seven million documents. He emphasized that his actions aimed at increasing transparency by publicizing public officials' salaries. Poikāns' actions have sparked debates on public transparency and data privacy, with legal consequences for such actions potentially including imprisonment, forced labour, or fines. Despite his arrest, Poikāns was honoured as a European person of the year in Latvia.

The broader implications of Poikāns' actions include promoting transparency in public sector salaries and increasing awareness of data protection. Moreover, the legal framework surrounding unauthorized acquisition and disclosure of trade secrets or personal data calls for a nuanced understanding of intent and public interest. Poikāns' actions, aimed at benefiting society without personal gain, exemplify the role of whistleblowers in exposing systemic flaws and promoting accountability. The case continues to spark debate about the balance between security, transparency, and the protection of individual rights within the legal and societal context (Gaile, 2014).

The debate sparked by the Neo case has indeed led to significant legislative changes in the areas it highlighted. The discussions and controversies surrounding the case brought attention to the gaps and vulnerabilities in the existing legal frameworks governing data security and the protection of personal information. Consequently, lawmakers were prompted to revisit and strengthen the legislation to ensure better protection of sensitive data and to address the responsibilities of both individuals and institutions in safeguarding this information.

Moreover, the case underscored the need for clearer guidelines and protections for whistleblowers, leading to legislative initiatives aimed at providing better support and legal safeguards for those who expose misconduct or systemic failures. These changes reflect a broader understanding of the importance of transparency and accountability in public administration, as well as the need to balance security concerns with the protection of individual rights. Thus, the Neo case has not only increased public awareness and sparked important debates but has also been a catalyst for legislative reforms that enhance data protection, support whistleblower activities, and promote a more transparent and accountable public sector.

Government measures might also include stricter regulations, improved cybersecurity standards, and increased funding for cybersecurity initiatives. By addressing both the immediate aftermath of a cyber incident and implementing long-term strategies, governments, IT sectors, and society as a whole can develop a robust and adaptive cyber resilience framework capable of withstanding future cyber threats.

Restoration leads to adaptation, requiring thorough analysis and lessons learned from previous incidents to convert these insights into effective policies. This adaptation process also involves continuously updating systems and processes to counter emerging threats. Such proactive measures ensure that both technological defences and human responses evolve in line with the dynamic cyber threat landscape. Connor and Davidson (2003) emphasize necessity of an individual to find mechanisms, which help to react to adversity by adjusting their reactions in order to reach initial task. All these activities must be communicated to society, enhancing public awareness and understanding. Transparent communication fosters trust and encourages collective responsibility in maintaining cybersecurity. By involving all stakeholders, including individuals, businesses, and government entities, in the adaptation process, societal cyber resilience is strengthened. This collective approach ensures that everyone is informed, prepared, and capable of contributing to a more secure digital environment, ultimately leading to a resilient society that can withstand and recover from cyber incidents more effectively. The aforementioned elements of cyber resilience – preparedness, restoration, response, and adaptation – are domains that must be addressed from policy, technology, and knowledge perspectives. However, the societal dimension is often overlooked or considered irrelevant in the context of cyber-attacks.

British scholars Joinson et al (Joinson et al., 2023) are bridging this gap by constructing a framework for developing a human cyber-resilience scale. They introduce parameters that aid in understanding individual and societal responses to cyber threats and risks, as well as potential individual reactions stemming from psychological characteristics. For instance, when addressing adaptation, the authors emphasize that building resilience requires positive adaptation. They argue (Joinson et al., 2023, p. 2), "It is likely that cyber-resilient individuals are those who are prepared to adapt positively to new and unexpected incidents. Cyber-resilient individuals should be able to learn from their mistakes and also accept that former behaviours and habits may have rendered them vulnerable to a cyber-attack". This perspective underlines the importance of adaptability from psychological perspective.

The human cyber-resilience scale is based on a range of characteristics examined through the lens of cybersecurity. For instance, mastery is linked to digital literacy, reflecting one's ability to navigate and utilize digital tools effectively. Self-efficacy relates to competence in the digital space, highlighting an individual's confidence in managing cyber-related tasks. Positivity plays a protective role, especially when confronting unfamiliar cybersecurity issues, by fostering a proactive and optimistic approach. Perseverance addresses stressors that require a more extended or sustained response and is integrated into several resilience models. Active coping involves resources that assist in managing stress, ensuring individuals can effectively respond to cyber threats. As authors underline (Joinson et al., 2023, p. 7): "there is a general trend of a negative correlation between overall human cyber resilience and the stress experienced following common cybersecurity victimization". Social support and connections pertain to strategies for coping with threats and risks through networks and communal resources. A structured environment encompasses protective mechanisms based on individual life strategies, where cyber hygiene practices are crucial. These components collectively contribute to a comprehensive understanding of human cyber resilience, emphasizing the importance of psychological and social factors in mitigating cyber threats. Authors (Joinson et al., 2023, pp. 2-3) underline that by integrating these characteristics into the cyber-resilience framework, individuals and organizations can better prepare for and adapt to the evolving cyber landscape, enhancing overall societal resilience.

So far, societal cybersecurity has been approached in this article from classical resilience, cyber resilience, and human perspectives. Each of these perspectives reveals specific characteristics derived from their respective sectors. At the same time, it is necessary to identify what functions as the "glue" that brings these perspectives into a coherent structure, delivering to both cyber and national security. There are at least three additional areas that should be included on the list of societal cyber security considerations: governance and policy, education and awareness, and collaboration and information sharing.

Effective governance structures and policies are foundational to cyber resilience. It was emphasized by Cavelty et al (2023) in their analysis stating that politics and policy making should be added to investigation of different aspects of cyber resilience. They (Cavelty et al., 2023, p. 805) correctly ask key questions which should be addressed to and by policy makers – "Who should cyber security be for? What kind of Cs do we want and need?". Governments are key players in establishing clear regulations, standards, and frameworks that promote cybersecurity best practices across all sectors. Public-private partnerships in this endeavour are essential for coordinating efforts and sharing information about threats and vulnerabilities. This collaboration ensures that both sectors are aligned in their defense strategies, can respond swiftly to emerging threats, and engaging society.

Continuous investment in cybersecurity research and innovation is also essential. This includes funding for the development of new technologies and support for academic and industry research initiatives. By prioritizing investment in cutting-edge cybersecurity solutions, governments can stay ahead of threat actors and protect national interests. Governments are also leading actors in promotion of international cooperation, as cyber threats do not respect national borders. Establishing global norms and frameworks can enhance collective security efforts.

Cyber resilience starts with an informed and vigilant populace. Education and awareness campaigns are thus the most powerful tools, helping individuals and organizations understand the risks and adopt safe online behaviours. There are several traditional tools used by governments, companies and individuals, such as regular training and awareness programs among citizens and employees; simple actions, like using strong passwords, enabling multi-factor authentication, being cautious of phishing attempts,

organizations conducting regular drills and simulations to prepare employees for potential cyber incidents; local initiatives to build awareness and preparedness at the community level and many others. However, these campaigns can have varying effects, including potential failures.

Effective education and awareness campaigns should acknowledge the specific characteristics of each target group, selecting adequate tools and experts, and analysing potential risks during the implementation process. According to a study by Eliana Stavro (Stavro 2022, p. 74), the human aspect of cybersecurity awareness efforts can serve as both an asset and a hindrance. She (Stavro 2022, p. 74) emphasizes the importance of awareness-raising experts who consider digital literacy adequately and ensure that selected messages reach the target audience. From the end users' perspective, there can be diverse attitudes that impede the success of these campaigns. These attitudes range from ignorance and lack of understanding to a preference for convenience over security. Additionally, there is often a mentality of complacency, where individuals believe that "nothing will happen to me". To overcome these challenges, it is crucial to tailor campaigns to the specific needs and mindsets of different groups, ensuring that the messages resonate and lead to meaningful changes in behaviour. Stavro (Stavro 2022, p. 75) indicates that the aim of the majority of campaigns is the introduction and strengthening of cyber resilience. This goal can be achieved by fostering societal acknowledgment of cyber situational awareness, encouraging the application of critical thinking, and promoting sustainable cyber hygiene behaviours. These elements are crucial because knowledge that translates into behaviour initiates and sustains a robust cyber culture. By integrating these principles, campaigns can effectively build a foundation of cyber resilience, ensuring that individuals are not only aware of cyber risks but are also equipped to take proactive steps to mitigate them, thereby enhancing overall digital security.

Cyber threats are global and borderless, necessitating international cooperation and information sharing. Governments, industries, international organizations and NGOs are main agents and knowledge hubs of different aspects of cyber security and cyber resilience. Collaborate among them on best practices and resources can lead to collective defence initiatives and in the end can enhance the overall resilience of the global digital ecosystem.

The "glue" that binds classical resilience, cyber resilience, and human perspectives into a coherent structure for delivering to societal cyber resilience includes effective governance and policy, robust education and awareness initiatives, and strong collaboration and information sharing mechanisms. In the next chapter the above-mentioned elements will be exemplified by Latvia's case leading to the assessment of societal cyber resilience in the country.

Societal cyber security in Latvia

The framework proposed in the previous subsection will be utilized to analyse the case of Latvia. This analysis will encompass several key categories: governance (including government, business, and NGOs), education and awareness, and international collaboration (focusing on entities such as the EU and NATO). These categories are crucial for understanding societal cyber resilience, which encompasses preparedness, risk assessment, response, recovery, and adaptation.

Specifically, societal cyber resilience through robust governance, comprehensive education, and active international collaboration significantly contributes to enhanced preparedness, accurate risk assessment, effective response, efficient recovery, and continual adaptation to cyber threats.

Based on this approach, the following categories will be examined in the case analysis:

1. **Governance and collaboration:** The roles and responsibilities of government bodies, businesses, and NGOs in promoting and maintaining societal cyber resilience. Latvia's cooperation with international organizations such as the EU and NATO to bolster societal cyber resilience.
2. **Risk Assessment, Awareness and Preparedness:** Processes for identifying and evaluating cyber risks by the society members. Measures taken to prepare society for potential cyber threats.
3. **Response, Adaption and Recovery:** Strategies and actions implemented to respond to cyber incidents at individual level. Societal efforts to recover from cyber incidents and restore normal operations. Ongoing societal adaptation to evolving cyber threats and vulnerabilities.

This comprehensive approach will provide a detailed analysis of Latvia's societal cyber resilience and highlight areas for improvement and best practices. It is important to emphasize that the focus is not on cybersecurity in general but specifically on societal cyber resilience. It means that this section will deal with community resilience and current resilience indicators, excluding governance mechanisms related to infrastructure creation, development, and operational continuity that pertain to cybersecurity but not directly to societal resilience. The study utilized snowball sampling to assess the current status and processes rather than legislative acts and strategic governmental documents. Additionally, personal conversations with stakeholders took place to gather comprehensive insights. This selection includes representatives from state institutions, civil society, state enterprises, and private companies. The diverse range of views ensures a comprehensive understanding of the different perspectives and roles in promoting and maintaining societal cyber resilience. Thus, the researchers had the opportunity to explore the ecosystem of various stakeholders in Latvia working on societal cyber resilience and examine their practices and attitudes. This perspective serves as a valuable lens through which to analyse and draw conclusions about the operations and roles stakeholders have in building societal cyber resilience, as well as about the knowledge and competences the society has in this regard. In third step quantitative socio-political analysis of cyber resilience will be provided based on descriptive statistics. It means that authors will summarize the basic features of the quantitative data about related societal measurements.

Governance and cooperation

Societal cyber resilience governance in Latvia is based on a multifaceted approach that integrates the efforts of governmental institutions, private sectors, and civil society. Consensus among stakeholders suggests that effective cyber resilience requires a collaborative effort across public, private, and NGO sectors, emphasizing the importance of continuous dialogue and cooperation. Ultimately, fostering a resilient digital society hinge on empowering individuals with the knowledge and tools to navigate and mitigate cyber threats, thereby strengthening the overall security posture of the nation. However, questions remain about whether the public perceives these

issues as equally important, whether the necessary actions have been taken to achieve the intended state of resilience, what cooperation mechanisms are in place, and which vulnerabilities require more attention.

The views on societal cyber resilience expressed by the main stakeholders are summarized in Table 1.

Table 1. **Stakeholders views on societal cyber resilience**

Companies/NGOs	Views on cyber resilience
Latvian Information and Communications Technology Association	In societal cybersecurity, one aspect is knowledge, referring to society's understanding and education regarding cyber-security. Another crucial aspect is critical thinking, which involves the ability to assess information logically and draw conclusions. In societal cyber resilience, individuals who possess the capacity to discern various threats, including SMS messages, emails, and fraudulent bank notifications, are crucial. This forms the foundation of societal resilience in cyberspace.
Women4Cyber	It is possible to divide society's cyber-resilience into two conditional levels: overall society's cyber-resilience (the ability of critical infrastructure of the state and private sector to ensure uninterrupted service during an attack/threat) and the individual ability of each member of society to cope with the threats and challenges that exist in everyday cyberspace
Localise	When an individual possesses the capability to recognize various forms of cyber-attacks, prevalent opportunities within the sphere, and subsequently respond appropriately
Tet	Cybersecurity is closely intertwined with physical security; they complement and reinforce each other. Resilience is built through a multi-dimensional approach that integrates various security aspects. It is crucial to consider both physical and cyber security together, as they collectively contribute to overall resilience. In cyberspace, resilience is defined by a society's ability to critically assess information and respond appropriately, akin to an immune system reacting to threats. This includes the capacity to recover from external malicious actions and threats, demonstrating the interconnectedness and importance of both physical and cyber security in maintaining societal resilience

RigaTechGirls	Societal cyber security is the capacity of society to autonomously detect and withstand cyber-attacks, as well as comprehend fundamental principles of cybersecurity without external assistance.
LMT	Societal cyber resilience is the ability of a society to operate reasonably successfully in an environment that provides both legitimate and safe resources in cyberspace, as well as those aimed at compromising the confidentiality, integrity, or availability of a cyberspace inhabitant. It should be noted that 'successful enough' is not the same as 'perfect,' so incidents are also possible. These must be dealt with appropriately to ensure that society's stability is maintained at the required level
Latvian State Radio and Television Centre	Societal cyber resilience of a society also contributes to the cyber resilience of the entire country. A country's cybersecurity is only as strong as its weakest link, such as a user or an individual who interacts with the system. I believe we can estimate the cyber resilience of society based on the most significant potential losses to our society. These could be data, finances, or identity. Therefore, these three indicators and risks should certainly be mitigated to enhance our society's resilience in cyberspace.

Source: views are collected by research assistant Elizabete Klēra Bože based on methodology elaborated by the authors of the article.

The Cybersecurity Strategy of Latvia 2023-2026 (CSL, 2003) outlines key areas of action including improved cybersecurity governance, enhanced resilience, and heightened public awareness and education. In the priority area of "enhancing cyber security and strengthening resilience," one key task is to provide the public with a foundational set of state-managed tools for secure electronic communication and to encourage their widespread adoption. The strategy (CSL, 2003) outlines that Latvia will provide citizens with digital equipment, including national electronic IDs and official electronic addresses, for secure communication with state institutions and access to digital services. It emphasizes the importance of citizens having access to and skills for using digital tools safely. The goal is to equip all residents with secure digital tools and skills through strengthened regulations, improved usability, expanded applications, and targeted digital skills development activities.

The second priority direction of action, titled "Societal Awareness, Education, and Research," also outlines the main tasks of state management regarding societal cyber resilience. Among the tasks outlined, in addition to training professionals and preparing educators, is the identification and implementation of specific measures, such as information campaigns, targeting certain societal groups – children and young people, seniors, and public administration employees. These measures aim to strengthen knowledge and understanding of cyber hygiene within these groups. The concept aims for residents to navigate their digital lives safely, using secure tools like eID cards and the e-Paraksts (auth.: E-Signature) mobile app. It targets children, youth, and adults to prevent cybercrime and digital fraud, emphasizing cyber hygiene as a cybersecurity cornerstone. According to the Strategy (CSL, 2003), these efforts will enhance public understanding of safe digital behaviour, including internet and digital service use, and provide in-depth cybersecurity education to specific groups, focusing on secure electronic identification and communication.

To achieve these goals, the Latvian government collaborates with various stakeholders. The National Cybersecurity Centre (NCSC), supported by "CERT.LV"[1] and the Constitutional Protection Bureau, plays a central role in managing cybersecurity incidents and coordinating national efforts. The cooperation network includes various state institutions, such as the Ministry of Culture and the Ministry of Environmental Protection and Regional Development, among others. This collaboration extends to public awareness campaigns and educational initiatives targeting children, youth, seniors, and public administration employees, aiming to enhance their understanding of cyber hygiene and critical thinking skills.

International cooperation is also a critical component of Latvia's cybersecurity governance. The country actively participates in global discussions and initiatives, such as the United Nations (Ministry of Foreign Affairs, 2024) thematic discussions on cybersecurity resilience, to share best practices and strengthen its cyber defence capabilities. This international engagement

[1] CERT.LV's mission is to enhance IT security in Latvia. Operating under the Ministry of Defense, CERT.LV is a part of the Institute of Mathematics and Informatics of the University of Latvia (LU MII), as defined by the IT Security Law. Its primary responsibilities include monitoring and updating information on IT security threats, supporting state institutions with IT security measures, assisting in the prevention of IT security incidents involving Latvian IP addresses or .LV domains, and organizing educational events for state employees, IT security professionals, and other stakeholders.

helps Latvia stay aligned with EU legislation and leverage global expertise to improve its national cybersecurity framework, as well as inhabitants of Latvia sees Latvia's expertise in cybersecurity as valuable knowledge to be shared for approbation on European level (Ministry of Foreign Affairs, 2021). Another example is ERT.LV, which has joined the global cybersecurity initiative STOP. THINK. CONNECT, which aims to help computer users recognize digital dangers and support safe internet usage habits. The initiative promotes awareness and encourages users to: STOP: Ensure that necessary safety precautions are followed; THINK: Understand the risks that may arise from online activities; CONNECT: Enjoy the virtual environment safely. Thus, the campaign underscores that internet security is a shared responsibility (CERT.LV).

Moreover, the involvement of non-governmental organisations (NGOs) and the private sector is crucial. There are some organisations, which actively engage and partner with the government, while other focus on serving society without building this type of partnerships. For example, Latvian Information and Communications Technology Association collaborates with CERT.LV and the Ministry of Defense, emphasizing the importance of these partnerships. The organisation representing the non-governmental sector, actively participates in the expanded council of the Ministry of Defence, where current issues of cybersecurity and related legislation are discussed. The association also collaborates with several universities and educational institutions that train cybersecurity specialists. Close cooperation with educational institutions aims to create a professional qualification framework to train competent cybersecurity specialists in Latvia.

While the organization RigaTechGirls significantly contributes to societal development, it does not currently form partnerships with the government. This NGO (RigaTechGirls) is the "first community in Latvia aimed at educating and inspiring women & girls about all things digital". It organizes hackathons, supports the development of startups for women, and runs educational and mentorship programs. Additionally, it provides community support and other digital skills-related activities. Over 28,000 participants have engaged in the organization's online programs, with 2,000 women enhancing their skills through professional IT training. Additionally, more than 600 individuals have taken part in various hackathons and the development of these start-ups (RigaTechGirls).

RigaTechGirls acknowledges that while the organisation does not conduct formal analysis on cybersecurity and societal cyber resilience, they stay updated on current affairs and trends to adapt their training programs accordingly. When developing these programs, they consider not only the latest developments in cybersecurity but also relevant public concerns that affect their participants. Among organisation's cooperation mechanisms, it occasionally collaborates with Women4Cyber Latvia, a community that originated from the RigaTechGirls. This is the primary partnership they currently maintain.

Youth organisations are active as well. For example, UN Youth Delegation Latvia in cooperation with the Ministry of Foreign Affairs of the Republic Latvia in August 2022 organised the Baltic Youth Forum (Ministry of Foreign Affairs, 2022), which focused on strengthening societal resilience by engaging young people security, including cyber security, discussions and initiatives.

Overall, Latvia's approach to societal cyber resilience governance is comprehensive, involving extensive cooperation between governmental institutions, international bodies, private sectors, and civil society. This collaborative effort aims to create a secure and resilient digital environment for all citizens. It is evident that the government often prefers to delegate the development of educational and informational campaigns to non-state actors. Meanwhile, some non-governmental organisations work on enhancing societal cyber resilience independently, without active collaboration with administrative institutions. In turn, the private sector's involvement in these efforts largely depends on the company's activity profile, management's vision of social responsibility, and the company's interests and priorities.

Risk assessment, awareness and preparedness

It is challenging to precisely measure the population's readiness for crises, such as cyber threats. However, various studies can provide insights by examining individuals' digital skills, anxiety levels, sense of security, and other relevant indicators. The population's understanding of potential threats and the actions needed to mitigate them is one of the most visible indicators. This includes threat perception, knowledge of potential threats, e.g., ability to recognize them and knowledge of emergency procedures,

awareness of risks. By deeply understanding the population's subjective perception of security (Ozoliņa et al., 2021, p.21), policymakers can better align public views of threats with those defined in national policies. This alignment helps develop security and defence strategies that reflect the synergy between professional responses and public concerns. Such synergy is crucial for changing civilian attitudes and behaviours, enhancing the population's ability to protect themselves.

The previous qualitative research on perception of cyber threats in 2019 demonstrates that Latvians are generally aware of cybersecurity challenges, their primary concern is personal internet security, particularly regarding personal data, bank information, and individual savings. In 2019, conspiracy theories about 5G impact on their lives also worried some residents. Despite recognizing these issues, proactive measures to strengthen personal online safety were lacking across all age groups. By 2021, public opinions shifted towards concerns about the government's handling of the COVID-19 pandemic, highlighting a gap between public perceptions of security threats and national policy priorities (Ozoliņa&Struberga, 2023), which emphasize the importance of cybersecurity and civil society's role in national defence efforts.

According to the Eurobarometer (Eurobarometer, 2021) in 2021, 64% of Latvians feel informed (13% very well informed and 51% fairly well informed) about the risks of cybercrime, compared to the European average of 71%. And respondents who consider themselves to be well informed about cybercrime are less concerned about cybercrime than those who do not feel informed. According to a survey (TvNet, 2024) conducted by the Baltic Computer Academy in November 2023, 28% of Latvian residents feel they are partially educated in cybersecurity but recognize the need for updated knowledge. This sentiment is most expressed by those over 50 and individuals aged 30 to 39. According to the survey, 12% of respondents in Latvia lack knowledge on how to protect themselves online but are eager to learn, 8% are unsure of their knowledge level, and 3% find such information uninteresting. Those rating their knowledge as insufficient typically include individuals with primary and secondary education, unskilled workers, residents earning below 550 euros per month, and senior citizens over 60 (TvNet, 2024).

According to recent Eurobarometer data (Eurobarometer, 2024), 61% of Latvians believe that they are getting basic and advanced digital education, training and skills well, what is close to average in Europe. Meanwhile,

perception of getting access to safe and privacy-friendly digital technologies is more critical than average in Europe. According to Eurobarometer, 50% of Latvians access this as well, while in Europe average is 55%. The same goes to assessment of getting control of one's own data, i.e., how it is used online and with whom it is shared. 44% of Latvians evaluate it positively, while average positive assessment in Europe is 47%. Here share of Latvian inhabitants not having opinion is high. 18% have responded that they do not know, while average "not knowing" answer in Europe is 9%.

Another survey (Labs of Latvia, 2022) revealed a positive trend: people are becoming more aware of the importance of antivirus programs. In 2021, 75% of the population reported installing antivirus software on their devices within the past two years, up from 55% in 2019. While it's encouraging that only 13% do not use any security solution, these 13% still represent individuals exposed to cyber-attacks. This indicates a need for focused initiatives to enhance public confidence in digital security measures and data control practices.

This self-assessment highlights a mixed picture of societal cyber resilience in Latvia, suggesting that while digital skills education is perceived positively, there are substantial gaps in the perception of digital safety and data privacy. While Latvians are making progress in digital skills education, there are still considerable gaps in their perception and implementation of cybersecurity measures. These findings underscore the importance of continuous public awareness campaigns and educational programs to build a more resilient digital society.

Regular public awareness campaigns and educational programs are essential in fostering a culture of cybersecurity vigilance. By promoting best practices and up-to-date information, both the public and private sectors can contribute significantly to enhancing societal cyber resilience. Despite this, the statistics on companies' policies do not present an encouraging picture for private sector cybersecurity and the development of employees' societal cyber resilience.

According to a survey conducted by Luminor bank (Luminor bank, 2024), 20% of Latvian small and medium-sized companies do not view cybersecurity as a priority for investment. Latvian companies recognize the importance of cybersecurity, with 80% of small and medium-sized enterprises implementing at least basic measures, and 42% taking additional steps

to enhance their cybersecurity practices. A survey of entrepreneurs revealed that 38% of Latvian small and medium-sized companies allocate minimal financial resources to cybersecurity, primarily investing in basic tools like antivirus systems or firewalls to protect their networks from intruders. 42% of Latvian small and medium-sized companies prioritize cybersecurity, with 14% developing detailed security strategies, regularly reviewing their systems, and training employees. Additionally, 15% continuously invest in new or upgraded systems, and 13% opt for secure, certified IT service providers to protect their businesses from cyber-attacks.

The Eurobarometer (Eurobarometer, 2021), which focused on conducting data from manager responsible for IT, or if not available, someone with decision-making responsibilities, indicates that only 14% of Latvian companies consider cybersecurity a very high priority in their workplaces, compared to the European average of 32%. Additionally, 37% of Latvians view cybersecurity as a fairly high priority (compared to 39% in Europe), while 39% perceive it as a fairly low or low priority in their workplaces (26% average in Europe). This suggests that while there is a general consensus in Europe that cybersecurity is a high priority among companies (71%), the perception among Latvian employees is less positive, with only 51% considering it a high priority.

The main challenge still remains acting. Although the situation is gradually improving, progress remains very slow. In 2021, only 14% of small and medium-sized companies in Latvia reported providing employees with training or awareness programs about the risks of cybercrime in the past year, compared to the European average of 19% (Eurobarometer, 2021). in the past 12 months, only 24% of European companies and 20% of Latvian companies have provided employees with any training or awareness-raising about cybersecurity. 85 % of Latvian companies' representatives believe that no training of employees was needed.[2] This highlights a significant gap in proactive cybersecurity measures in both Europe and Latvia. At the same time, 69 % of Latvians also recognize that there are no aspects of their cyber security handled by individuals or companies outside their own company (Eurobarometer, 2024).

[2] In addition, 6 % stands that the cost of training was a reason why they did not provide any training or awareness raising about cyber security for company's employees. 2 % thought that there is no relevant training, while 7 % stated that they do not know about relevance of training.

The private sector's performance in supporting societal cyber resilience building appears inadequate. Despite recognizing the importance of continuous training and awareness, there is a noticeable lack of prioritization and proactive measures among companies. The statistics indicate that many companies do not see the need for employee training, leading to insufficient preparedness against cyber threats. This gap between awareness and action suggests that the private sector needs to enhance its efforts in fostering a culture of cybersecurity and resilience, ensuring that both employees and the broader community are better equipped to handle cyber risks. This shortfall highlights the necessity for a more integrated approach, combining policy initiatives, corporate responsibility, and public awareness campaigns to build a more resilient cyber environment.

To enhance societal awareness and preparedness in Latvia, the state needs to continue and extend implementation of several comprehensive measures. Public awareness campaigns utilizing various media channels should be launched to educate citizens about common cyber threats and safe online practices. Integrating cybersecurity education into school curricula and organizing regular workshops and seminars for different population segments, including vulnerable groups such as seniors, is essential. More extensive collaborations with private companies, NGOs, and community organisations can develop and deliver effective cybersecurity training and awareness programs, ensuring information reaches all parts of society.

Robust cybersecurity standards for businesses must be enacted and enforced to ensure the secure handling of personal data. Establishing more extended hotlines and support services for reporting cyber incidents and maintaining incident response teams will enhance the country's resilience. While CERT.LV operates effectively, increasing its activities could help prevent cyber threats and attacks that many Latvian companies and individuals may be unaware of. Expanding their efforts could provide better protection and awareness against potential unseen risks.

Investing in research and development to advance cybersecurity technologies and conducting regular surveys to monitor the state of cybersecurity awareness will help identify gaps and areas for improvement, enabling more effective government initiatives. By implementing these measures, Latvia can foster a more resilient digital environment for all citizens, contributing to national security and individual safety.

Response, adaption and recovery

Response, adaptation, and recovery are vital components of societal cyber resilience. Immediate and effective response to cyber incidents minimizes damage and prevents the spread of threats by implementing predefined protocols and trained personnel. Adaptation involves learning from past incidents and updating strategies and technologies to counter evolving threats, maintaining a proactive defence stance. Recovery ensures that normal operations are quickly restored, including technical systems and public trust, while also analysing incidents to prevent future occurrences. Together, these elements enable societies to withstand, manage, and learn from cyber threats, thereby enhancing overall resilience.

Successful response, adoption and recovery of new behaviours or technologies is influenced by several psychological and cognitive factors. These include perceived usefulness and ease of use, where individuals are more likely to adopt something if they believe it will benefit them and is easy to use. Self-efficacy, or the belief in one's ability to succeed, also plays a critical role. Positive attitudes, shaped by prior experiences and cultural norms, and social influence from peers and society can significantly impact adoption. Motivation, both intrinsic and extrinsic, can drive individuals towards response, recovery and fast adoption, as can the perception of risks associated with non-adoption. Access to information and understanding of the new behaviour or technology reduce uncertainty and build confidence. Simplified processes and clear instructions lower cognitive load, making fast recovery and adoption more likely. Lastly, trust in the information source and the reliability of the technology or behaviour is crucial for adoption. This ongoing adaptability ensures that both individuals and organizations can maintain robust cybersecurity measures in a constantly changing digital landscape.

Currently, Latvian residents exhibit an elevated level of anxiety. According to the study (Struberga, 2024) respondents feel most threatened by economic difficulties (41%) and least by climate change-related threats (43%). Additionally, 22% of Latvians believe their security threat level is very high or significantly high, while another 34% consider it to be moderate. Latvian residents are experiencing increased stress levels due to the economic situation in the country and the ongoing war in Ukraine. Elevated

anxiety levels negatively impact ability of people to respond, recover fast and to adopt to new environments by impairing decision-making, reducing adherence to security practices, and decreasing participation in training and education. Anxiety also lowers trust and cooperation, which are crucial for effective cybersecurity efforts, and makes individuals more vulnerable to social engineering attacks. These factors collectively weaken the ability of society to respond to and recover from cyber threats, thereby compromising overall cyber resilience.

Latvia's societal response, recovery and adaptation to new circumstances and collaboration with other social institutions is hindered by the population's critical attitude towards government performance. For instance, only 29% of Latvian residents believe the government makes the right decisions during crisis situations, including the ongoing war in Ukraine (Struberga, 2024). This scepticism impacts the quality and effectiveness of collective adaptation efforts.

Low levels of mutual trust among residents and trust in state institutions. In Latvia, trust in public media is low, with only 42% of respondents trusting news from Latvian public media and 37% expressing distrust. The lack of mutual trust among residents is also a concerning factor. Nearly half (47%) of respondents believe that most people cannot be trusted. More than half of respondents trust the President of Latvia (57%) and the Latvian police (55%). Conversely, a majority of those surveyed do not trust the Latvian Parliament (70%) and the Latvian government (66%). Only 38% of respondents are willing to cooperate with the Latvian government (Struberga, 2024). In such circumstances, it is difficult to envision successful resilience-building without changing public sentiments.

At the same time, according to the Eurobarometer (Eurobarometer, 2024), 78% of Latvians believe that the digitalization of daily public and private services makes their lives easier, which is 3% higher than the European average/ 18% sees this process as the leading to more difficult life (5 % lower than the European average). 83 % of inhabitants see an improved cybersecurity, better protection of online data and safety of digital technologies and more education and training to develop skills for using digital services as steps that would facilitate their daily use of digital technologies. This demonstrates that despite the challenges, Latvian society is generally open to changes in cyberspace and shows interest in opportunities to build

individual resilience. However, there is a lack of understanding regarding personal and collective responsibility in enhancing cybersecurity. A significant portion of the population lacks strong motivation to invest in strengthening individual cyber resilience.

Overall, while Latvian society shows readiness for digital transformation, enhancing cyber resilience will require improving public sentiment, increasing trust in institutions, and fostering a deeper understanding of cybersecurity responsibilities.

Conclusion

The research literature on societal cyber resilience underscores the importance of a holistic, multi-layered approach that encompasses technical, organizational, and human factors. These factors require further elaboration to fully grasp their interdependencies and impacts. The stakes of societal cyber security are extraordinarily high, with the potential for cyber threats to disrupt essential services, undermine public trust, and cause significant economic and social harm.

A comprehensive approach to cyber resilience necessitates not only technological innovation but also robust regulatory frameworks, strong public-private partnerships, extensive education, and meticulous resilience planning. These components are crucial to safeguarding society from evolving threats. By fostering a collaborative and proactive cyber security culture, we can better protect the digital foundations of our modern world.

Building cyber resilience requires a concerted effort across sectors and disciplines, continuous learning and adaptation, and a proactive stance towards emerging threats. Embracing these principles enables societies to better withstand cyber disruptions and maintain critical functions in the face of cyber adversities. Ultimately, the adoption of a cyber-resilient culture (World Economic Forum, 2024) ensures not only reactive recovery but also proactive adaptation.

Societal cyber resilience is not just a technical challenge; it is a comprehensive endeavor that demands the collective efforts of governments, businesses, and individuals. By understanding the importance of cyber resilience, investing in key components, and taking proactive steps, societies can build a secure and resilient digital future. As we continue to embrace the

benefits of digital technologies, ensuring cyber resilience will be paramount in safeguarding our way of life.

Latvia's case study demonstrates the necessity of an integrated approach to cyber resilience. The collaborative efforts between government institutions, private sector entities, and non-governmental organisations are vital in promoting cybersecurity awareness and education, which in turn foster a culture of proactive defence and resilience. Despite the general openness of Latvian society to digital transformation, challenges such as low trust in government and mutual trust among residents, high anxiety levels, and a lack of understanding regarding individual and collective cybersecurity responsibilities remain significant barriers.

To address these challenges, continuous public awareness campaigns and educational programs are essential. They help build a more informed and vigilant populace capable of recognising and responding to cyber threats. The importance of these efforts is highlighted by the gaps identified in the perception and implementation of cybersecurity measures among Latvian residents. For instance, while many are aware of the risks, proactive measures to strengthen personal online safety are still lacking.

The private sector's involvement in fostering societal cyber resilience is also critical. However, the current performance indicates a need for improvement, particularly in prioritizing cybersecurity training and awareness programs for employees. This gap between awareness and action suggests that more robust efforts are required from companies to build a culture of cybersecurity and resilience.

Latvia's approach to societal cyber resilience governance is comprehensive, involving cooperation between various stakeholders. This includes national efforts and international collaborations, such as those within the European Union and with organizations like NATO. These partnerships enhance Latvia's ability to respond to and recover from cyber threats, leveraging global expertise and resources.

What are the challenges which are topical and will stay there as future challenges for Latvia and other countries? One of the primary issues is the limited financial and human resources available for implementing comprehensive cyber resilience strategies. These constraints can hinder the development and deployment of advanced cybersecurity measures and training programs, which are essential for building resilience. Ensuring adequate

budget allocation for cybersecurity amidst competing national priorities is also challenging, potentially affecting the scope and effectiveness of resilience initiatives.

Another significant challenge is the rapidly changing cyber threat landscape. Cyber threats are continually evolving, often outpacing defensive measures. The rapid development of new attack vectors, such as sophisticated phishing schemes, ransomware, and state-sponsored cyber-attacks, requires constant vigilance and adaptation. Technological advancements also provide cybercriminals with new methods and tools, demanding ongoing research, innovation, and adaptation in cybersecurity practices.

Effective coordination among diverse stakeholders is another complex challenge. Cyber resilience necessitates seamless collaboration among various government agencies, each with its mandates and operational procedures. This complexity can make interagency coordination difficult to manage. Additionally, public-private partnerships are crucial but aligning the interests and efforts of these diverse entities can be challenging. Private companies may have different priorities and levels of commitment to cybersecurity compared to governmental bodies. Engaging with international partners, such as the European Union and NATO, is also vital for enhancing cyber resilience, but differences in regulatory environments, threat perceptions, and resource capabilities can complicate these collaborative efforts.

Building societal cyber resilience in Latvia, as in other countries, is not just a technical challenge but a comprehensive endeavour that demands collective efforts across all sectors of society. By addressing the outlined challenges, investing in key components of cyber resilience, fostering a collaborative cybersecurity culture, and ensuring continuous adaptation to emerging threats, Latvia can enhance its cyber resilience, safeguarding its digital future and ensuring the security and well-being of its citizens. The path forward involves not only leveraging existing strengths but also strategically addressing the limitations and obstacles that lie ahead. This comprehensive approach will ensure that Latvia remains resilient in the face of an ever-evolving cyber threat landscape.

The Role of Individuals in Strengthening Cybersecurity

Elizabete Klēra Bože
Associate researcher, the Latvian Political Science Association

The objective of this article is to examine the current state of cybersecurity in Latvia, with a specific focus on public awareness and the influence of the human factor in the management of cyber risks. While technical infrastructure and institutional frameworks remain critical components of cybersecurity, the most prevalent vulnerabilities are frequently attributed to the insufficient preparedness and limited understanding of cyber hygiene among individual users. The analysis highlights that the accelerated pace of Latvia's digital transformation, coupled with the complexities of the geopolitical environment, has contributed to an escalation in cyber threats. However, the prevailing level of public awareness remains inadequate. Consequently, enhancing public education and fostering a pervasive cybersecurity culture are imperative, as comprehensive and inclusive awareness initiatives are essential to strengthening the resilience and overall efficacy of the nation's cybersecurity posture.

Key words: cybersecurity, resilience, individuals, cyber threats

Raksta mērķis ir analizēt kiberdrošības stāvokli Latvijā, īpašu uzmanību pievēršot sabiedrības izpratnei un cilvēkfaktora nozīmei kiberrisku pārvaldībā. Neskatoties uz tehniskās infrastruktūras un institucionālo sistēmu nozīmīgumu, būtiskākās neaizsargātības visbiežāk rodas no indivīdu nepietiekamas sagatavotības un izpratnes par kiberhigēnu. Analīze atklāj, ka Latvijas digitālās transformācijas straujums un ģeopolitiskās situācijas sarežģījumi palielina kiberdraudu risku skaitu, taču sabiedrības izpratnes un informētības līmenis joprojām nav pietiekami augsts. Būtiska loma ir cilvēku izglītošanai un kiberdrošības kultūras veicināšanai – plaša un iekļaujoša sabiedrības informēšana var veicināt valsts kiberdrošības noturību un efektivitāti.

Atslēgvārdi: kiberdrošība, noturība, indivīdi, kiberdraudi

Introduction

While significant emphasis has traditionally been placed on ensuring high levels of cybersecurity within institutions and large organizations, comparatively less attention has been directed toward the critical role individuals play in maintaining and enhancing overall cybersecurity resilience. This trend is also evident in Latvia, where the primary responsibility for meeting national cybersecurity expectations – aligned with broader European cyber resilience standarts – is largely placed on organizations, while the role of individual users remains underemphasized. Cybersecurity remains a broadly used yet inconsistently defined term, and the absence of a clear, widely accepted definition limits progress by reinforcing a primarily technical perspective and hindering the interdisciplinary collaboration essential for addressing its complex, multifaceted challenges.[1] To define cybersecurity by breaking it down, one might begin with the term 'security', commonly understood as "the condition of being protected from danger or threat".[2] The word 'cyber' doesn't clearly specify what individuals are being protected from – it simply indicates that the threat or activity is occurring in the digital or virtual realm.[3] Following this line of reasoning, cybersecurity can be defined as a state in which cyber threats are absent. In reality, the digital world has become deeply integrated into the daily lives of society. Individuals don't just share photos and videos – they also, often carelessly, hand over personal information and critically sensitive data. As a spokesperson for an IT organization once put it, "cybersecurity is only as strong as its weakest link".[4] The role of individuals is far more important than it is often acknowledged.

The primary goal of this paper is to explore the state of cybersecurity in Latvia, with a particular focus on public awareness and the human factor in cyber risk. While technical infrastructure and institutional frameworks are crucial, this analysis argues that the most significant vulnerabilities often lie with individual users whose lack of awareness and preparedness

[1] Craigen, D., Diakun-Thibault, N., Purse, R. *Defining Cybersecurity*. (2023). Technology Innovation Management Review. Available: https://www.timreview.ca/article/835

[2] Bay, M. (2016). *What Is Cybersecurity? In search of an encompassing definition for the post-Snowden era.* French Journal For Media Research – n° 6/2016 – ISSN 2264-4733

[3] Ibid.

[4] Bože, E.K. (2024). Kiberdrošības kompetenču kopiena kā ES rīcībpolitikas instruments. Latvijas Universitāte.

can undermine even the most robust cybersecurity systems. To achieve this goal, the paper sets out to explore several key tasks:

1. Examine why cybersecurity is an urgent and growing concern in Latvia, particularly in the context of rapid digitalisation and increasing geopolitical tensions.
2. Assess the current state of cybersecurity culture and public awareness in Latvian society, highlighting individual users as a key point of vulnerability.
3. Identify existing gaps and offer reflections on how Latvia is strenghening and could strengthen its cybersecurity through a more human-centered and education-focused approach.

Cybersecurity Today

The importance of cybersecurity is growing rapidly as society becomes increasingly dependent on technology. With digital identities and everyday lives deeply intertwined with integrated technologies, people are more exposed to cyber threats than ever.[5] The European Union is taking several measures to strengthen cybersecurity. For instance, directives like NIS2 require organizations to enhance their security practices, and agencies such as ENISA, ECCC, and others play key roles in this effort. However, much of the focus is placed on organizations, while the responsibility to understand the unique needs of society and individuals within each member state is largely entrusted to national institutions. This allows each country to find the most effective way to address cybersecurity challenges in its specific context. To understand the situation of individuals affected by cyberthreats, it is essential to examine data and statistics. In January 2020, a special Eurobarometer survey was released with the aim of assessing EU citizens' awareness, experiences, and perceptions regarding cybersecurity.[6] A survey this specific, focused on individuals and citizens, has not been conducted since. 52% of respondents in 2020 considered themselves fairly or very well

[5] Allurity (n.d.). Cybersecurity Today. Available: https://allurity.com/cybersecurity-today/

[6] Wahl, T. (2020). Eurobarometer: Europeans Attitudes towards Cyber Security. Available: https://eucrim.eu/news/eurobarometer-europeans-attitudes-towards-cyber-security/

informed about cybercrime, an increase from 46% in 2017.[7] Confidence in personal protection against such crimes had declined, with only 59% of Europeans feeling adequately protected – down from 71% in 2017.[8] The most recent survey of this kind was conducted in May 2024, focusing on cyber skills. Unlike earlier surveys centered on individuals (in 2017 and 2020), this one emphasized institutions and organizations – specifically, how much of a priority they place on cybersecurity and what prevents them from training their employees. This approach may suggest a shift in perception, with greater responsibility now being placed on organizations to ensure their employees are equipped with the necessary skills, rather than focusing primarily on individual citizens. The results showed that although 71% of companies in the survey agree that cybersecurity is a high priority, taking concrete action remains a significant challenge.[9] A striking 74% have not offered any training or awareness-raising activities for their employees.[10] Furthermore, 68% of companies believe such training is unnecessary, 16% are unaware of available training opportunities, and 8% cite budget limitations as a barrier.[11] It is evident that the importance of individuals possessing fundamental cybersecurity knowledge is not sufficiently emphasized and deserves further research on all levels. The ways in which individuals are most frequently targeted on a daily basis should not only be monitored and addressed, but also clearly communicated to the public in an understandable and accessible manner.

In Latvia, this task falls to CERT.LV – an organization responsible for monitoring and updating information on IT security threats. Its main responsibilities include supporting state institutions in matters of cybersecurity, assisting individuals and organizations in resolving IT security incidents involving Latvian IP addresses or .LV domains, and organizing educational events for public sector employees, IT security professionals, and other interested audiences.[12] As of April 2025, data from CERT.LV highlights the main

[7] European Union. (2020). Europeans' attitudes towards cyber security (cybercrime). Available: https://europa.eu/eurobarometer/surveys/detail/2249

[8] Ibid.

[9] European Union (2024). Cyberskills. Available: https://europa.eu/eurobarometer/surveys/detail/3176

[10] Ibid.

[11] Ibid.

[12] CERT.LV (2025). Par mums. Available: https://cert.lv/lv/par-mums

point of this article: the majority of cyberattacks target individuals. These are mostly everyday incidents that affect regular IT users or cause only minor damage to organizations and institutions.[13] To better understand the scope of cyberthreats, CERT.LV categorizes incidents into six levels:

C1	National-level threats that impact the provision of essential services and pose risks to public administration, as well as economic or political stability
C2	High-stakes threats targeting public institutions or national IT infrastructure
C3	Significant threats with a broad impact on the commercial sector, as well as state and local government institutions
C4	Significant threats with a moderate impact on businesses and public sector institutions
C5	Moderate threats causing minor disruptions to the commercial sector and public institutions
C6	Everyday threats that primarily affect individual users of IT services and have minimal or no impact on companies or government bodies.[14]

The categorization is also further detailed based on two additional dimensions: the breakdown of hazards by impact and the severity breakdown of victims. Breakdown of hazards by impact (from 1 to 5, with 1 being the lowest impact):

Lowest impact (1)	Activities such as vulnerability scanning, information gathering, and the spread of harmful content
Low impact (2)	Incidents including phishing, fraud, targeted information collection, attempted intrusions, loss of insignificant data, and configuration weaknesses
Medium impact (3)	Malware infections, compromised devices, and temporary system disruptions or service unavailability
High impact (4)	Extraction, corruption, or deletion of confidential or sensitive data, and targeted attacks
Highest impact (5)	Long-term disruptions to essential services and related systems.[15]

[13] CERT.LV (2025). Pieejama statistika par 2025. gada aprīli. Available: https://cert.lv/lv/2025/05/pieejama-statistika-par-2025-gada-aprili

[14] CERT.LV (2025). Pieejama statistika par 2025. gada aprīli.

[15] Ibid.

Severity breakdown of victims (from 1 to 6, based on the type and importance of the affected party):

Level 1	Individual IT service users
Level 2	Small businesses, individual entrepreneurs
Level 3	Medium-sized enterprises, schools, libraries, public organizations, and sectors of the public administration
Level 4	Significant threats with a moderate impact on businesses and public sector institutions
Level 5	Regional governments, municipal capital companies, ISPs, hosting providers, academic and research institutions, political parties, media, and large enterprises along with their supply chains
Level 6	critical infrastructure or basic national services affected, or a large number of service users impacted.[16]

As of the previously mentioned April 2025, category C6 under the first mentioned category – which includes individual users of IT services – accounted for 186 incidents, making up 73.23% of all reported cases.[17] Although this category is not considered the most critical, it provides a gateway for hackers and cybercriminals to exploit weaknesses in human behavior and Latvian society. By targeting these vulnerable points, they could gradually work their way toward larger, more impactful attacks – gaining access to companies, institutions, or even families, especially if their ultimate goal is to drain a specific bank account. For comparison, other categories were reported significantly less frequently. C5 – moderate threats with minor impact on the commercial sector and public institutions – accounted for 35 cases, or 13.78%, C4, representing significant threats with a medium-level impact, was recorded 20 times (7.87%), while C3, indicating significant threats with widespread consequences, was documented 13 times (5.2%).[18] Notably, no incidents were reported in the most severe categories, C2 and C1.[19] Thus, the more individualized the threat, the more frequently it occurs and proves effective.

[16] CERT.LV (2025). Pieejama statistika par 2025. gada aprīli.
[17] Ibid.
[18] Ibid.
[19] Ibid.

The causes of rising cyberthreats and cyberattacks

Cybersecurity issues and attacks are continuously increasing in this era of rapid digitalisation. The surge in remote work after the COVID-19 pandemic caused a notable rise in the frequency and severity of cyberattacks as well, making this issue even more urgent as time goes on.[20] The geopolitical situation for the European Union, particularly concerning neighboring border countries facing aggression, further amplifies the importance of this issue. Despite companies investing heavily in technical safeguards and security tools, the human element remains the most vulnerable point in the defense chain.[21] Practices like leaving work computers unlocked or leaving files and documents on public computers significantly weaken workplace security. Therefore, it is crucial for organizations and institutions to closely monitor and promote responsible behavior among all employees regarding these safety measures. It's not that people do not want to follow safety standards; rather, they often lack knowledge of these principles. Additionally, they may not realize that the data they have access to is important and can cause damage if compromised. For example, even if the lowest-ranking employee leaves their computer unlocked, it creates an easy pathway for attackers to access sensitive information such as finances, passwords, and other critical data that could cause harm. It is essential for managers to increase employee awareness of potential cyber threats and provide education on the various defense strategies they can implement.[22] While large organizations and institutions, especially those closely connected to IT, generally pay sufficient attention to these issues, it is the individuals in smaller organizations that need greater education on the topic, as they often lack the knowledge or resources to effectively address them. It has been concluded that educating users about e-commerce threats and training them in proper security practices can lead to positive behavioral changes, ultimately improving online security for both the individuals and the organizations

[20] Klein, G., & Zwilling, M. (2023). *The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home*. Journal of Computer Information Systems, 64(3), 408–422. Available: https://doi.org/10.1080/08874417.2023.2221200

[21] Ibid.

[22] Ibid.

they work for.[23] People are more likely to pay attention to certain measures when they understand why they are necessary, even more so if they recognize the personal impact those measures can have on them.

Tactics of cyberattackers and fraudsters

Risks and attacks do not always originate from work computers or major platforms. It is essential to stay informed about and adapt to the latest tactics employed by cyber attackers and fraudsters in order to ensure the safety of individuals across all levels of society. Cyber attackers operate through various methods, and in the case of Latvia, these approaches differ depending on whether the target is an individual, an entire institution, or the objective is to commit fraud.

Against individuals in Latvia, as of April 2025, malicious activities have been carried out not only through emails and text messages but also via QR codes.[24] These QR codes can be found anywhere, whether it's on a streetlamp or on a ticket for public transportation routes. While most of these attempts were detected and avoided in time, there have been cases where fraudsters succeeded in their schemes. Residents have reported ads on Facebook leading to fake websites that imitate popular online stores like Etsy and Shein, enticing users with large discounts and promises of free products.[25] Fake investment and crypto-investment scams using counterfeit Delfi.lv websites are particularly common.[26] Disturbingly, double-extortion tactics have emerged, where victims who lost money on fake platforms were then contacted by supposed "lawyers" offering to recover their losses, only for victims to end up losing even more money.[27] Fraud attempts have also been made impersonating the Maintenance Guarantee Fund's Administration, sending false text messages about initiating debt recovery procedures.[28] Another new

[23] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). *Influence of Awareness and Training on Cyber Security*. Journal of Internet Commerce, 9(1), 23–41. Available: https://doi.org/10.1080/15332861.2010.487415

[24] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Available: https://cert.lv/lv/2025/05/kiberlaikapstakli-2025-aprilis#Krapsana

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid.

tactic involves fraudsters posing as State Social Insurance Agency employees, warning residents about allegedly freezing their second-tier pension capital, often including malicious links in these messages.[29] Since the start of the year, fraudulent campaigns have been ongoing, peaking in April with scammers impersonating employees of the State Revenue Service (SRS).[30] Phishing attacks have also increased, targeting well-known organizations such as Facebook, Microsoft, Swedbank, Latvijas Pasts, CSDD, and others. Data from the State Police reveal that during the first quarter of 2025, Latvia recorded 1,260 fraud cases, resulting in total losses exceeding 3.9 million euros for residents.[31] This represents an increase of over 17% in the number of fraud cases compared to the previous year.[32] As observed, many of these attacks are carried out through personal messages, making individuals more emotionally vulnerable. From a psychological perspective, when fear and strong emotions are involved, people are more likely to believe false information and often do not even think to verify it or contact official sources. This has led to an increase in highly personalized attacks, indicating that cybercriminals have found a way to exploit individual traits and behaviors within society.

When it came to fraud against organizations, CERT.LV observed a number of instances in which fraudsters tried to deliver malicious acts in phishing emails to businesses and institutions, both large and small. Fraudsters pretend to be law firms known in Latvia, claiming they represent the national television of Latvia (LTV).[33] They notify e-mail recipients of alleged copyright infringements, inviting them to consult the Annex for more information. Ironically, these PDF documents actually contain malware for data theft purposes. Fraudsters say works belonging to LTV, such as songs, sound recordings or videos, were illegally uploaded without permission, with detailed "evidence" supposedly found in attached PDF or ZIP format files,

[29] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Available: https://cert.lv/lv/2025/05/kiberlaikapstakli-2025-aprilis#Krapsana

[30] Ibid.

[31] Ibid.

[32] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Krāpšana. Available: https://cert.lv/lv/2025/05/kiberlaikapstakli-2025-aprilis#Krapsana

[33] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Ļaunatūra un Ievainojamības. Available: https://cert.lv/lv/2025/05/kiberlaikapstakli-2025-aprilis#LaunaturaUnIevainojamibas

prompting recipients to open them.[34] In a number of cases, careless users have opened these malicious attachments, leading to malicious activation in their computer systems. In both situations described, cybercriminals use social engineering techniques, manipulating the emotions of recipients, creating a sense of haste and fear.[35] Ominous phrases are used, such as: "Please comply with the above requests and inform us of the results within 7 days of receiving this letter, failure to comply may lead to strict legal action".[36] By doing so, fraudsters hope to get the victim to recklessly open the attachments for fear of consequences. There are also various tactics used to access an organization's finances, for example, identifying the name of the director or financial officer and sending emails requesting financial data or access while pretending to be them. It is crucial to carefully check the sender's email address and ensure it is the official one before responding or sharing any information. Situations like these highlight an essential point: knowledge and clear procedures for handling such incidents are crucial for all employees, not just IT specialists or those in senior positions. It is a common misconception that only high-level staff need this awareness, when in reality, everyone plays a role in cybersecurity. For example, if a cleaning staff member virtually shares the door code to an organization, it could provide a physical entry point for a cyberattacker to commit fraud or access sensitive documents and information.

When examining these threats and tactics side by side, the primary distinction lies in the scale of potential damage. Financial impact varies, as does the number of individuals whose safety may be compromised by a single error or successful attack. What consistently stands out is that individuals remain the most vulnerable element – even within well-established companies and large organizations. It is often the human factor, including emotional responses, that enables these attacks to succeed. However, this vulnerability can be mitigated through knowledge. This reinforces the argument that cybersecurity awareness and education must become a standard for all individuals – regardless of age, profession, or role. Only through widespread, inclusive knowledge can a truly secure cyberspace be achieved.

[34] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Ļaunatūra un Ievainojamības. Available: https://cert.lv/lv/2025/05/kiberlaikapstakli-2025-aprilis#LaunaturaUnIevainojamibas

[35] Ibid.

[36] Ibid.

Public awareness and behavior

As noted by authors Hans de Bruijn and Marijn Janssen, there are several key points to consider when evaluating public awareness of cybersecurity and its significance. First, cybersecurity is a matter of public concern that currently receives inadequate attention.[37] People often perceive cybersecurity as something distant and irrelevant to their daily lives. There is also a common belief that the data they possess is not valuable or interesting enough to attract the attention of hackers or cybercriminals. Second, it is inherently complex, intangible, and difficult for many to fully understand or conceptualize.[38] Cybersecurity often feels difficult to grasp and understand. It's usually discussed using complex, technical IT language and legal directives. However, for an individual, ensuring a higher level of security begins with simple but essential steps, such as never leaving a computer unlocked and making sure all connections are secure. It is also crucial to prevent unauthorized access to personal accounts, work devices, banking apps, and other sensitive platforms. As highlighted in other research, while nearly everyone has heard of cybersecurity, people's actions and sense of urgency often do not reflect a strong level of awareness.[39] The internet is still frequently perceived as a safe space for sharing information, conducting transactions, and even managing aspects of the physical world.[40] In reality, this is not the case and there are a lot of signs to be aware of.

Cybersecurity awareness can be defined as the extent to which individuals recognize, understand, and are informed about various aspects of cybersecurity or information security.[41] This includes not only an awareness of cyber risks and threats but also knowledge of the proper protective measures to mitigate them.[42] Although organizations in Latvia are considered

[37] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Ļaunatūra un Ievainojamības.

[38] CERT.LV (2025). Kiberlaikapstākļi 2025 | APRĪLIS. Ļaunatūra un Ievainojamības.

[39] Bruijn, H., Janssen, M. (2017). *Building Cybersecurity Awareness: The need for evidence-based framing strategies.* Government Information Quarterly. Volume 34, Issue 1, January 2017, Pages 1-7. Available: https://doi.org/10.1016/j.giq.2017.02.007

[40] Ibid.

[41] Taherdoost, H. (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. Procedia Computer Science 235 (2024) 1649–1663

[42] R.C.Nurse,J.(2021).*CybersecurityAwareness.*EncyclopediaofCryptography,SecurityandPrivacy. Available: https://link.springer.com/referenceworkentry/10.1007/978-3-642-27739-9_1596-1

the strongest in the Baltics in terms of cybersecurity,[43] there is still a noticeable rise and high number of cyberattacks targeting individual users. Information and communication technologies (ICTs) now form the backbone of modern society. They fuel innovation, power industries, and play a growing role in how governments operate and how people interact – both professionally and publicly. However, as these technologies become more deeply embedded in everyday life, the risks and threats targeting them have also grown significantly.[44] What might seem like harmless or routine information to share can quickly turn into a serious risk. Even something as simple as losing access to your email, whether it's the individuals work or personal account, can have significant consequences. This represents a portion of the knowledge that should be communicated to individuals in a clear and accessible way, and meaningfully integrated into their daily lives.

Best practices in Latvia

While we do not live in a utopian world where every member of society can be reached, efforts must be directed toward engaging as many individuals as possible. Latvia demonstrates exemplary cybersecurity practices that serve as valuable references. A prominent institution in this regard is CERT.LV, whose data was used in this study. CERT.LV was founded as a unit within the Institute of Mathematics and Informatics at the University of Latvia and functions under the auspices of the Ministry of Defence, operating within the legal framework established by the National Cybersecurity Law and it's primary mandate is to strenghten the nation's cybersecurity.[45] CERT.LV not only assists organizations and institutions in identifying and neutralizing cyberattacks but also plays a crucial role in educating the public by communicating information in clear and accessible language. This approach is essential to ensure that individuals are not discouraged or intimidated by overly complex technical terminology.

[43] Labs of Latvia. (2024). Latvijas uzņēmumi – apzinīgākie kiberdrošībā Baltijā. Available: https://labsoflatvia.com/aktuali/latvijas-uznemumi-apzinigakie-kiberdrosiba-baltija

[44] R. C. Nurse, J. (2021). *Cybersecurity Awareness*. Encyclopedia of Cryptography, Security and Privacy.

[45] Aizsardzības ministrija (n.d.) Kiberdrošība. Available: https://www.mod.gov.lv/lv/kiberdrosiba

Other noteworthy organizations to consider when discussing the emphasis on individuals and their skills in the cybersecurity field are "Riga TechGirls" and "Women4Cyber Latvia." Riga TechGirls is a community-driven organization that empowers and inspires individuals to engage with technology and build their expertise.[46] Riga TechGirls offers a range of opportunities, including courses, training camps, and mentorship programs – from foundational skills to advanced real-world challenges – catering to individuals of all ages. By enhancing digital skills, it promotes greater equality and inclusion both in Latvia and beyond. Women4Cyber is dedicated specifically to cybersecurity, with the primary goal of building a robust cyber community and encouraging greater participation in the cybersecurity field.[47] Women4Cyber produces various blogs and publications addressing current cybersecurity issues and emphasizing the importance of details. They offer numerous free online and in-person events featuring industry professionals. Many of these sessions are conducted in an informal setting, encouraging participants to engage comfortably and expand their knowledge.

Numerous initiatives and organizations host events tailored for individuals of all ages. The growing recognition of the importance of providing education and essential knowledge from a young age highlights the significance of TET's social initiative for children. This initiative is particularly valuable because when even one family member, including a child, understands basic safety principles, the likelihood of that knowledge spreading throughout the entire family increases significantly. The social initiative, titled "Ričijs Rū un internets," features a beloved bear character popular among children in Latvia.[48] Through songs and cartoons, it delivers important knowledge in a charismatic and easily accessible manner. This digital school also provides resources for parents and teachers to support them in educating children about the importance of internet safety and helping the younger generation become more cybersecurity-aware than previous ones.[49] Such initiatives and communities, though not always widely recognized or acknowledged, play a vital role in educating individuals by making information easily accessible and easy to understand.

[46] Riga TechGirls. (n.d.) About us. Available: https://rigatechgirls.com/about-us/

[47] Women4Cyber Latvia. (n.d.) Kas mēs esam? Available: https://w4clatvia.lv/

[48] Tet. (n.d.) Sociālā iniciatīva. Ričijs Rū un internets. Available: https://digitaladrosiba.lv/sakumlapa.html

[49] Ibid.

Building cybersecurity resilience

One might question the emphasis placed on organizations throughout this paper, given that its primary objective is to address individual users. However, this focus reflects the broader strategic approach adopted by the European Union and its institutions, which aim to reach individuals through their interactions with organizations, institutions, and workplaces. This method is both logical and effective, as it offers the most efficient and opportunity-rich pathway to engage individuals on a large scale. Additionally, the frequent reference to organizations stems from a notable limitation within the cybersecurity landscape in the EU: there is a significant lack of individual-level data. Most existing research and initiatives are directed toward organizations, institutions, and businesses – whether targeting internal stakeholders such as employees or external audiences like consumers, media audiences, and others. For instance, the 2024 ENISA report highlights the importance of promoting a unified strategy by leveraging existing policy initiatives and aligning national efforts. The goal is to ensure a consistent and high level of cybersecurity awareness and cyber hygiene among both professionals and citizens, regardless of demographic differences.[50] Even this recommendation underscores the absence of a clear division between professionals and citizens, as the relationship often functions in both directions. Many individual – referred to as citizens in this context – are simultaneously members of organizations, institutions, or various communities, whether as employees, consumers, or media audiences. These affiliations often represent the most effective, and at times the only, channels through which individuals can be reached. Nevertheless, what remains concerning is the uneven distribution and accessibility of cybersecurity knowledge across different levels and types of individuals.

There are many ways to address this across all levels, whether in large or small organizations, workplaces, or for individuals. When it comes to individuals within organizations or institutions, it's essential to normalize and emphasize that 1) regular cybersecurity awareness training should be a

[50] ENISA (2024). 2024 Report on the State of the Cybersecurity in the Union. Available: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

standard practice, no matter the size or sector of the organization.[51] This should involve comprehensive annual training sessions, complemented by short, practical refreshers delivered regularly throughout the year to keep awareness high and knowledge up to date.[52] This is crucial because the cybersecurity landscape in the digital world is constantly evolving and represents one of the fastest-growing sectors and industries. Its significance is only expected to increase in the future. 2) Institutions should implement clear, straightforward procedures for reporting suspicious activity and responding to potential threats,[53] such as notifying colleagues about a suspicious message or attempted scam. Sharing this information helps raise awareness and reduces the likelihood of someone else falling victim to the same threat. 3) It is equally important to promote a no-blame culture within the organization.[54] This means avoiding negative reactions when an employee makes a mistake and instead focusing on collaboration to address the issue, by reporting it promptly and taking the necessary steps to mitigate any risks. This approach is essential for maintaining transparency and ensuring that threats and attacks can be more easily tracked and addressed. If an employee feels ashamed or afraid to speak up, they may choose not to report the issue or fail to grasp the full extent of the threat, potentially leading to far more serious consequences. There are also effective ways to test employees, such as using positive phishing simulations, where the emphasis is on analyzing the mistakes and providing constructive feedback, rather than punishing the individual.[55] This approach can be applied across all age groups, starting in schools and continuing throughout professional life.

When it comes to individuals and their personal lives, there are also important steps to take – such as participating in cybersecurity education, building stronger digital habits, and verifying the information they receive.

[51] KeepNetLabs (2024). How Often Should Employees Receive Cyber Security Awareness Training? Available: https://keepnetlabs.com/blog/how-often-should-employees-receive-cyber-security-awareness-training

[52] Ibid.

[53] Global Anti-Scam Alliance (2025). Strategies to Combat Online Scams: A Comprehensive Approach. Available: https://www.gasa.org/post/strategies-to-combat-online-scams-a-comprehensive-approach

[54] Secure Schools (2024). Positive Phishing: Building a culture of cybersecurity in schools. Available: https://www.secureschools.com/en-au/blog/positive-phishing-building-a-culture-of-cybersecurity-in-schools

[55] Secure Schools (2024). Positive Phishing: Building a culture of cybersecurity in schools.

It's important to stress once more that cyberattacks are employed to steal data, monitor users, disable or manipulate computer systems, and more.[56] These attacks do not just target individual personal computers but can also affect entire networks and can be executed by lone hackers, hacker groups, or even nation-states.[57] It is important to recognize that not all cyberattacks come in familiar forms that can simply be learned and memorized. Vigilance must be maintained at all times and individuals should stay updated on the latest cybersecurity news and take advantage of the free resources available. The European Union places strong emphasis on cybersecurity through initiatives and legislative measures such as the NIS2 Directive, the EU Cybersecurity Strategy, and the EU Cybersecurity Act as these efforts aim to create a resilient and secure digital environment for everyone.[58] Additionally, ENISA offers valuable resources and guidance to help individuals protect themselves online, and opportunities for self-education in cybersecurity continue to expand.[59] As the volume of information and the number of sources continue to increase, it becomes essential to adopt specific strategies to maintain individuals' interest and focus.

Conclusions

Cybersecurity is no longer a concern limited to large organizations or governmental institutions – it is a critical issue that affects every individual in today's highly digital and interconnected world. The data from Latvia's CERT.LV clearly illustrates that the majority of cyberattacks target everyday users rather than major institutions. These individual-level threats, while often perceived as less severe, serve as the primary entry points for cybercriminals to exploit vulnerabilities, which can then escalate into larger, more damaging attacks. This reality highlights the urgent need to expand cybersecurity efforts beyond the organizational and institutional levels to include individuals as active participants in maintaining cyber resilience. Despite

[56] European Commission (n.d.) Cybersecurity. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity

[57] Ibid.

[58] European Commission. (n.d.) Cybersecurity Policies. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[59] Ibid.

widespread recognition of cybersecurity's importance, public awareness and understanding remain limited. Many individuals underestimate their personal risk or believe that their information holds little value to attackers. Compounding this is the complexity and technical nature of cybersecurity language, which can alienate those without specialized knowledge. This disconnect creates gaps in security that cybercriminals readily exploit through increasingly sophisticated and psychologically targeted tactics, such as phishing, scams, and social engineering attacks that prey on emotions like fear and urgency.

Efforts by Latvian institutions like CERT.LV, as well as community-driven organizations such as Riga TechGirls and Women4Cyber Latvia, provide positive examples of how to engage and empower individuals with knowledge and skills. Initiatives like the "Ričijs Rū un internets" social campaign further demonstrate the importance of starting cybersecurity education early, making it accessible and relatable for children and their families. These initiatives contribute to building a culture of cybersecurity awareness that spans all age groups and societal sectors. However, there remains a significant gap in consistently integrating individual-focused cybersecurity education and awareness into national strategies. Organizations often emphasize technical defenses but overlook the human element, which is frequently the weakest link. Cybersecurity resilience requires a comprehensive approach that includes regular training, clear communication, no-blame cultures within organizations, and accessible education for individuals at all levels.

Latvia's experience underlines that strengthening national cybersecurity is not solely about protecting infrastructure or institutions – it is about empowering every user to act knowledgeably and responsibly online. To truly enhance cyber resilience, greater attention must be paid to the role of individuals. Only by elevating individual awareness and capabilities can the broader cybersecurity ecosystem become stronger, more adaptive, and truly effective against evolving digital threats.

Recognizing and Protecting Informal Caregivers: Comparative Legal Frameworks in Europe

Rachid Al Bitar
PhD Candidate, University of Debrecen,
Géza Marton Doctoral School of Legal Studies

This article examines the comparative legal frameworks protecting informal caregivers in Europe, with case studies on Germany, Sweden, and France. As populations age and chronic care needs rise, informal caregivers, often unpaid family members, have become critical to sustaining home-based care. Yet they frequently lack clear legal recognition, labor protections, or social security coverage, creating a fragmented and unjust policy landscape. The article reviews European Union initiatives, including the Work-Life Balance Directive and the European Care Strategy, and analyzes their impact on national legal systems. It then explores national innovations such as Germany's pension credits for family carers, Sweden's municipal support obligations under the Social Services Act, and France's recent move to paid caregiver leave via the Allocation Journalière du Proche Aidant (AJPA). It also highlights persistent challenges: inadequate financial support, poor intergovernmental coordination, migrant caregiver vulnerabilities, and fragmented service provision. Best practices from emerging reforms including flexible caregiver leave, respite entitlements, and the integration of informal carers in care teams are identified as promising avenues to build a more cohesive framework. The authors conclude by advocating for a unified, rights-based approach to support informal caregivers across Europe, stressing that legal innovation and stronger enforcement mechanisms are essential to prevent burnout, social exclusion, and long-term economic disadvantages for millions of carers.

Keywords: Informal caregivers, comparative analysis, long-term care, social protection, better care, intergovernmental coordination

Šajā rakstā veikta salīdzinošā analīze tiesiskajiem regulējumiem, kas aizsargā neoficiālos aprūpētājus Eiropā, veicot gadījumu izpēti par Vāciju, Zviedriju un Franciju. Pieaugot iedzīvotāju vecumam un hroniskās aprūpes vajadzībām, neformālie aprūpētāji, bieži vien neapmaksāti ģimenes locekļi, ir kļuvuši kritiski svarīgi, lai uzturētu aprūpi mājās. Tomēr tiem bieži vien trūkst skaidras juridiskās atzīšanas, darba aizsardzības vai sociālā nodrošinājuma seguma, radot sadrumstalotu un netaisnīgu politikas ainavu. Rakstā apskatītas Eiropas Savienības iniciatīvas, tostarp Direktīva par darba un privātās dzīves līdzsvaru un Eiropas aprūpes stratēģija, kā arī analizēta to ietekme uz valstu tiesību sistēmām. Aplūkoti tādi valstu jauninājumi kā Vācijas pensiju kredīti ģimenes aprūpētājiem, Zviedrijas pašvaldību atbalsta pienākumi saskaņā ar sociālo pakalpojumu likumu un Francijas nesen ieviestais apmaksātais aprūpētāja atvaļinājums. Tajā arī uzsvērtas pastāvīgas problēmas: neatbilstošs finansiālais atbalsts, slikta starpvaldību koordinācija, migrantu aprūpētāju neaizsargātība un sadrumstalota pakalpojumu sniegšana. Jauno reformu paraugprakse, tostarp elastīgs aprūpētāju atvaļinājums, tiesības uz atpūru un neformālo aprūpētāju integrācija aprūpes grupās, ir iespēja veidot vienotāku sistēmu. Nepieciešams iestāties par vienotu, uz tiesībām balstītu pieeju, lai atbalstītu neformālos aprūpētājus visā Eiropā, uzsverot, ka juridiskās inovācijas un stingrāki izpildes mehānismi ir būtiski, lai novērstu izdegšanu, sociālo atstumtību un ilgtermiņa ekonomiskos trūkumus miljoniem aprūpētāju.

Atslēgvārdi: Neformālie aprūpētāji, salīdzinošā analīze, ilgtermiņa aprūpe, sociālā aizsardzība, labāka aprūpe, starpvaldību koordinācija

Introduction

Home health care, including care provided by informal, unpaid family members, has become a crucial component of aging societies' support systems. As populations age and chronic care needs rise, millions of Europeans and others globally rely on informal caregivers who are typically family or friends, to provide daily assistance.

Legal and policy mechanisms have struggled to keep pace, often leaving informal caregivers without clear status, rights, or support. The result is a patchwork of laws and gaps. In many countries, caregivers receive little recognition or protection, increasing their risk of burnout, poverty, and ill health. This article examines and compares three national legal frameworks

on home care and informal caregiving across Europe. It focuses on how different jurisdictions recognize informal caregivers and what rights/protections they afford.

Best practices, recent reforms, and legal innovations are highlighted, alongside persistent legal gaps, regulatory fragmentation, migrant caregiver vulnerabilities, and intergovernmental coordination challenges. The discussion draws on relevant case law, EU directives, and scholarly doctrine to support a legal analysis. The conclusion offers a policy argument for strengthening the legal status of informal caregivers through more cohesive and rights-based frameworks.

Methods

In this article we carry out a qualitative comparative legal analysis to examine how European legal frameworks recognize and protect informal caregivers. The research is based on a doctrinal legal method, systematically analyzing relevant statutes, case law, and policy documents across three carefully selected jurisdictions: Germany, Sweden, and France. The selection of countries is related to diverse welfare state traditions and policy models each of them has adopted: Germany's conservative-corporatist social insurance, Sweden's social-democratic universalism, and France's familial solidarity approach. In addition to the comparative analysis between the three jurisdictions, the study situates its analysis within the broader context of European Union law and international human rights frameworks.

Sources were collected from legal databases (EUR-Lex, national legislation repositories), academic journals, government reports, and COST Action BETTERCARE and COST Action IGCOORD network resources. The analysis was carried under a critical legal perspective to identify normative gaps, implementation challenges, and best practices.

Finally, this methodology benefits from triangulation through policy documents, secondary literature, and national reports to verify consistency and interpretive accuracy. This approach ensures robust comparative insight into how legal norms shape the recognition, support, and rights of informal caregivers in Europe, while also allows to identify innovative reforms and still existing gaps in their safeguarding.

European Union framework and initiatives

At the European Union level, competence over long-term care and social support largely lies with Member States, resulting in diverse national approaches. There is *no single EU directive specifically on informal caregiving* or long-term home care. However, the EU has begun to address caregivers' rights indirectly through employment law and soft-law strategies. A cornerstone is Directive (EU) 2019/1158 on Work-Life Balance for Parents and Carers[1], which required all Member States by 2022 to provide at least *5 working days of carers' leave per year* for workers to care for ill or dependent relatives, as well as the right to request flexible working arrangements. This directive marked the first EU-wide statutory leave specifically for caregivers. Another key influence is EU anti-discrimination law: while EU equality directives do not list "caregiver" status as a protected ground, the Court of Justice of the EU in the landmark *Coleman v. Attridge Law* case[2] (2008) interpreted the Equal Treatment Directive (2000/78/EC)[3] to prohibit *"discrimination by association*" – meaning an employee cannot be treated unfairly due to their association with a disabled person under their care. The *Coleman* ruling effectively extended workplace discrimination protections to family carers of persons with disabilities, a principle now reflected in many countries' laws.

Beyond binding law, the EU has promoted coordination on long-term care through initiatives like the European Care Strategy (2022)[4] and a new Council Recommendation on Access to Affordable Long-Term Care

[1] European Union. (2019). Directive (EU) 2019/1158 of the European Parliament and of the Council of 20 June 2019 on work-life balance for parents and carers and repealing Council Directive 2010/18/EU. Official Journal of the European Union, L 188, 79–93. https://eur-lex.europa.eu/eli/dir/2019/1158/oj

[2] Court of Justice of the European Union. (2008). Coleman v. Attridge Law and Steve Law, Case C-303/06, ECLI:EU:C:2008:415. Judgment of 17 July 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CJ0303

[3] European Union. (2000). Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation. Official Journal of the European Communities, L 303, 16–22. https://eur-lex.europa.eu/eli/dir/2000/78/oj

[4] European Commission. (2022). European Care Strategy: COM(2022) 440 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0440

(2022)[5]. These instruments call on states to improve support for informal carers – for example by providing training, respite services, and financial assistance – and to ensure care responsibilities do not result in social exclusion or gender inequality. The European Commission's 2021 Long-Term Care Report[6] and related policy documents highlight that high reliance on informal care (over 80% of all care hours in some countries) is unsustainable without better support structures. Indeed, the EU recognizes that inadequate support for carers exacerbates gender disparities, since a majority of carers are women, and undermines labor market participation.

However, EU measures remain mostly soft-law or minimum standards, and enforcement is left to national implementation. The result is significant divergence across Europe in caregivers' legal rights – a challenge for EU social cohesion and mobility.

There is also emerging influence of international human rights law: notably, the UN *Committee on the Rights of Persons with Disabilities (CRPD)* in Bellini v. Italy (2022)[7] found that lack of support for a family caregiver can violate the rights of the person with disabilities by extension. The Committee noted that while carers themselves are not explicitly granted rights under the CRPD, *"the rights of persons with disabilities cannot be realised without the protection of family caregivers"*, and thus states have an obligation to provide such protection as part of ensuring an adequate standard of living for disabled persons. This interpretation signals an evolving international doctrine linking carers' rights to human rights of dependent persons, putting moral pressure on governments to fill legal gaps.

[5] Council of the European Union. (2022). Council Recommendation of 8 December 2022 on access to affordable high-quality long-term care (2022/C 476/01), ST/13948/2022/INIT. Official Journal of the European Union, C 476, 1–16. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022H1229%2801%29

[6] European Commission: Directorate-General for Employment, Social Affairs and Inclusion. (2021). Long-term care report : trends, challenges and opportunities in an ageing society. Volume II, Country profiles. Publications Office. https://data.europa.eu/doi/10.2767/183997.

[7] United Nations Committee on the Rights of Persons with Disabilities. (2022). Bellini v. Italy, Communication No. 41/2017, CRPD/C/27/D/41/2017.

National legal frameworks

European countries vary widely in how they legally recognize and support informal caregivers. Only a few EU Member States have enacted comprehensive national laws specifically addressing informal carers' status and rights (e.g. Germany, Sweden, Austria, Belgium), while others rely on scattered provisions or regional legislation[8].

This section examines three illustrative European jurisdictions Germany, Sweden, and France which represent different welfare models and legal approaches to home care.

Germany offers one of the most developed legal frameworks for long-term care and explicitly integrates informal family caregivers into its social insurance system. Since 1995, Germany's mandatory Long-Term Care Insurance (*Pflegeversicherung*) has recognized family caregivers as vital care providers and provides direct support to them. Notably, if an insured person opts to be cared for at home by relatives, they can receive a cash allowance (*Pflegegeld*) to help compensate the family carer, or professional services can be partly substituted by informal care[9].

Crucially, the law treats substantial caregiving as pensionable work: the long-term care insurance funds pay contributions towards the informal caregiver's state pension and accident insurance, provided the caregiver invests significant time (generally >10–14 hours/week) in care[10]. This means German caregivers earn retirement credits for caregiving periods (analogous to an income of average wage for pension calculations)[11], a recognition aimed at preventing poverty in old age due to years spent out of formal employment. Furthermore, Germany statutorily protects caregiving employees through family caregiver leave legislation. Under the Care Leave

[8] Santini, S. (2025). Intergenerational Informal Caregiving in an Ageing European Society. In: Teti, A., Neuderth, S., Pavlova, M.K., Ziese, G. (eds) Soziale und gesundheitliche Ungleichheit im Alter. Vechtaer Beiträge zur Gerontologie. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-48005-9_5

[9] Ibid.

[10] Jensen, S. E. H., Pinkus, D., & Ruer, N. (2025, January 23). *Prepare now: Europe must get ready for the coming long-term care surge. In many countries, demand for long-term care services outpaces supply, leading to a 'care gap'*. Bruegel Policy Brief. https://www.bruegel.org

[11] Bund, E. S., & Towers, J. (2011). International paid leave for personal or family health problems: The United States is far behind. Social Security Bulletin, 71(4), 61–71. https://www.ssa.gov/policy/docs/ssb/v71n4/v71n4p61.html

Act (*Pflegezeitgesetz*) and Family Care Leave Act, workers in medium-large companies may take up to 6 months of unpaid leave to care for a dependent relative at home[12]. They are also entitled to a shorter emergency leave of up to 10 working days with income replacement, a "*care support allowance*" if they need time off suddenly to organize urgent care. Since 2015, an additional option allows up to 24 months of reduced working hours, with partial wage, while caregiving, supported by government loans to mitigate income loss. In sum, German law provides a relatively robust package: job-protected leave, pension credits, training courses for family carers, respite care services paid by insurance (replacement professional care so caregivers can take a break), and even inclusion of family carers in care planning. In 2023, Germany expanded respite care benefits by increasing their duration and flexibility[13].

Overall, Germany's legal model stands out for formally acknowledging informal caregivers as part of the care systemand providing them social security, leave entitlements, and financial support. The German approach – a universal insurance scheme that includes caregiver benefits – is often cited as a best practice in balancing formal and family care[14]. Yet it also illustrates the need for vigilance that labor standards and caregivers' own rights (especially for migrants or non-family aides) are protected amid growing demand.

Sweden represents a contrasting paradigm: a Nordic social-democratic model historically premised on extensive formal state-provided care and an expectation that the public sector, rather than family, shoulders primary responsibility for eldercare. As such, Sweden lacked explicit legal recognition of "informal carers" for many years – supporting relatives was seen as a natural part of the welfare state's remit, and family caregiving was somewhat de-emphasized. However, as the population ages and pressures on formal services grow, Sweden has increasingly acknowledged the role of informal carers and introduced measures to support them. A significant development

[12] Jensen, S. E. H., Pinkus, D., & Ruer, N. (2025, January 23). Prepare now: Europe must get ready for the coming long-term care surge. In many countries, demand for long-term care services outpaces supply, leading to a 'care gap'. Bruegel Policy Brief. https://www.bruegel.org

[13] Ibid.

[14] Santini, S. (2025). Intergenerational Informal Caregiving in an Ageing European Society. In: Teti, A., Neuderth, S., Pavlova, M.K., Ziese, G. (eds) Soziale und gesundheitliche Ungleichheit im Alter. Vechtaer Beiträge zur Gerontologie. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-48005-9_5

was a 2009 amendment to the Social Services Act[15], which for the first time mandated that municipalities *"shall offer support to relatives who provide regular care"* for an older or disabled person. This change, while modest, is viewed as a "*break from the traditional Swedish model*" by formally recognizing caregivers' needs in law.

In employment law, Sweden has provisions to accommodate workers with caregiving duties, though these have been recognized relatively recently. Under the National Insurance Act, an employee can receive paid temporary leave (Närståendepenning) when caring for a seriously ill relative, with compensation from the state similar to sick leave. This benefit can be considerable (up to 100 days per ill person, paid at ~80% of income) and is often used for end-of-life care. However, outside such critical cases, Sweden historically lacked a general carers' leave entitlement. The issue of work-care reconciliation gained political attention only in the 2010s when studies showed tens of thousands of Swedes reducing work hours or quitting jobs to care for aging parents[16] [17][18]. Today, while there is no blanket "*carer's leave*" for non-critical caregiving, Swedish employees have strong rights to request flexible working or reduced hours (under the Working Hours Adjustment Act) and cannot be unfairly dismissed for caregiving, aligning with EU norms.

Sweden's approach illustrates both strengths and gaps. On one hand, by providing generous public home care services (covered under universal Social Services law), it reduces the burden on families and promotes gender equality in care. Indeed, Sweden reports a relatively high share of older persons receiving formal home care, and family carers often cite *indirect support* – ensuring their loved one has quality professional care – as their most

[15] Socialtjänstlagen (2001:453) [Social Services Act]. (Sweden). Retrieved from https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/socialtjanstlag-2001453_sfs-2001-453

[16] Szebehely, M., Ulmanen, P., & Sand, A. B. (2014). Att ge omsorg mitt i livet: Hur påverkar det arbete och försörjning? Stockholm: Stockholm University, Department of Social Work.

[17] Schön, P., & Johansson, S. (2016). European social policy and family caregiving. European Journal of Social Work, 19(5), 758–773. https://doi.org/10.1080/13691457.2015.1084274

[18] National Board of Health and Welfare. (2012). *Support for informal caregivers: Situation, needs and interventions* [in Swedish: Stöd till anhöriga – lägesbeskrivning 2012]. Stockholm: Socialstyrelsen.

important need[19]. On the other hand, informal carers in Sweden have been called *"invisible welfare providers"*, as the law still does not define who is a "carer" and support policies remain an "*add-on*" rather than integrated into labor, pension, or social security legislation[20]. Recent years have seen Sweden adopt its *first national carer strategy* (2022)[21] to coordinate efforts, and increase funding to NGOs that support carers. In summary, Sweden legally mandates that *"no one should have to care alone"* – the state is a partner in care – but it is still grappling with how to systematically support those family members who do provide significant care.

France has traditionally maintained a family-oriented social model with a mix of state and family solidarity in caregiving. In French law, informal caregivers known as *"proches aidants"*, have progressively gained recognition over the past decade through targeted legislation. A notable reform came with the Law on Adapting Society to Aging (2015)[22] and subsequent measures, which explicitly acknowledged the rights of *aidants*. France introduced a statutory caregiver leave, "*Congé de proche aidant*" in 2017, giving employees the right to take time off to care for a dependent relative. The leave can last up to 3 months, renewable, with a lifetime maximum of one year per worker. Initially this leave was unpaid. However, effective October 1, 2020, France added a government-funded caregiver allowance to compensate such

[19] Stratmann, B., Grafström, M., & Olsson, L.-E. (2021). *Ageing in Sweden: Regional perspectives on policy and practice.* Nordic Welfare Centre. https://nordicwelfare.org/en/publikationer/ageing-in-sweden-regional-perspectives-on-policy-and-practice/

[20] The 2009 legislation (the amendment to the Social Services Act regarding support to informal carers) points towards a break from the traditional Swedish model and a revision of the existing social contract. But it is still an add-on policy, not integrated with other policies, such as pension and employment legislation. When announcing the 2009 amendment though, the government website used the phrase "legal rights to support for carers". This gave an image, that the amendment was an entitlement to support. But the amendment gives carers the right to an assessment of their needs, no more no less.

[21] Government Offices of Sweden. (2022). *Nationell anhörigstrategi inom hälso– och sjukvård och omsorg* [National carers strategy in health and social care]. Ministry of Health and Social Affairs. https://www.regeringen.se/498267/contentassets/29579d4400834b759d3c78faf438dece/nationell-anhorigstrategi-inom-halso–och-sjukvard-och-omsorg.pdf

[22] République Française. (2015). Loi n° 2015-1776 du 28 décembre 2015 relative à l›adaptation de la société au vieillissement [Law no. 2015-1776 of 28 December 2015 on adapting society to aging]. Journal Officiel de la République Française, no. 302, 29 December 2015, text no. 2. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031704236

leave[23]. Eligible employees, as well as self-employed carers, can now receive the *Allocation Journalière du Proche Aidant (AJPA)*[24] – a daily allowance of about €52 per day for single persons or €44/day if the carer lives with a partner. The allowance is paid by the national family insurance funds (CAF/MSA) rather than employers[25]. A carer can receive AJPA for up to 66 days in total, which corresponds to the 3-month leave at full-time, extendable if taken part-time. This reform is a significant legal innovation, making France one of the first EU countries to remunerate family caregiving time off work on a national scale. It aims to soften the financial sacrifice of those who interrupt employment to fulfill caregiving duties.

Beyond leave, France provides several other protections to informal carers. Carers on leave continue to accrue pension rights: periods of caregiver leave count towards social security for retirement and do not penalize future unemployment benefits calculations. French law also offers short-term leave, the *Congé de solidarité familiale*[26], for end-of-life care, with a similar allowance, ensuring carers can be with a terminally ill relative for up to 21 days. In the social security system, France has long had mechanisms to credit caregivers. For example, a person who leaves the workforce to care full-time for a family member with a significant disability may be eligible to have the state pay their pension contributions under the scheme called *Assurance vieillesse des parents au foyer*[27], which extends to carers of disabled dependents. Additionally, since 2002, France's allowance for elderly

[23] République Française. (2019). Loi n° 2019-1446 du 24 décembre 2019 de financement de la sécurité sociale pour 2020, Article 68. Journal Officiel de la République Française, no. 298, 26 December 2019, text no. 2. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039666574

[24] République Française. (2019). Allocation Journalière du Proche Aidant (AJPA), introduced by Article 68 of Loi n° 2019-1446 du 24 décembre 2019 de financement de la sécurité sociale pour 2020. Journal Officiel de la République Française, no. 298, 26 December 2019, text no. 2. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039666574

[25] République Française. (2019). *Loi n° 2019-1446 du 24 décembre 2019 de financement de la sécurité sociale pour 2020*[Law no. 2019-1446 of 24 December 2019 on Social Security financing for 2020]. Journal Officiel de la République Française, no. 298, 26 December 2019, text no. 2. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039666574

[26] République Française. (2008). Loi n° 2008-1330 du 17 décembre 2008 de financement de la sécurité sociale pour 2009, articles 9 and 10, establishing the Congé de solidarité familiale. Journal Officiel de la République Française, no. 293, 18 December 2008, text no. 1. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000019961645

[27] République Française. (1972). Code de la sécurité sociale, articles L. 381-1 à L. 381-4: Assurance vieillesse des parents au foyer (AVPF). Consolidated version available at https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006742113

dependence[28] can be used by the older person to pay a family member other than spouse or partner for care, thereby formalizing and modestly remunerating family care. The 2015 law established a "*right to respite*" for caregivers: if an informal carer is at risk of burnout, an additional respite subsidy can be granted to finance replacement care while the carer rests. Local carers' support platforms[29].

France stands out for its recent policy momentum to strengthen carers' rights. It demonstrates best practices like *paid carer's leave, pension credits for caregiving, and a legislated entitlement to periodic respite*, backed by public funding[30]. The French example shows how a country can move from treating family care as a private matter to formally recognizing caregivers as a category deserving state support. Continuous monitoring will be needed to see if these measures sufficiently alleviate caregivers' burdens and whether further steps (such as longer paid leave or direct caregiver allowances beyond leave periods) will be taken.

Key challenges and gaps in the protection of caregivers

Across these jurisdictions, several common challenges and legal gaps emerge, despite differing systems:

Legal Invisibility and Patchwork Protections: In many countries, informal caregivers remain *legally invisible* or only weakly defined in law. Only a handful have comprehensive caregiver statutes, while others have ad hoc provisions. This results in a patchwork of support. A European survey[31] noted that only a few countries, Germany, Sweden, Austria, Belgium have

[28] République Française. (2001). Loi n° 2001-647 du 20 juillet 2001 relative à la prise en charge de la perte d›autonomie des personnes âgées et à l›allocation personnalisée d›autonomie (APA). Journal Officiel de la République Française, no. 167, 21 July 2001, text no. 1. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000404718

[29] République Française. (2015). Pierres des aidants program, established under Loi n° 2015-1776 du 28 décembre 2015 relative à l›adaptation de la société au vieillissement. Journal Officiel de la République Française, no. 302, 29 December 2015. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031704236

[30] Jensen, S. E. H., Pinkus, D., & Ruer, N. (2025, January 23). Prepare now: Europe must get ready for the coming long-term care surge. Bruegel Policy Brief. https://www.bruegel.org/policy-brief/prepare-now-europe-must-get-ready-coming-long-term-care-surge

[31] Courtin, E., Jemiai, N., & Mossialos, E. (2014). Mapping support policies for informal carers across the European Union. Health Policy, 118(1), 84–94. https://kclpure.kcl.ac.uk/portal/en/publications/mapping-support-policies-for-informal-carers-across-the-european-

national laws specifically protecting informal carers, whereas others rely on regional policies or general social support laws. Consequently, *who qualifies as a caregiver and what support they can get depends largely on where they live*. The lack of uniform recognition also means data on caregivers is poor, perpetuating their political invisibility.

Insufficient Financial Support and Social Security Gaps: Despite some innovations, most informal caregiving is unpaid labor that can impoverish families. Few countries offer direct compensation or income replacement beyond short-term leaves. Many caregivers have to reduce paid work, which affects their lifetime earnings and pensions. Without stronger financial support, caregivers risk "*falling through the cracks*" into poverty and relying on welfare due to their caregiving duties.

Access to Services and Respite: Legal fragmentation leads to inequitable access to respite care and home care support. The EU has noted stark disparities,[32] for example, only *4.7% of seniors with long-term care needs receive home care in Romania versus 54% in Belgium*[33], indicating huge gaps in service availability that put more pressure on family carers in some countries. In many cases, carers go without any break: studies show this leads to burnout and health decline. Even though respite is proven to help sustain caregiving relationships, it is not a guaranteed right in most jurisdiction[34]. Moreover, rural caregivers or those in regions with weak infrastructure particularly struggle to get support services. This uneven support structure exacerbates inequalities and undermines social justice for both carers and care recipients.

Migrant Caregiver Vulnerabilities: A significant portion of home care in wealthier countries is provided by migrant workers – whether as domestic workers employed by families or as informal "live-in" carers working around the clock. These workers often occupy a legal loophole between labor,

[32] European Commission. (2021). Long-term care report: Trends, challenges and opportunities in an ageing society (Volume I). Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/71f0ffa2-1d56-11ec-b4fe-01aa75ed71a1/language-en

[33] Belgian Health Care Knowledge Centre. (2024). *Care for the elderly in Belgium*. Healthy Belgium. https://www.healthybelgium.be/en/health-system-performance-assessment/specific-domains/care-for-the-elderly

[34] with some exceptions like France's "right to respite"

migration, and care regimes, making them prone to exploitation[35]. Migrant caregivers frequently are not fully protected by labor laws (especially if they are considered "domestic workers" excluded from overtime or maximum hours rules)[36]. They may also face abuse, excessive hours, and poor living conditions, with little recourse due to fear of losing their job or residency. *Legal frameworks often do not effectively enforce rights in private households*[37]. Furthermore, immigration policies can tie a caregiver's right to reside to a specific employer, deterring complaints about conditions. Migrant carers also suffer from lack of training and language barriers, which can impact care quality and their own well-being. Addressing migrant caregiver rights is a major challenge requiring better regulation of placement agencies, labor inspections in homes, and bilateral agreements between sending and receiving countries to ensure fair standards.

Coordination and Integration Challenges: Effective support for informal carers requires coordination across different levels of government and sectors such as health care, social services, employment, etc, is often lacking. Intergovernmental coordination problems arise, for example, in countries where funding and responsibility are split[38].The EU's lack of binding framework means that a mobile EU citizen who is a caregiver may lose entitlements when moving countries, unless bilateral arrangements step in. At the EU level itself, attempts to create a more unified approach (such as a potential *European Carers' Strategy or Directive*) have not yet materialized,

[35] Muntinga, M. E., Bakker, C., Goh, A. M. Y., Spruyt, O., McLoughlin, K., Hinks, T., & de Vries, N. K. (2022). Informal caregivers' perspectives on the continuity of care for older people living with dementia: A qualitative study. Frontiers in Human Dynamics, 4, Article 818351. https://doi.org/10.3389/fhumd.2022.818351

[36] Martikke, S., Chatzidimitriou, E., & Orton, L. (2023). Enforcing decent work in personal and household services: A European comparative perspective. European Journal of Public Health, 33(Supplement_2), ii22. https://doi.org/10.1093/eurpub/ckad160.074

[37] European Labour Authority. (2021). Study report on the personal and household services sector. https://www.ela.europa.eu/sites/default/files/2022-03/Study-report-on-personal-and-household-sector.2021_EN.pdf

[38] For instance, Canada struggles at times with federal EI programs interfacing with provincial home care services; in Spain or Italy, regional governments handle services while national programs handle cash benefits, leading to overlap or gaps. In Sweden, the division between health at national level, and social care at local level can result in carers navigating two systems for help. Internationally, when caregivers care for someone across borders, when an EU citizen caring for a parent in another EU country, social security coordination is complex, pension credits or carer's benefits are not easily transferable across jurisdictions.

partly due to subsidiarity concerns and differing national priorities. Fragmented governance also leads to carers falling between the cracks of health and social care[39]. Without integrated policy, carers often must act as coordinators of care with little guidance, compounding their burden[40].

Legal Enforcement and Awareness: Even when laws exist, enforcement and awareness lag. Many eligible caregivers do not take advantage of leave or benefits because they fear workplace retaliation or simply do not know their rights. Some employers are not be fully aware of their legal obligations to accommodate carers. Anti-discrimination protections like those stemming from the *Coleman* case, rely on individuals coming forward to assert rights, which is intimidating for many. Culturally, caregiving is still seen in some societies as a private family duty, not something one would expect legal relief for – this mindset can discourage people from seeking the support they are entitled to. Thus, a challenge is not only writing good laws but also ensuring carers are informed and empowered to use them, and that there are accessible remedies such as ombuds offices, help lines, etc. when rights are denied.

In sum, while there has been progress in carving out legal space for informal caregivers, significant gaps remain. Many carers still lack basic labor rights, financial security, or respite, and face a maze of fragmented policies. Migrant carers remain an under-protected underclass in many places. These challenges point to the need for more cohesive and innovative legal solutions, as discussed in the next section.

Identified good practices and innovative approaches

Amid the challenges, there are emerging best practices and legal innovations from various countries that offer models for improving the status of informal caregivers. By highlighting these, we can envision a more supportive legal framework for caregivers globally:

[39] Kenway, E. (2025, June 30). Carers like me connect patients and doctors – so why are we so often made to feel invisible? The Guardian. https://www.theguardian.com/commentisfree/2025/jun/30/carers-patients-doctors-feel-invisible-health

[40] U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation. (2017). Research on care coordination for people with dementia and family caregivers. https://aspe.hhs.gov/reports/research-care-coordination-people-dementia-family-caregivers-0

Comprehensive Caregiver Leave with Compensation: One best practice is to provide extended leave from employment to care for relatives, coupled with income support. For example, the EU Work-Life Balance Directive's baseline of 5 days is a start. France's recent step to pay caregivers on leave via a social security allowance is particularly innovative. This acknowledges caregiving as a form of work. Governments that fund such allowances ensure that even small businesses can let employees take caregiving leave without financial strain. Early data from France suggest that paid leave uptake is increasing, indicating carers will use leave if it's financially feasible. Another good practice is allowing flexibility in leave taking, or the Netherlands allowing partial leaves – which helps caregivers fine-tune leave to actual needs. In the Netherlands, the *Work and Care Act*[41] *(Wet Arbeid en Zorg)* provides for both short-term and long-term care leave. Employees can take short-term care leave amounting to twice the number of hours they work per week, receiving at least 70% of their salary. Long-term care leave allows for up to six times the weekly working hours over a 12-month period, though it is typically unpaid. These provisions offer flexibility, enabling caregivers to adjust their work schedules to accommodate caregiving responsibilities

Respite and Support Services as a Right: Leading systems ensure that *respite care* – temporary replacement care – is readily available. Slovenia's new LTC law (2023)[42], for instance, guarantees respite services and even provides partial wage replacement so family carers can reduce work. France's right to respite fund is another model. Making respite an enforceable part of the care plan rather than an afterthought, is key to sustaining carers. Additionally, offering training, counseling, and psychosocial support to carers has shown positive results.

Integrating Informal Carers into Care Teams: Some jurisdictions have moved toward seeing informal caregivers as *partners* in the healthcare team. For example, Italy's 2023 LTC reform plans to formally recognize family caregivers in an Individualized Care Plan, involving them in assessment and

[41] Wet arbeid en zorg [Work and Care Act], Stb. 2001, 350 (Netherlands). Retrieved from https://wetten.overheid.nl/BWBR0013008/

[42] Republic of Slovenia. (2023). *Zakon o dolgotrajni oskrbi (ZDOsk-1)* [Long-Term Care Act]. Official Gazette of the Republic of Slovenia, No. 133/23. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2023-01-2930/zakon-o-dolgotrajni-oskrbi-zdosk-1

training[43]. In *France*, hospitals are developing "Carer passports" to identify family carers and include them in discharge planning. Recognizing carers in medical settings can improve care continuity and empower carers with knowledge. It also opens the door to liability protections and guidance for carers – an important legal area (for instance, clarifying that a trained family caregiver following medical instructions should not be liable for accidents, etc., which today is often murky).

Migrant Care Workforce Reforms: To tackle migrant caregiver abuses, best practices include legalizing and regulating the domestic care sector. For instance, Israel has a regulated system for live-in migrant carers for elders, including standardized contracts and labor rights enforcement – reducing informality. Germany's court enforcement of wage law, and moves to bring migrant carers under labor protection are setting a precedent in Europe. Ratifying and implementing the ILO Convention No. 189 on Domestic Workers[44] which mandates decent work standards for domestic caregivers, is a crucial step. So far, many EU countries have ratified it, but some big ones have not[45]. Another promising practice is providing language and integration courses for foreign carers, as done in Germany for some refugees working in care. This not only improves care quality but also reduces isolation of migrant carers.

International and Regional Frameworks: On the broader stage, harmonizing standards and sharing best practices through international law can drive national changes. The CRPD Committee's stance in *Bellini v. Italy*[46] effectively urges all states party to CRPD to consider supporting family carers as part of their human rights obligations. In Europe, the possibility

[43] Santini, S. (2025). Intergenerational Informal Caregiving in an Ageing European Society. In: Teti, A., Neuderth, S., Pavlova, M.K., Ziese, G. (eds) Soziale und gesundheitliche Ungleichheit im Alter. Vechtaer Beiträge zur Gerontologie. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-48005-9_5

[44] International Labour Organization. (2011). Convention No. 189 concerning decent work for domestic workers. Adopted 16 June 2011, entered into force 5 September 2013. https://www.ilo.org/global/topics/domestic-workers/lang--en/index.htm

[45] International Labour Organization. (n.d.). *Ratifications of C189 - Domestic Workers Convention*, 2011 (No. 189). NORMLEX Information System on International Labour Standards. https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:11300:0::NO::P11300_INSTRUMENT_ID:2551460

[46] United Nations Committee on the Rights of Persons with Disabilities. (2022). Bellini v. Italy, Communication No. 41/2017, CRPD/C/27/D/41/2017. https://juris.ohchr.org/Search/Details/2872

of an EU Carers' Directive or further Council recommendations could push lagging countries to action (similar to how EU directives improved parental leave and flexible work policies over time). The European Parliament has repeatedly called for stronger EU action[47] on long-term care and carers[48]. Best practice would be the EU eventually setting minimum caregiver support standards (even if just in soft law) – for instance, recommending each Member State ensure caregivers have access to at least X hours of respite, Y days of leave, and some form of financial aid. This would help reduce the extreme fragmentation currently seen.

Legal Empowerment and Awareness Campaigns: Finally, a best practice would be not just to legislate but to ensure carers know their rights and can use them. Some governments fund public awareness campaigns or support caregiver associations that disseminate information and provide legal advice. Legal aid systems could prioritize cases involving caregiver discrimination or denial of benefits, recognizing the public interest in protecting carers.

Incorporating these best practices broadly would mark a significant shift: treating informal caregivers as integral stakeholders in health care systems with enforceable rights and supports, rather than as an invisible, taken-for-granted labor force.

Conclusion

Informal caregivers are the backbone of long-term care, and it is both unjust and unsustainable to leave them without robust legal protections. As populations age and care needs grow, relying on invisible, unsupported labor – predominantly by women – is neither ethically acceptable nor practically viable. The experiences of Germany, Sweden, France, and others show that acknowledging caregivers in law leads to better outcomes: caregivers with rights and support are more likely to remain healthy, financially secure, and able to continue providing care if they choose, whereas those left to fend

[47] European Parliamentary Research Service. (2023). Reforming long-term care in Europe: At a glance (EPRS_ATA(2023)751475). European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/751475/EPRS_ATA(2023)751475_EN.pdf

[48] Marck, M. (2023). Reframing family care: Recognising, valuing and supporting informal carers through European Union law. Utrecht Law Review, 19(2), 1–15. https://doi.org/10.36633/ulr.879

for themselves often burn out or drop out of the workforce, creating larger social costs.

Policy-makers should therefore pursue a multifaceted legal reform agenda for informal caregiving, drawing on best practices identified. Key recommendations include:

Establishing a clear legal status for informal carers in each jurisdiction, through either dedicated legislation or amendments to existing laws, that codifies who qualifies as a caregiver and what rights and services they are entitled to.

Guaranteeing essential labor rights for caregivers: at minimum, the right to short-term leave for emergencies, long-term leave for critical caregiving periods (with appropriate income support), protection from dismissal or discrimination due to caregiving, and rights to request flexible working arrangements.

Ensuring financial support and social security inclusion: no caregiver should be driven into poverty because they cared for a loved one. Regular caregiver allowances could be provided to those who give up substantial working time to care.

Protecting migrant caregivers and integrating care labor markets: Countries should formalize the status of domestic and care workers, closing exemptions in labor laws and extending inspections and enforcement into private homes, with due respect for privacy.

Improving intergovernmental coordination: whether via national strategies that align health, social, and labor sectors, or via international frameworks. Coordination gaps must be addressed.

Empowering caregivers through information and support networks: Laws are only as good as their implementation. Governments and civil society should ensure carers are informed of their rights.

Framing caregiver support as a societal obligation: There needs to be a continued cultural shift in how we value caregiving. Legal reforms can lead this shift by explicitly recognizing in statutes that caregiving is important work.

Ultimately, the goal is to build an infrastructure of care that shares responsibility between families and the state, rather than simply transferring more load onto overstrained families. As the Bruegel think-tank recently warned, Europe faces a "coming long-term care surge" and must *"prepare*

now" by bolstering both formal care capacity and informal carer support. Legal innovation is a crucial part of this preparation. Countries that have embraced reforms – like Japan's LTC insurance easing burdens on families, or France paying caregiver leave – show that progress is possible and beneficial. Those lagging can draw lessons and avoid re-inventing the wheel.

In conclusion, providing comprehensive legal rights and protections to informal caregivers is a moral imperative grounded in principles of equity, dignity, and justice. It is also a sound economic and social policy, as it enables caregivers to continue contributing to society without sacrificing their well-being. A carer-inclusive legal framework ultimately benefits not only caregivers, but care recipients, employers, and society at large by promoting shared responsibility for the vulnerable. As case law and human rights norms increasingly affirm, caring for the carers is not just a compassionate choice – it is a requirement for any society that claims to value its members' health and family life. It is time for legislators and governments worldwide to act on this insight, bridging the legal gaps and forging a future where those who give care are themselves cared for by the law.

II

INTERVIEWS

Eiropas drošības stiprināšanas meklējumi

Intervija ar Rihardu Kolu Eiropas Parlamenta deputātu

Sigita Struberga
Latvijas Universitātes lektore

Viena no lielākajām Eiropas diskusiju platformām, kurā ikdienā notiek viedokļu sadursme, apmaiņa un saskaņošana, ir Eiropas Parlaments. Starp deviņiem Latvijas deputātiem aktīvi mūsu valsts pozīciju pauž arī Rihards Kols. Tuvākajos gados Eiropas Savienības dalībvalstīm būs jāveic daudzi mājas darbi. Eiropas līmenī būs jāpieņem nepopulāri, bet nepieciešami lēmumi. Sarunā ar Rihardu Kolu uzmanība pievērsta drošības diskusijām Eiropā.

Kādas ir Eiropas Savienības drošības prioritātes un vai tiek domāts par jaunu stratēģisku plānu veidošanu?

Es esmu skeptisks par daudziem stratēģiskiem plānošanas dokumentiem un vīzijām. Bija "Globālā Eiropa", tad nāca "Stratēģiskais kompass", un tā veidojas, kā saka, stratēģijām stratēģijas. Drošībā un aizsardzībā lielais lietussargs ir NATO – NATO funkcijas. Eiropas Savienība (ES) var būt papildinoša ar saviem lēmumiem, jo tā savos pamatos raksturojama kā sociālekonomisks projekts.

Krievijas agresijas Ukrainā dēļ vairāk tiek runāts par kopīgo drošības un aizsardzības politiku. Ir dalībvalstis, kas pasaka, ka Eiropa nevar kļūt par militāru aliansi. ES līgumos ir ierakstīta kopējā drošības un aizsardzības politika, drošības un ārējā politika, tai skaitā arī tirdzniecības politika. Viss, kas saistīts ar "*hard*" aizsardzību, ir gūlies uz dalībvalstu pleciem, arī caur NATO prizmu.

ES ir nepieciešama vienota, praktiski realizējama politika, kura ir ne tikai stratēģiju un vīziju līmenī. Eiropas Komisijas prezidente turpina pildīt savus pienākumus, un viņas skaļais paziņojums – apņemšanās izveidot pretgaisa aizsardzības kupolu Eiropai – ir viens no daudzajiem, bet viss atduras pret "maciņu", jo ir saistīts ar NATO apstiprinātajiem izdevumiem aizsardzībai. Divpadsmit dalībvalstis aizsargā ES sauszemes ārējo robežu un piecas – jūras robežu. Desmit valstīm šādas funkcijas nav. ES budžets nav paplielināts jau diezgan ilgu laiku, pašlaik tas ir nepilni 200 miljardi eiro gadā. Jaunais aizsardzības un kosmosa komisārs aplēsa, ka militārajai mobilitātei nepieciešami 70 miljardi eiro. Pašlaik ir vērojama kavēšanās, "gumijas vilkšana". Ambīcijas ir, bet izpildījuma nav.

Paredzamas arī diskusijas par jauno finanšu plānošanas periodu – vai tiks veidots lielāks ES budžets. Ar 1 % no IKP tās vajadzības nav iespējams fiziski apmierināt. Ir dalībvalstis, īpaši no Dienvideiropas, ar izteiktu pretestību, ka ES budžeta finansējums tiek novirzīts militārajai jomai. Tagad tiek lauzti šķēpi arī Eiropas Parlamentā par grozījumiem regulās attiecībā uz spēkā esošajiem finanšu avotiem. Jo dalībvalstis ir tālāk no agresora, jo mazāka izpratne tām ir par tiešo apdraudējumu. Robežvalstīm, tostarp Baltijas valstīm, nav ilūziju par apdraudējuma līmeni. Ir skaidrs, ka jāinvestē kopējā drošībā – tā nav tikai Baltijas, bet visas ES drošība un aizsardzība.

Jūs vairākkārt minējāt NATO un Eiropas Savienības sadarbību tādās jomās kā militārā mobilitāte, noturība, kiberdrošība. Kā jūs redzat NATO un ES sadarbības statusu šobrīd? Vai tā ir uzlabojusies un kādi ir izaicinājumi?

Es nedomāju, ka pastāv kādas īpaši samilzušas attiecības institūciju starpā. NATO dalībvalstīm ir pienākumi saskaņā ar līgumiem, un katra dalībvalsts tos pilda pēc savas izpratnes – viena ar uzviju, cita "pieklibojot". Attiecībā uz ES situācija ir mazliet citāda – līgumu un funkciju ir vairāk un

tās ir plašākas. NATO nevar kaut ko pieprasīt no ES kā veidojuma, jo viss atduras pret dalībvalstu izpratni un spējām īstenot dažādus projektus, bet dialogs pastāv. No ES puses ir izpratne, ka visam, ko darām drošības un aizsardzības jomā, ir jābūt papildinošām NATO aktivitātēm.

Attiecībā uz Eiropu ir trīs aizsardzības plānošanas reģioni, aizsardzības plāni ir apstiprināti. To īstenošana atkarīga no dalībvalstu gatavības, tostarp savienojamības. Kohēzijas politika un izlīdzināšanās ir svarīgas, jo ES ir ļoti dažāda attīstības līmeņa ziņā, īpaši kritiskās infrastruktūras un militārās mobilitātes jomā. Jaunākās dalībvalstis joprojām redz būtiskas atšķirības starp Rietumu un Dienvideiropas valstīm savienojamības ziņā – ceļi, dzelzceļš, enerģētiskā infrastruktūra ir dramatiski atšķirīga. Līdz ar to pastāv viedoklis, ka šie projekti, ko tagad plāno īstenot, ir vērsti tieši uz ES kohēziju – attīstības līmeņa izlīdzināšanos.

Divējāda pielietojuma infrastruktūra nozīmē, ka tā ir vērsta gan civiliem, gan militāriem mērķiem. Te arī parādās simbioze, ja drīkst teikt, NATO funkcijām ES teritorijā. Pašlaik es nesaskatu kādu konfliktsituāciju. Jā, ir bijušas diskusijas citās jomās, ko ES definē kā stratēģisko autonomiju, – ka jāpaliek absolūti neatkarīgiem virknē jomu, tai skaitā arī aizsardzība, izejvielas un citas stratēģiski nozīmīgas nozares. Bet tās, man šķiet, ir tēmas, kas ik pa brīdim tiek iepilinātas, lai sabiezinātu krāsas un spriedelētu nedēļu, divas par lietām, kuras visi apzināmies, ka tās nedarbosies, tādējādi novēršot uzmanību no akūti nepieciešamā.

Noteikti jāmin, ka NATO beidzot arī sāk pārskatīt civilās un militārās attiecības. Kritika, kas izskanējusi, ir ne tikai par iespējamo funkciju dublēšanos vai par stratēģiskās autonomijas centieniem, bet arī par to, ka, lai gan ir laba griba sadarboties, reālā sadarbība birokrātiskajā līmenī nenotiek. Lai gan abas organizācijas atrodas Briselē, tāda aktīva ikdienas sadarbība faktiski nav vērojama. Tas ir viens no būtiskākajiem kritikas punktiem pētnieku kopienā.

Esmu izstrādājis priekšlikumu, kas balstīts NATO rekomendācijās, par duālās pielietojamības enerģētikas infrastruktūru, kas nepieciešama militārajai mobilitātei, piemēram, militārās aviācijas degvielas infrastruktūras nodrošināšanai. NATO sniedz rekomendācijas, bet tas jau ir ES uzdevums skatīties, ko varam īstenot ar centralizētajiem finanšu līdzekļiem. Līdz 2027. gadam mērķis ir atslogot nacionālos budžetus šādiem projektiem.

Kā piemēru varu minēt vienu iestrādi, kas nāks no Eiropas Parlamenta puses (ceru, ka to atbalstīs), – tā paredz ne tikai militāro mobilitāti, bet arī pretmobilitātes pasākumus. Pretmobilitāte attiecas arī uz kritiskās infrastruktūras aizsardzību.

Papildus ir aizsardzības industriju atbalstošas programmas NATO ietvaros, kas atbalsta inovācijas, piemēram, DIANA. Tagad ar šo "Miniomnibusu" tiek atvērta arī "Apvārsnis Eiropa" programma, ar kuras palīdzību var atbalstīti duālā pielietojuma tehnoloģiju attīstības projektus.

Ja ES tiešām, kā paredz to Emanuela Makrona vīzija, spētu īstenot visas šīs funkcijas, diez vai Zviedrija un Somija iestātos NATO. Kāpēc viņiem to vajadzētu darīt? Tāpēc, ka viņi saprot – funkcijas un atbildības jomas ir stingri nodalītas. Kolektīvās aizsardzības jomā NATO tiešām spēj īstenot atturēšanas politiku.

Jūs minējāt noturību. Kā varētu attīstīties Eiropas Savienības politika attiecībā uz noturību? Kādas iespējas būtu Baltijas valstīm?

ES politikās sabiedrības noturība nav pietiekami novērtēta. Baltijas valstis ir pirmrindnieki, piemēram, informatīvās telpas stiprināšanā un aizsargāšanā, kas ir viens no lielākajiem Ahileja papēžiem Eiropā.

Nozīmīga ir informatīvās telpas aizsardzība no Krievijas propagandas un trešo valstu mēģinājumiem torpedēt un iedragāt sabiedrības uztveri par dažādiem procesiem Eiropā un pasaulē. Eiropas Parlamentā jau vairāk nekā deviņus mēnešus cīnos, lai "*Russia Today*" nebūtu pieejams, bet trūkst dzelžainu, drastisku sankciju. Noturības jautājumā mani visvairāk tracina tas, ka ES tiek runāts, ka tūlīt īstenosim noturības politiku, mums ir "*toolbox*", izstrādāta instrumentu kaste, kuru varam pielietot, utt. Bet nav bijušas nevienas demokrātiskas vēlēšanas pēdējā pusotra gada laikā, kuras nebūtu mēģināts ietekmēt no ārvalstīm ar dezinformāciju, informatīvo karu un dažādiem nelegāliem finansēšanas aspektiem.

Ir arī dalībvalstis, piemēram, Francija, kur joprojām regulējums atļauj politiskās partijas finansēt no trešajām valstīm; tas parāda, ka mums pašiem ir problēmas ar to, ko angliski sauc par **"*enforce*"**, t.i., īstenot pieņemtos lēmumus. Tirdzniecības bilance ar Krieviju ir samazinājusies, bet joprojām ir nepieņemami lielā apjomā. ES uz vienprātības principa pieņem lēmumus par sankcijām, jā, tā tas ir. Bet nekas neliedz, ja arī vienprātība netiek panākta ES Padomes sanāksmē, dalībvalstīm individuāli pašām pieņemt šos lēmumus.

Es varbūt filozofēju, bet daudz kas ir saistīts ar sabiedrības redzējumu, kā pašas ES institūcijas un politikas veidotāji ievēro savus lēmumus un publiski pausto nostāju pret agresoru. Tāpēc, man šķiet, ES būtu ar nulles toleranci jāvēršas pret sankciju neieviešanu. Tas sabiedrībai parādītu, ka politiķi, politikas veidotāji, aicinot sabiedrībai būt noturīgiem, demonstrē konsekvenci, nevis ar savu divdomīgo rīcību vairo šaubas un skepticismu sabiedrībā. No tā veidojas attieksme. To jau mūsu iedzīvotāji, pilsoņi redz un jūt. Nerodas pārliecība, ka mēs paši esam spējīgi īstenot politiku, ko sludinām.

Svētdienas "Nekā personīga" raidījumā bija stāsts par Lietuvas sportistu, kurš Maskavā atklājis dārgu autosalonu. Šīs mašīnas ir gājušas arī caur Latviju. Tas, protams, sabiedrībai rada jautājumus.

Bet tas jau arī ir Kremļa režīma mērķis – sēt sabiedrībā neuzticību demokrātiski ievēlētajām institūcijām. Kad mūsu politiķu vārdi nesakrīt ar reālo situāciju dzīvē, ticība un uzticēšanās tiek sadragāta. Nav nekā dārgāka (te es nedomāju naudas izteiksmē) vai vērtīgāka kā uzticība, it īpaši apstākļos, kad mūsu reģionā ir tāds apdraudējums, kāds nāk no Krievijas un, protams, satelītvalsts Baltkrievijas. Bet, cik es saprotu, tagad parādījās ziņa, ka Somija pilnībā slēgusi robežu ar Krieviju. Redz, kādēļ Latvijai?

Es domāju, kā spilgtu piemēru var minēt Otavas konvenciju, par kuru diskutēja, kad es vadīju Saeimas Ārlietu komisiju. Latvija bija pirmā, kas paziņoja par izstāšanos no tās, un tad kā domino kauliņi pievienojās Igaunija, Lietuva, Somija, Polija un pat simboliski Ukraina. Kanādieši neko īpaši neteica, nu nebija nekādas drastiskās reakcijas.

Mēs investējam aizsardzībā, veidojam jaunus poligonus, piemēram, Sēlijas poligonu. Mums ir daudz iespēju kļūt par reģionāliem spēlētājiem. Sēlijas poligonā mums ir infrastruktūra, noliktavas, kur var uzglabāt visas nepieciešamās munīcijas. Te ir visi nosacījumi, lai uzturētu augstu kaujas gatavību.

Līdzīgas rekomendācijas bija saistībā ar Lietuvas-Latvijas sadarbību NATO ietvaros. Šāda veida sadarbību varētu veidot attiecībā uz Sēlijas poligonu.

Netālu jau ir arī Lielvārdes lidosta, kuru varētu savienot ar Sēlijas poligonu, izmantojot dzelzceļa līniju. Tas atkal ir mobilitātes jautājums.

Ja mēs runājam par aizsardzību, es arī uzskatu, ka Baltijas valstīm ir jāslēdz trīspusējie drošības sadarbības līgumi, kas praktiski būtu zem piektā

NATO panta. Tas nozīmē, ja mums ir iekšēja vai ārēja agresija, mēs negaidām ne ceturtā panta iedarbināšanu, konsultācijas, ne piekto pantu, bet mūsu bruņotie spēki, mūsu vienības sniedz uzreiz atbalstu tai valstij, kurā šāda agresija ir.

Un trešā dimensija – transatlantiskā, sadarbība starp ASV, Eiropas un ES dalībvalsts. Mēs redzam, ka tiklīdz Zviedrija, Somija pievienojās NATO, viņi noslēdza jaunus sadarbības līgumus drošības un aizsardzības jomā ar ASV. Mums būtu Vašingtonā jāiet ar priekšlikumiem slēgt jaunus līgumus.

Noslēgsim mūsu sarunu uz optimistiskās nots. Jūs jau pieminējāt vairākas nozīmīgas Eiropas Savienības iniciatīvas. Ko no šīm iniciatīvām varētu izmantot? Kas ir tas iespēju logs, kas ir pavēries Latvijai?

Tas tūlīt pavērsies. Es ļoti ceru, ka vēlākais līdz septembra beigām, oktobra sākumam tiks pieņemts šis "Mini-omnibus". Tie ir līdzekļi, kas attiecas uz kohēziju, uz Atveseļošanās fonda līdzekļiem, lai dalībvalstis šī fonda līdzekļus novirzītu prioritārajiem projektiem drošības un aizsardzības jomā.

Bet man ir bažas par Latvijas valdību. Šaubos, vai viņiem būs spēja operatīvi rīkoties, jo termiņš būs ļoti īss – praktiski līdz šī gada beigām. Dalībvalstīm vajadzēs pārskatīt programmas finansējumu, un es neesmu pārliecināts par Finanšu ministriju, kas visticamāk nāks klajā ar attaisnojumu: "Nu, kā mēs tā varam? Visi taču rēķinās ar kohēzijas līdzekļiem."

Bet es pieļauju, ka iespējas vēl būs. Ir lielais "Omnibus", pie kura strādā komisārs Kubiļus, un tā jau būs plašāka iniciatīva. Tas būs atsevišķs fonds nākamajā plānošanas periodā (līdzīgi kā kohēzija) aizsardzības jomā. Bet jārēķinās, ka būs daudz kritēriju, kas, manuprāt, ir pozitīvi – tie spiedīs dalībvalstis sadarboties. Jo lielā problēma, uz ko NATO norāda, ir tā, ka dalībvalstīs ir pārāk dažādas sistēmas, piegādes ķēdes – tas visu padara sarežģītu.

Ja sākam veidot kopīgos iepirkumus daudzās jomās, tas padara efektīvākus arī NATO aizsardzības plānus. Protams, nācās daudz lauzt šķēpus ar kreisajiem, sociālistiem un pavisam kreisajiem, kuriem joprojām ir tabu aizsardzības finansēšana no ES līdzekļiem.

Tagad ir pretestība "Mini-Omnibusam", jo daudzi uzskata, ka kohēzijas finansējums nedrīkst tikt izmantota citiem mērķiem. Kohēzijas līdzekļi tikai kohēzijai, un viss. Uz to arī mana atbilde – tā ir dalībvalsts kompetence, vai izmantot šo iespēju vai nē. Tā nav obligāta. Tad turpiniet izmantot savu

kohēzijas aploksni tā, kā sākotnēji 2021. gadā apstiprinājāt un īstenojāt, bet neliedziet citām dalībvalstīm elastību!

Latvijā ir viens cilvēks, kas atbildīgs par ES fondiem, tas ir Ints Dālderis. Viņš joprojām ir premjerministres padomnieks ES fondu jautājumos. Neesmu dzirdējis, ka viņš komunicētu, kad tuvojas valsts budžeta pieņemšana. Visur runā – kur ietaupīsim, ko griezīsim, iesaldēsim algas. Bet nesaka: "Klausieties, mums būs iespēja pārdalīt ES finansējumu!" Varbūt atsakāmies no viena vai otra baseina kādā pašvaldībā, bet ieguldām to robežā un atslogojam budžetu.

The Asia-Europe Foundation[1] – a platform for cooperation

Interview with Stein Verschelden EU Policy Officer for the Asia-Europe Meeting

Sigita Struberga
Lecturer, University of Latvia

Despite evolving geopolitical challenges, the European Union (EU) maintains diplomatic relations with nearly every country in the world, engaging with strategic partners, major global actors, and emerging or developing powers through a comprehensive range of instruments. This broad diplomatic network – one of the largest globally – enables the EU to promote its interests and values via bilateral and multilateral dialogue, development cooperation, crisis response, and structured foreign policy tools. Within this framework, the Asia-Europe Foundation (ASEF) serves as a key mechanism for interregional cooperation between Asia and Europe and remains the only permanent institution established under

[1] The EU's engagement with Asia is framed through the European External Action Service (EEAS), which promotes not only the Union's political and economic interests but also its commitment to follow the operational logic of the normative power, which puts emphasis on democracy, rule of law, and multilateral governance. Founded in 1997, ASEF facilitates structured engagement between the two regions by supporting initiatives in education, culture, youth, public diplomacy, and sustainable development. In the context of intensified geopolitical competition and rivalry, ASEF aims to provide a consistent platform for soft diplomacy and societal exchange, complementing more traditional state-driven foreign policy mechanisms. Despite differences in national priority settings – and, consequently, in the level of financial, human, and other related resource commitments – as well as differing geopolitical orientations, the foundation has so far succeeded in keeping this multilateral format active, but also questioned in terms of its sustainability and complementability with other programms.Latvia joined ASEF in 2004- the same year, when it joined EU and NATO- and has been an active member since. However, not all EU member states demonstrate the same level of engagement – some do not contribute membership fees at all, contribute only minimal amounts, or do not actively participate in ASEF's activities.

the Asia-Europe Meeting (ASEM) process. The role of ASEM in fostering cooperation between the two regions is the focus of a discussion with Stein Verschelden, EU Policy Officer for the Asia-Europe Meeting.

How would you define ASEF's role in the EU's broader Asia-Europe engagement strategy?

ASEF is an important platform because it addresses those subjects and connections that go beyond what is currently at the top of everyone's agenda – defense, trade, and security. There is so much more out there. Yes, there are things that divide us, but there are also so many things that unite us, where we can meet each other. And this is what ASEF is for me – it provides us with that occasion.

Particularly in the area of culture – but also in public diplomacy, journalism – they organize events on these topics. It brings people together. And in doing so, it brings together networks from both regions. That is what ASEF's work is really about, and it is very important. We call it soft diplomacy. It is often overlooked, but it is incredibly important and cannot be underestimated. So, that is what ASEF is about, I think. And that's why it matters for the EU.

What are the EU's main objectives in participating in ASEF? Beyond your personal perspective on its importance, what defined or formalized goals guide this engagement?

This brings us to the multilateral level. Coming from the European institutions, we operate as a multilateral platform, and we have seen what the EU has achieved for its own members and how it has helped them progress. From the perspective of EU institutions, inter-regionalism is a key angle – and one of the most important. We see ourselves as natural counterparts with others, and in that sense, ASEF is a clear example. Of course, there is also the UN and other multilateral organizations across various areas, and it is important for the EU – already uniting 27 member states – to seek synergies with other platforms and multilateral structures.

Again, it is all about bringing people together, encouraging dialogue, building networks, and identifying what unites us.

We have the EU Indo-Pacific Strategy, adopted in 2021, which highlights seven focal areas – sustainable development, climate, security, trade,

and maritime cooperation being among the most important. At the same time, I sometimes hear from colleagues, including from member states, questions like: "Why should we care about ASEAN (The Association of Southeast Asian Nations), especially now that it is in a standstill due to Russia?" and "What about ASEF – why is it relevant?" My response is that while the Indo-Pacific Strategy is significant, it does not replace the value of ASEF.

ASEF continues to work in areas not directly addressed in that strategy but that are equally important – such as culture, education, and public diplomacy. That is why I believe ASEF should remain part of our overall strategic approach toward the region and the EU's broader engagement.

Thank you for highlighting the fundamentals like regional cooperation and maritime issues! But the EU is also strongly values-based. Do you see mechanisms through which it promotes democratic values in this format?

The EU is seen as one of the most, if not the most, important actors when it comes to values. There is an annual survey conducted within ASEAN that consistently shows how highly the EU is regarded as a reliable partner in this area. So, it is something we should continue to uphold – to be a guiding light for them. Of course, this should be done without any sense of colonialism or finger-pointing – our role is to support. And I believe that' is also what our partners expect from us: to be there to help them develop further, in a constructive and respectful way.

ASEF can be instrumental in this. It allows us to showcase and share our experiences. Being an informal platform, it encourages open conversation, making it easier for people to speak freely. Through such exchanges, we can convey values and build understanding. These networks, formed through ASEF and other events, play an essential role in that process.

For us, ASEF is a key tool – especially in promoting values. We incorporate this into most of our discussions and dialogues. Human rights, for example, is a core issue we consistently raise – not only in high-level political talks but also through a bottom-up approach, which is equally important.

And the temporary suspension of Russia's participation is also linked to the EU's values-based approach, isn't it?

Yes, absolutely. Suspending Russia's participation in ASEF was fundamental – it was the only way to ensure that ASEF could continue its work. With Russia in the room, I do not see how it would have been possible for

us – meaning the EU – to maintain cooperation or continue providing support. We also attempted to address this within the ASEM framework, but since all decisions there are made by consensus, we couldn't achieve it – which was somewhat expected.

However, within the EU, there was clear consensus: if we couldn't resolve it at the ASEM level, then we would effectively "put it in the fridge." The unfortunate part is that it's already been four years. And the longer it goes on, the harder it becomes to revive ASEF's components and get things running again. That said, it is just an observation. In the end, it will depend on the dynamics – on how motivated people are to restart ASEF.

Beyond the temporary suspension of Russia, which could be seen as a success, what other key initiatives or projects reflect the EU's strong engagement – particularly in areas such as education, culture, or broader cooperation?

We are – speaking from the perspective of the European institutions – pleased to see that many European members are actively stepping in. To be clear, we are a member like any other country. We're not in a higher position, even though we currently hold the chairmanship of the Board of Governors. Next year, another country will take over, and it will likely be another European country. Then they will take the lead, and we will become just another member again. Still, we maintain oversight and stay in close contact with the executive team.

It's very encouraging to see strong buy-in from the member states, which I believe is a positive sign. It is not always about the European Union itself – what matters is that member states are also involved. We contribute actively, provide significant financial support, and our funding is earmarked, meaning it is directed to specific areas. Communication is a major part of our support.

I believe we contribute to almost all of ASEF's pillars – perhaps with the exception of health. So, our focus is mainly on education, culture, and communication. These are the three key areas where we provide support. For us, the most important thing is that ASEF can carry out its work, and that we help enable that. We also try to offer in-kind support where possible, though this can be more challenging – such as seconding someone to ASEF. As an

institution, and for many governments, that is something that has to be considered more carefully at the moment.

You mentioned that the EU is, as another member in here, but does not the EU do any coordination? I believe in this pledge for the EU there is – or for European countries – there is some coordination work which the EU does.

Not in this one, no. If you mean, like, that we would consult and experience – maybe something to explore – like sort of a Team Europe approach, which we have out there with countries or with organizations. We coordinate the European caucus, so we have our meetings, we call them together. But now that is because we are the chair. Take it over – should take it over. We are always there to help. We have this network of contacts, so we keep the overview to make sure that all the members stay together. But so far, as far as I remember, there has not been that kind of coordination. Members – also European members – they decide how they can, how they would coordinate the spending of the money or where the focus will be.

But it is an interesting topic. It is definitely something maybe to put on the table and see if we could develop something. The thing is also – this budgetary support is very volatile and fluid, particularly in these days, with what is going on with the global challenges that we are facing. But that does not take away that we should not try it.

Looking ahead, do you think the EU's priorities will shift, or will the current focus remain the same?

Whether it is us or others, this is where soft diplomacy plays a crucial role – and it truly matters. For ASEF, it is important to stand out and avoid duplicating efforts already taking place on many other fronts. The goal should be to find a unique angle that further raises ASEF's visibility and impact.

I believe the area of education – particularly youth – is especially significant. And it is not just about formal education; youth engagement goes beyond that. The cultural dimension is also key. Alongside that, promoting core values such as human rights remains essential. Public diplomacy is an interesting area. We have engaged in it before, but the question remains – should it continue? I would say yes. As for a broader approach, perhaps there is a need to slightly refocus or retarget.

We do not have a formal document outlining "this is what we should pursue," but that does not mean we should not pursue it.

Is it more a matter of reaching consensus during the discussions here, isn't it?

Yes, of course. ASEAN partners also have their voice, and rightly so. While we may be ready to move ahead more quickly, they sometimes require a bit more time. That is the nature of a balanced, inclusive platform like this. You can express aspirations, but decisions cannot be unilaterally made in the room – and that is a strength, not a weakness.

LATVIJAS
POLITOLOGU BIEDRĪBA

LATVIJAS INTERESES EIROPAS SAVIENĪBĀ