Human and More-Than-Human Futures: Innovating Technologies for Coexistence

Together with MISTI Lithuania

Bolstering the digitalization, defense, and life sciences sectors in Lithuania

Policy recommendations

In Collaboration with Lithuanian Business, Academic, Venture Capital, and Public Sector Representatives*

* These policy recommendations reflect the outcomes of a conference held on October 8 and 9, in which MIT researchers participated.

Human and More-Than-Human
Futures: Innovating
Technologies for Coexistence

Together with MISTI Lithuania

VILNIUS TECH
Vilniaus Gedimino technikos universitetas

Strengthening Digitalization in Lithuania

Policy Recommendations

Prepared by the MISTI Lithuania consortium for Lithuania's cooperation with MIT, with the participation of representatives from Lithuanian business, academia, venture capital, and the public sector

EXECUTIVE SUMMARY

Lithuania stands at a pivotal moment in its digital transformation journey. This white paper outlines strategic recommendations to accelerate digitalization, enhance competitiveness, and ensure inclusive growth. The focus areas include strengthening innovation ecosystems, improving human capital through education and reskilling, expanding digital infrastructure, and fostering adoption across public and private sectors.

While Lithuania has achieved strong digital infrastructure and leadership in e-government services, significant gaps remain in digital skills, firm-level technology adoption, and R&D investment. Addressing these challenges can unlock substantial economic and social benefits: higher productivity, increased public revenues, improved inclusion, and stronger global competitiveness.

The proposed roadmap emphasizes coordinated actions – such as creating a Chief Scientist office, incentivizing R&D, promoting lifelong learning, and leveraging international partnerships – to position Lithuania as a regional leader in digital innovation. By acting decisively, policymakers can ensure that digitalization becomes a driver of sustainable growth and societal well-being.

CURRENT STATE OF DIGITALIZATION IN LITHUANIA

Lithuania has made significant strides in digitalization over the past decade, particularly in digital infrastructure and public services. High-speed broadband coverage exceeds 90% of households, and 5G networks now cover nearly the entire population (OECD, 2025; EU Digital Decade Country Report, 2024). The country ranks among the European leaders in e-government services, with strong adoption of electronic identification, pre-filled forms, and access to digital health records (EIMIN Lithuania, 2024). These achievements have positioned Lithuania as a regional hub for digital public services, enhancing efficiency, transparency, and accessibility for citizens and businesses alike.

Despite these advances, several critical gaps limit the full potential of digitalization. Only about 50% of the population possesses above-basic digital skills (OECD, 2025), and approximately 80% of firms exhibit low digital intensity (OECD, 2025). Digital adoption among small and medium-sized enterprises, particularly in advanced technologies such as AI, cloud computing, and data analytics, remains below the EU average (EU Digital Decade Country Report, 2024). Similarly, teleworking opportunities are extremely limited, with only 5% of employees able to work remotely (OECD, 2025). These gaps highlight that infrastructure alone is not sufficient; human capital and firm-level adoption are crucial for realizing the full benefits of a digital economy.

The OECD 2025 Economic Survey emphasizes that strengthening digital skills, innovation, and adoption can generate substantial economic gains. Increasing digital competencies would enable firms, particularly small and less-productive ones, to adopt advanced technologies more effectively, boosting productivity, competitiveness, and resilience (OECD, 2025). Enhanced digital adoption in the private sector could also expand the digital economy, improve operational efficiency, and create high-skilled jobs, helping to retain talent domestically and mitigate brain drain (EU Digital Decade Country Report, 2024).

From a financial perspective, better digitalization in public administration and finance could yield measurable revenue gains. Wider adoption of digital payments and improved e-government processes can reduce VAT compliance gaps, improve tax collection, and lower administrative costs. The OECD estimates that aligning Lithuania with digital best practices in taxation could increase government revenues by approximately 1% of GDP (OECD, 2025).

Socially, advancing digitalization promises to enhance inclusion, accessibility, and quality of life. Broader digital literacy would empower citizens to participate in online public services, e-health, education, and lifelong learning initiatives (EU Digital Decade Country Report, 2024). Improved access to telework opportunities, online training, and digital tools would particularly benefit rural populations, younger generations, and underrepresented groups, fostering equitable participation in the economy. Stronger digital services also enhance transparency and trust in institutions, contributing to better governance outcomes (OECD, 2025).

In addition, targeted investment in digital R&D and innovation could strengthen Lithuania's competitive position in emerging sectors such as fintech, AI, and cloud services. Currently, gross R&D expenditure remains low at around 1% of GDP (OECD, 2025), limiting the country's capacity to develop and scale innovative digital solutions. Strategic public support and policies fostering digital entrepreneurship could unlock private investment, accelerate technology adoption, and promote sustainable long-term growth (EU Digital Decade Country Report, 2024).

In summary, while Lithuania has established a strong foundation in digital infrastructure and public services, its full economic and social potential remains unrealized due to gaps in digital skills, firm adoption, and innovation investment. Policymakers have a clear opportunity: by investing in digital skills development, incentivizing firm-level adoption of advanced technologies, and fostering innovation, Lithuania can achieve significant productivity gains, higher public revenues, improved social inclusion, and long-term competitiveness, positioning itself as a digital leader in the region.

KEY DIRECTIONS FOR IMPROVEMENT

A comprehensive analysis of Lithuania's digitalization landscape reveals that multiple factors interact to shape the country's current performance. To clarify the main levers for improvement, key factors have been identified and summarized in a hierarchical structure below (see Fig. 1). While most of these factors are interconnected and influence each other, a simplified version is presented here to highlight the primary directions for action.

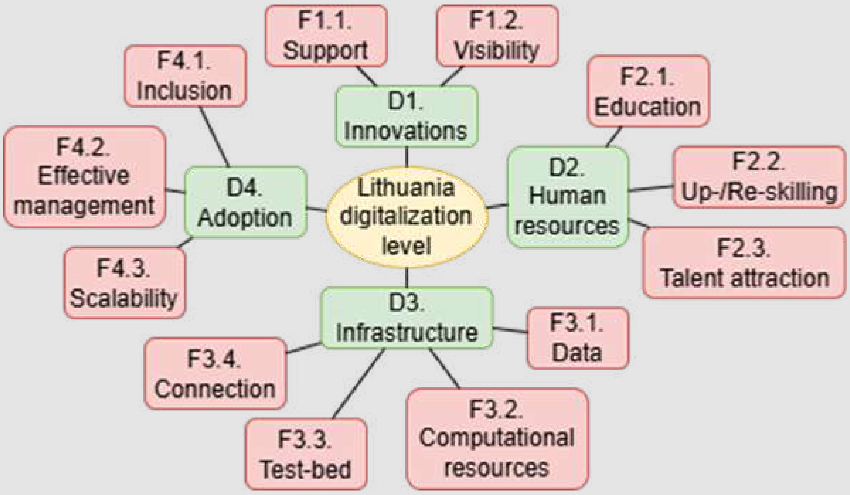


Fig. 1. Main direction and factors for Lithuanian digitalization strengthening

This structure distinguishes between Innovations, Human resources, Infrastructure, Industry/ SMEs and Public sector to prioritize interventions that can strengthen Lithuania's digital ecosystem, enhance productivity, and generate both social and financial benefits. Each of these areas have second level factors, indicating what are the main priorities, which could lead to measurable economic and social gains.

For better understanding, there is a short description for each of these key factors:

F1.1. Innovation support. Innovation support is crucial for nurturing a thriving digital ecosystem in Lithuania. It encompasses financial, technical, and regulatory assistance for startups, SMEs, and research institutions that develop new digital technologies. By fostering partnerships between academia, industry, and government, innovation support encourages collaborative R&D projects and pilot initiatives. Programs such as grants, incubation, and mentorship are essential to help innovators translate ideas into scalable solutions and accelerate the country's digital transformation.

F1.2. Innovation visibility and availability. Ensuring that innovations are visible and easily accessible is vital for their adoption and impact. This involves creating platforms, databases, and networks where new technologies, research outcomes, and best practices can be shared with potential investors, collaborators, and end-users. Innovation visibility also includes promoting digital achievements through conferences, online portals, and case studies, which helps generate awareness, stimulate partnerships, and increase the likelihood that solutions are adopted across sectors.

F2.1. HR education. Building a foundation of digital literacy and competence starts with education. HR education in Lithuania focuses on integrating digital skills, AI literacy, and STEM knowledge into formal education at all levels. By equipping students with coding, analytical thinking, and problem-solving skills, the country ensures a future-ready workforce capable of driving and sustaining digital transformation. Education also serves as the entry point for lifelong learning and innovation-oriented mindsets.

F2.2. HR upskilling and reskilling. Beyond formal education, continuous upskilling and reskilling are essential for keeping the existing workforce relevant in a rapidly evolving digital landscape. Programs that provide training in AI, data analytics, cybersecurity, and other emerging digital competencies enable employees to adapt to technological changes and fill skills gaps. By investing in professional development, Lithuania can maintain a flexible workforce capable of leveraging new technologies for economic and societal benefits.

F2.3. Talent attraction. Attracting top digital talent from abroad strengthens Lithuania's innovation ecosystem by bringing new expertise, perspectives, and networks. Talent attraction relies on competitive salaries, supportive visa policies, and a vibrant innovation-friendly environment that encourages international professionals to settle and contribute. By positioning the country as a hub for tech startups, AI research, and digital services, Lithuania can draw skilled individuals who help accelerate national digitalization initiatives.

F3.1. Data (as part of infrastructure). Data forms the backbone of digitalization, serving as a resource for analytics, AI solutions, and evidence-based decision-making. Strengthening Lithuania's digital infrastructure includes ensuring high-quality, secure, and accessible datasets that can be leveraged by businesses, public institutions, and researchers. Well-governed and interoperable data ecosystems enable innovations to scale effectively while maintaining privacy and security standards.

F3.2. Computational resources. High-performance computing and cloud infrastructure are essential for processing large datasets, running AI algorithms, and supporting advanced simulations. Access to robust computational resources allows startups, research institutions, and SMEs to develop and deploy complex digital solutions efficiently. Providing equitable access to these resources ensures that innovation is not limited by technological constraints and helps accelerate Lithuania's digital maturity.

F3.3. Test-beds. Test-beds are controlled environments where new technologies can be piloted, validated, and refined before large-scale implementation. They enable experimentation with AI, IoT, and other emerging solutions in a real-world context while minimizing risks. By fully utilizing test-beds, Lithuania can accelerate the adoption of cutting-edge digital technologies, demonstrate their value, and provide confidence to stakeholders considering full-scale deployment.

F3.4. Connection (as part of infrastructure). Reliable connectivity is fundamental to any digital ecosystem. High-speed broadband, 5G networks, and robust IoT infrastructure ensure that digital services are accessible to urban and rural areas alike. Strong connectivity supports seamless collaboration, enables real-time data exchange, and allows digital solutions to operate effectively at scale. Enhancing network infrastructure thus forms a critical pillar of Lithuania's digitalization efforts.

F4.1. Public sector, industry, SMEs inclusion, motivating digitalization. Broad participation in digital transformation is crucial for national impact. Engaging the public sector, industry, and SMEs ensures that a wide range of stakeholders benefit from and contribute to digital initiatives. Motivating organizations to adopt digital solutions can be achieved through awareness campaigns, incentives, and showcasing tangible benefits. Inclusive engagement ensures that digitalization strengthens the economy and society as a whole.

F4.2. Effective management of digitalization. Effective management is key to aligning digital initiatives with national goals and resources. It involves coordinating strategies across sectors, setting clear priorities, providing optimized pipelines for innovative solutions, and establishing governance frameworks that monitor progress and ensure accountability. Strong leadership and structured management practices help avoid fragmentation, optimize investments, and guarantee that digital transformation delivers sustainable results.

F4.3. Scalability and availability of existing solutions. To maximize impact, digital solutions need to be scalable and widely available. Proven technologies should be adaptable, interoperable, and cost-effective to facilitate their adoption across sectors and regions. By promoting reuse and standardization of successful digital solutions, Lithuania can accelerate nationwide implementation, reduce duplication of efforts, and enhance the overall efficiency of digitalization initiatives.

Taking into account the existing connectivity level, planned investment into LitAI project and existing initiatives for Baltic AI Giga Factory, work on AI Act implementation (RRT, 2025) and ongoing initiative to provide wide data lake (VDV, 2024) to open data, the strategic direction towards infrastructure direction is set. Meanwhile the rest of the direction could be improved. Therefore, this document further lists some recommendations for more holistic digitalization strengthening in Lithuania.

STRATEGIC ROADMAP OF POSSIBLE ACTIONS

To support the innovation ecosystem (D1), the following actions could be taken in Lithuania:

1. Establish a dedicated office within the Prime Minister’s office (Chief Scientist) to prioritize and coordinate R&D activities across Lithuania.
2. Increase transparency in R&D project competitions to build trust and provide learning opportunities for new innovators.
3. Improve coordination between R&D agencies to streamline support and avoid fragmentation.
4. Define new policies to incentivize additional funding for R&D (e.g., tax incentives, co-funding).
5. Promote institutional and systematic reforms in R&D to create a modern and competitive ecosystem.
6. Develop AI plug-and-play centers to accelerate practical application and visibility of digital solutions.
7. Leverage partnerships with internationally recognized institutions (e.g., MIT) to transfer knowledge, enhance innovation credibility, and attract talent.

To improve the situation with human capacity (D2), these actions are recommended:

1. Dedicate funding to prepare engineers with advanced digital skills throughout all education phases (early education, STEM promotion, higher education, professional upskilling and reskilling) to raise societal readiness for new technologies.
2. Promote AI-enhanced, constantly updated and Lithuanian strategy matching personalized learning tools as supplemented life-long learning assistants.
3. Provide incentives (e.g., tax reductions) for companies to support employee upskilling, reskilling, and establishment of innovation/upskilling divisions.
4. Establish joint governmental and business funds to motivate innovative students to develop and share ideas from a young age.
5. Set ICT professional qualification requirements with progressive certification, encouraging continuous competency growth while maintaining attractiveness of the profession.
6. Promote multi-disciplinary studies to encourage collaboration and innovation across sectors.

7. Define interdisciplinary reskilling initiatives to fasten reskilling path and its potential success, by defining reskilling programs for different sectors and building necessary competencies to work (design, apply, test, etc.) in the intersection between the sector and ICT field.
8. Support open-access learning resources adapted from advanced partners (such as MIT) for Lithuanian citizens.

Digital infrastructure (D3) direction has set action plans, which should be continued and strengthened in the future.

Digitalization adoption direction (D4) by different players (public sector, industry, SMEs, etc.) could implemented with these actions:

1. Create a new Lithuanian science strategy defining priorities for R&D activities at all levels (research institutions, business, public sector).
2. Increase incentives for R&D activity promotion in business and public sector, providing additional resources to invest into digitalization.
3. Develop showcase system, illustrating developed digital solutions and its benefits, limitations, those providing better understanding of digitalization potential and forming directions for personal institution development paths.
4. Promote open data and open course products to facilitate access to implemented solutions and accelerate digital solution development.
5. Promote international mentoring programs (delivered by advanced partners, such as MIT) to gain skills in research, digital innovation, and practical application, ensuring broader adoption in Lithuania.

The listed actions do not provide very detailed implementation path, allowing to adapt to possible budget and strategic planning activities. However, this document present experts' position on what are the main key points, which have to be solved as soon as possible, to keep up with Europe and the World tendencies.

LIST OF CONTRIBUTORS

The situation analysis and recommendations were generated by MISTI Lithuania consortium, members of session #4 on Strengthening digitalization, during the conference "Human and More-Than-Human Futures: Innovating Technologies for Coexistence". The list of contributors is the following:

Elijus Čivilis

CEO (General Manager) of Invest Lithuania (Investuok Lietuvoje), Lithuania

Dr.
Sergey Paltsev

Deputy Director of the MIT Center for Sustainability Science and Strategy (CS3) and a Senior Research Scientist at MIT Energy Initiative (MITEI), Massachusetts Institute of Technology (MIT), USA

Dr.
Fox Harrell

Professor of Digital Media and Artificial Intelligence in the Comparative Media Studies Program and Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT, USA

Dr.
Tomas Krilavičius

Professor and dean of the Faculty of Informatics at Vytautas Magnus University (VMU), Professor at VMU, Lithuania

Vilma Purienė

Director of Knowledge and Technology Transfer Centre at Vilnius Gediminas Technical University, Lithuania

Dr.
Agnė Paulauskaitė-Tarasevičienė

Head of the Kaunas University of Technology AI Excellence Centre, Lithuania

Dr.
Kęstutis Zaleckis

Professor at Vilnius Academy of Arts (VAA) and Kaunas University of Technology, as well as a Senior Researcher at the VAA New European Bauhaus Centre, Lithuania

Dr.
Daiva Vitkutė-Adžgauskienė

Professor and head of Applied Informatics Department at Vytautas Magnus University, Lithuania

Dr. Simona Ramanauskaitė	Professor and senior researcher at Vilnius Gediminas Technical University, Lithuania
Dr. Paulius Jurčys	Senior lecturer at Vilnius University, Lithuania
Dr. Violeta Motuzienė	Professor and senior researcher at Vilnius Gediminas Technical University, Lithuania
Margarita Prokopovič	Project specialist of Knowledge and Technology Transfer Centre at Vilnius Gediminas Technical University, Lithuania
Laurynas Vanagas	Business Development at Qunasys, Lithuania
Dr. Darius Milčius	Director of Research and Innovation, Head of Center for Hydrogen Energy Technologies, Vytautas Magnus University, Lithuania

CONCLUSION

Digitalization is a cornerstone for Lithuania's future economic resilience and global competitiveness. The provided insights and recommendations highlight that infrastructure alone is not enough; success depends on human capital development, innovation support, and widespread adoption of advanced technologies.

Implementing the proposed strategic actions will enable Lithuania to bridge current gaps, foster a dynamic digital ecosystem, and create high-value jobs. This transformation will strengthen public governance, empower businesses, and enhance citizens’ quality of life.

By prioritizing digital skills, incentivizing innovation, and ensuring inclusive access to technology, Lithuania can secure its position as a leading digital nation in Europe – driving sustainable growth, attracting talent, and shaping a future-ready economy.

Human and More-Than-Human Futures: Innovating Technologies for Coexistence

Together with MISTI Lithuania

ktu 1922

Enhancing Lithuanian Defense

Policy Recommendations

Prepared by the MISTI Lithuania consortium for Lithuania’s cooperation with MIT, with the participation of representatives from Lithuanian business, academia, venture capital, and the public sector

This document is based on the conclusions and recommendations of the strategic session "Enhancing Lithuanian Defense," initiated in Lithuania by the Massachusetts Institute of Technology (MIT) MISTI program. The session took place in October 2025 at a joint conference of Lithuanian universities and MIT.

During the session, **representatives of Lithuanian universities, industry and business, the government**, and **MIT** identified critical aspects of Lithuania's preparedness to counter external threats and the key challenges in strengthening it. Several priority areas were discussed: dual-use technologies that meet both civil and security, defense, and deterrence needs; cyber resilience, post-quantum computing, and critical systems protection; information defense and defense policy; and the innovation ecosystem.

Due to its geopolitical position – bordering aggressors Russia and Belarus, membership in the European Union (EU) and the North Atlantic Treaty Organization (NATO) – Lithuania **has the potential to become a testing ground for European information and defense resilience**. This document provides guidelines on the practical steps that should be taken to not only strengthen Lithuania's resilience to external threats but also to increase its contribution to regional, European, and transatlantic security.

KEY INSIGHTS

- **Targeted defense innovation**. It is proposed to bring together academia, industry, and defense forces, introduce simplified funding instruments for priority innovations, and clearly define the mechanisms for their implementation. Areas where Lithuania has real potential to specialize include unmanned platforms, mechatronics, optoelectronics, photonics, and biotechnology. It is very important not only to create and demonstrate technologies, but also to develop manufacturing technologies and innovations that would enable large-scale production at high speed and at the lowest possible cost.
- **Cyber resilience base**. Lithuania's IT and OT infrastructure is under constant pressure, so it is necessary to create a unified cyber resilience system: security operations centers, a data management platform, a hybrid cloud, and an eID infrastructure.
- **Multimodal transport infrastructure**. Lithuania's roads, railways, electricity, and communications networks need to be modernized by creating multimodal corridors. It is necessary to create and develop alternative aircraft landing and take-off sites and ensure the safety of sea routes.

- **Fostering information resilience**. It is necessary to change the mindset by creating not only deterrence but also active information defense solutions: creating counter-narratives, applying strategic communication, involving the cultural sector and the diaspora; it is necessary to establish a national information space monitoring system.
- **Society – an active force in national defense**. When considering defense and defense innovations, it is time to expand the traditional “triple helix” model (science–business–government) by adding society as a fourth link.

SITUATION OVERVIEW

The defense innovation ecosystem is not working effectively enough

In September 2025, speaking at the United Nations General Assembly[1], Ukrainian President Volodymyr Zelensky called on the world’s countries to use Ukraine's battlefield knowledge to develop defense innovations, singling out unmanned aerial vehicle technology as one of the priority areas. Crises force us to pool resources and accelerate innovation. Unfortunately, the price of breakthroughs brought about by war is unjustifiably high.

Lithuania faces an urgent need for defense innovations due to its geographical location. Technological superiority on the front lines is measured in days. However, the country’s current defense innovation ecosystem remains fragmented – there is a lack of coordination, shared vision, and interoperability between ministries, agencies, academia, and industry. This hinders decision-making and slows progress.

The formulation and implementation of defense policy is currently weakened by limited inter-agency coordination. In the area of financing and procurement, there is no consistent financing cycle from idea to implementation. Calls for proposals from different ministries are not coordinated in time, leaving projects without continuity. There is a vicious circle: the military does not fund research because it needs to purchase an already developed product, and businesses cannot develop it without funding. In addition, due to high technological readiness level requirements (TRL 5+), many promising early-stage defense and dual-use ideas do not reach the prototype development stage.

[1] https://www.youtube.com/watch?v=oGFqB9sU3nQ

The war in Ukraine has revealed the problem of insufficient production capacity in all NATO / EU countries and clearly demonstrated that it is not only high-tech products and solutions that are important, but also the ability to produce them quickly, on time, and on an appropriate scale at an affordable price. We need to learn to interact with the existing engineering and technology industry so that it can contribute to the development of production potential and supply chains. Innovation and investment are needed to develop production technologies, manage supply chains, and adapt or create alternative raw materials.

The culture of innovation is weakened by low levels of trust between science, industry, and government institutions. It must be acknowledged that the Lithuanian Armed Forces and the entire national defense system lack experience in interacting with industry and academia, in creating new technologies and developing production potential, which is why organizations often operate in isolation. Information sharing practices and procedures have not been established or standardized, and there is a lack of common language and goals.

The public lacks knowledge about real battlefield experiences – there is no structured defense education, critical thinking training, reservist training systems, or a universal resilience program. Furthermore, this knowledge is not sufficiently integrated into the innovation creation infrastructure.

Lithuania also needs to address the challenges of production and supply chains by strategically defining niches where innovations can have the greatest added value. The strong scientific and engineering base in Lithuanian science and study institutions allows for the creation of not only fundamental but also applied dual-use innovations that can become critical components of air defense, autonomous systems, situational awareness, and electronic warfare capabilities.

Cybersecurity challenges

Lithuania’s information technology (IT) and operational technology (OT) infrastructure operates under constant pressure, with cyber and information attacks on the rise, especially in times of crisis. The main risks arise from weak links between IT and OT systems, software supply chains, and data sharing barriers.

Risks include obstacles to data and intellectual property protection, lack of expertise, fragmentation of institutions, and challenges in implementing encryption technologies. Different sectors and organizations (ministries, agencies, regulators, critical infrastructure operators, academia, etc.) use different technologies, standards, and processes, collect and store cyber data in different formats, have separate management and accountability chains, and lack a unified, coordinated cyber resilience architecture. Under such conditions, it is difficult to get a common view of the situation across sectors, to quickly exchange log and incident data, to effectively manage IT / OT interfaces, and to respond to hybrid attacks in a coordinated manner.

There is a clear need to create a common resilience base: national security operations centers, a data management system, a hybrid cloud, and a European digital identity (eID) infrastructure. This should be supported by a simplified legal framework for data sharing, standardization of code signing, a national training center at universities, IT consolidation, supply chain transparency, and regular cyber resilience exercises.

Without these systemic steps, Lithuania's cyber resilience remains fragmented into separate islands. The interdisciplinary expertise of Lithuanian science and study institutions could be used more effectively to shape the architecture of cyber resilience, from deep encryption and quantum-resistant algorithms to real-time situational awareness and autonomous decisions for threat detection in OT environments.

Vulnerability of critical infrastructure

Lithuania's transport infrastructure – roads, railways, airports – remains insufficiently efficient, reliable, and sustainable by Western European standards[2]. There are currently no comprehensive solutions to ensure the movement of civilian and military cargo, people, and critical services in the event of war or natural disasters.

Lithuania's energy infrastructure is critically vulnerable. The current electricity networks are not adapted[3] to wartime conditions: there is a lack of decentralized generation at logistics hubs, no reserve energy islands, insufficient mobile generation capacity, and some transformer stations could be physically destroyed in the first hours of a conflict. This would cause a chain reaction of disruptions to communications and transport systems, paralyzing mobilization.

Wireless communication systems and telecommunications networks are particularly vulnerable, including global navigation satellite systems (GNSS, such as the US GPS and EU Galileo systems), communication services, and mobile communication networks, which could be easily disrupted or neutralized[4] by electronic warfare methods during wartime. This vulnerability is already evident in peacetime, with disruptions to aircraft and vehicle navigation systems in Lithuania caused by Russian GNSS jammers deployed[5] in the Kaliningrad region.

An additional risk is posed by the vulnerability of food supply chains, determined by Lithuania's geographical location between Belarus and the Kaliningrad region. In the event of a conflict, communication with the West via the Suwalki Corridor could be blocked or controlled by Russian forces, which would directly affect both civilian and defense supplies.

[2] Justification for the 2022-2030 Lithuanian Transport Development Program and EC data, available online at: https://ec.europa.eu/transport/facts-fundings/scoreboard/countries/lithuania/investments-infrastructure_en

[3] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52022DC0551

[4] Starburst (2025). Navigating the Unknown: The High Stakes Risks of GNSS Outages in an Era of Conflict, Logistics and Digital Economy. https://starburst.aero/news/navigating-the-unknown-the-risks-of-gnss-outages/

[5] GPS Spoofing & Jamming Map, https://gpswise.aero/

Given these vulnerabilities, it is necessary to develop Lithuania's transport infrastructure as an integrated multimodal transport corridor. This means expanding existing railways and roads, installing electricity distribution, optical communications, and mobile network infrastructure alongside them.

It is also important to develop situational awareness technologies that allow real-time monitoring of transport flows and detection of disruptions, even in the event of GNSS signal degradation. Research by Lithuanian scientific and academic institutions shows that there is a mature academic basis for the development of such infrastructure.

An especially important part of strengthening infrastructure is ensuring the security of the sea route to the West to maintain uninterrupted civil and defense communications even during a crisis or conflict. To protect Lithuania's waterways, defense solutions focused on the use of a wide range of surveillance and attack unmanned platforms are needed. In addition, technological solutions for unmanned systems and their countermeasures are relevant, which can be applied not only to defense but also to internal security tasks – for example, to technically prevent active smuggling activities originating in Belarus.

Lack of information resilience

When discussing external threats to Lithuania in the public sphere, the focus is usually on deterrence – repelling hostile attacks and defense. Hybrid warfare, which involves physical armed forces, cyber-attacks, and the domination[6] of the information space with malicious information, requires a shift from deterrence alone to proactive[7] defense.

The cognitive resistance of Lithuanian society to manipulation and psychological pressure remains limited, and monitoring of the information space and intelligence gathering on narratives is not carried out systematically – there is a lack of impact assessment and priority threat hunting capabilities. Early warning mechanisms are still being developed, and the potential of the diaspora to resist remains untapped. In addition, with the abolition of compulsory military service, practical understanding of defense and realistic war scenarios has significantly declined in society.

The protection of democratic processes is not sufficiently integrated into information defense strategies, and public leaders and influencers are not yet included in the resilience network. Communication interaction with social media platforms remains fragmented, and the state still lacks a clear strategy for information operations and counter-narratives.

[6] Sascha-Dominik Dov Bachmann, Dries Putter, Guy Duczynski. Hybrid warfare and disinformation: A Ukraine war perspective. Wiley, 2023. https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13257

[7] DGAP Policy Brief (Nov 2025). European Security in the Era of Hybrid Warfare, https://dgap.org/en/research/publications/european-security-era-hybrid-warfare

Low resilience of Lithuanian society to crises

A study conducted by researchers at the Faculty of Social Sciences, Arts and Humanities at Kaunas University of Technology revealed that although Lithuanian residents have some knowledge[8] about crisis preparedness, it is insufficient. For example, only 14% of respondents know where the nearest evacuation routes are. A small proportion of respondents know how to prepare their homes (35%), what forms of civil resistance exist (26%), or how to behave if mobilization is declared (24%).

The knowledge economy is usually described using the triple helix model, which characterizes the interaction between science, business, and government in the innovation process. However, when discussing defense innovation in a global context and in the geopolitical situation of Lithuania, it is necessary to include a fourth component: society.

A properly prepared society becomes a powerful force in deterring and repelling enemy attacks, both in virtual space and in reality. In Finland, civilians and civil organizations play an important role in strengthening society's resilience[9] to crises, while in Israel, public security needs are incorporated into public regulation and legislation. Similar examples can be found in other countries.

Globalization and technological progress have created closely interlinked economic, social, and infrastructural systems. As a result, even local disruptions can quickly spread across sectors and countries, turning into cascading crises – a phenomenon that risk management researchers have been analyzing for almost a decade. As daily life becomes increasingly dependent on critical infrastructure, such crises can disrupt energy, communications, logistics, or food supply chains. In such circumstances, strengthening societal resilience becomes essential for national security.

[8] Balžekienė, Aistė; Budrytė, Paulina; Pelikšienė, Rūta; Telešienė, Audronė; Vitkauskaitė-Ramanauskienė, Jonė, 2026, "Crisis Preparedness and Societal Resilience, October 2024", https://hdl.handle.net/21.12137/4DZYRL, Lithuanian Data Archive for SSH (LiDA), V1, UNF:6:vFxWC4spSkSKKqsNy2ZC3g== [fileUNF]

[9] https://intermin.fi/en/rescue-services/preparedness

Development of a defense innovation ecosystem

In the near future, Lithuania needs to create the foundations for a functioning defense innovation ecosystem – clear processes, responsible structures, and pilot programs that allow for a quick transition from idea to prototype. This would include **a one-stop shop** for idea submission and funding, including the implementation of low-risk idea development and prototype testing mechanisms, a rapid prototype development funding scheme, and dual-use technology priorities.

At the same time, it is necessary to ensure **the systematic return of war experience and expert knowledge to the innovation cycle**, actively involving reserve officers, defense experts, and other professionals with field experience. **Targeted educational programs** are needed – from defense literacy and critical thinking to innovation implementation in the military – to ensure that the technologies and solutions developed meet real operational needs.

Development of critical technologies and infrastructure

Unmanned platforms and **countermeasures, optoelectronics and photonics, mechatronics**, and **biotechnology** could become the quick-start areas in which Lithuania has real potential to specialize and become a leader. Prioritization would not only allow for the effective development of defense solutions, but also for the practical resolution of today's threats – for example, preventing the intensive smuggling carried out by Belarus using weather balloons and drones.

The development of dual-use technologies should become one of the main objectives and evaluation criteria of state R&D&I programs. In this context, it is necessary to support scientific and academic institutions as well as small and medium-sized enterprises by providing access **to funding from the early stages of technological readiness** (e.g., from TRL 2-3) through simplified schemes (the logic of the US SBIR/STTR programs[10] can be taken as a good practice example). This would allow innovations to move quickly towards prototyping and testing.

Innovation **ideas based on battlefield experience** must be given priority, as they directly address the challenges of the real battlefield and generate the greatest impact.

Europe lacks the infrastructure to test air defense, autonomous, electronic warfare, and long-range systems. Lithuania, with its more open spaces and rapidly growing unmanned platform development sector, can fill this niche and create **testing grounds**.

[10] https://www.sbir.gov/about

It is recommended to promote innovation in defense products based on alternative materials from local raw materials and the latest manufacturing technologies to involve more regional industry in supply chains and expand **production capacity and scale**.

It is necessary to continue strengthening Lithuania's transport infrastructure at a rapid pace – the Rail Baltica railway, Via Baltica, and other highways – and transform railways and roads into **multimodal transport corridors** by expanding electricity distribution, communications (optical fiber, mobile base stations) networks, and logistics support capabilities in their areas. This is important for both military and civil mobilization in the event of war.

Strengthening cyber security

Considering the Government's planned priorities, the following investment proportions are proposed for cyber security in 2025–2030: 35% for cyber resilience, 30% for technological platforms (state hybrid cloud, eID, data governance), 20% for information defense (early warning and takedown mechanisms), and 15% for the innovation ecosystem (artificial intelligence sandboxes, innovation procurement, defense industry clusters).

During the first stage, it is proposed to create a sectoral mesh-type **security operations center** in the energy and transport sectors, to implement a **hybrid cloud** landing zone environment with resilient recovery tests, to create **a model for eID interaction with strong encryption guidelines**, and to carry out pilot programs **for encryption migration**. Supply chain security measures should also be implemented, and **an information defense chain** should be created for election and crisis periods. The national cyber range should be integrated with the SOC network to shorten response times and close detected gaps more effectively.

These systemic steps would help avoid institutional fragmentation and allow for progress towards a unified, cross-sectoral architecture.

Strengthening information resilience

It is recommended to strengthen the capacity to identify and remove misinformation, and to create a **national information space monitoring** and rapid response system both in Lithuania and in the diaspora. **Fact-checking** and **counter-narrative teams** should be formed for periods of crisis and elections, involving the cultural and creative industries sector, and **information literacy training** should be organized for target groups in society. A protocol for protecting influential figures from account hijacking and a coordinated communication mechanism **at the government level with social media platforms** are also necessary.

GUIDELINES (5–10 YEARS)

In the long term, Lithuania needs to transform its defense innovation ecosystem into a coordinated, **trust-based "quadruple helix" model**, in which government, business, academia, and society operate as an integrated system. This requires a national defense innovation chain – from idea to market – with shared infrastructure, testing platforms, interagency coordination, and a policy-making culture that encourages competition. The strategic ambition is to create a European-scale integrated defense innovation ecosystem in which new solutions could be transferred from early-stage ideas to field testing in a matter of months rather than years.

Long-term strengthening of defense capabilities should be based on **public-private partnerships**, with the state taking a significant (around 50%) share of the capital for the development of dual-use technologies and production capabilities. To ensure the country's ability to dynamically increase production volumes during crises, it is necessary to consistently develop Lithuania's industrial capabilities and create clear areas of specialization.

To this end, it is necessary to highlight and strengthen the role of **Lithuania's engineering industry** – mechanical, electronic, optical, mechatronic, and manufacturing engineering companies. These sectors form the backbone of defense innovation: they develop prototypes, manufacture critical components, maintain the functioning of supply chains, and ensure capacity expansion during crises. Without the consistent integration of this sector into the national innovation chain, it is impossible to create a functioning dual-use technology cycle or achieve the scale of production required in the event of war.

In the long term, it is necessary to strengthen the resilience of logistics and infrastructure: develop diverse and sustainable logistics channels, build up strategic reserves, strengthen electricity and communications networks, expand multimodal corridors on railways and roads, and ensure alternative supply routes.

In the long term, Lithuania needs to ensure **a secure sea route to the West**, which would become the main channel for supplying allied forces and supplies in the event of war if the Suwalki Corridor were disrupted. This requires capabilities to maintain secure sea lines: anti-mine vessels, air defense, coastal surveillance solutions, infrastructure, and modern autonomous maritime (surface and underwater) infrastructure monitoring and logistics systems.

A particularly promising solution is the integration of autonomous and remotely controlled surveillance and attack **unmanned platforms** for the protection of this route and the organization of logistics, based on Ukraine's experience in neutralizing the Black Sea fleet. This is one of the few technologies that allows a small-capacity state to compensate for its lack of conventional military power.

Lithuania's scientific and engineering base can be used to develop navigation and maritime situational awareness technologies that are resistant to GNSS jamming. Such technologies are critical to the security of the maritime corridor and could become a long-term area of specialization for Lithuania.

In addition, it is recommended to develop at least medium-range **offensive technologies**, as Lithuania's relatively small strategic depth requires defensive capabilities that allow for effective counterattacks and the transfer of the theater of operations to the opponent's territory.

In the field of cybersecurity, it is planned to achieve universal SOC network coverage by 2030, integrate OT event monitoring and dark web intelligence, ensure that all critical systems use NIST, ISO, and ETSI standards, and that digital platforms meet the criteria for mature hybrid cloud computing. Coordination of the public security sector should be carried out by the Ministries of the Interior and National Defense of the Republic of Lithuania, applying portfolio management principles and regular "stop-go-fix" reviews.

The long-term goal in the information space is universal information maturity, where information literacy and critical thinking are integrated into the education system at all levels. Lithuania should create a robust system **for protecting democratic processes**, audited before elections, and a model **for civil and military cooperation** that encompasses the cultural sector, creative industries, and communities. The state's leadership in communication should ensure dominance in the information space and offensive communication that strengthens the national reputation.

International practice shows that **the diaspora** can become an important link in information resilience: citizens living abroad can be involved in threat monitoring and strategic communication, with volunteer networks being relied upon in the information war.

Finally, in strengthening public resilience, the long-term goal is to integrate defense and citizenship education at different levels of education, develop systems for training reservists and officers, and actively involve reserve officers and experts with military experience in innovation, education, and strengthening the public sector.

STRATEGIC COOPERATION AND COORDINATION

It is proposed to establish **an Army Innovation Office (AIO)**, whose main functions would include inter-agency coordination for effective communication between ministries, scientific institutions, business and industry (see Figure 1). The AIO would systematically collect real operational needs, translate them into clear technological tasks, and pass them on to industry and researchers. Such an office would serve as a central hub in the national innovation chain, ensuring that innovation development starts from battlefield experience – technologies that actually increase survivability, mobility, and effectiveness. This is a common practice in advanced defense ecosystems (Israel, Finland, the US), where the innovation cycle is based on feedback from soldiers and officers.

The Army Innovation Office would help address the challenge of fragmentation in the defense innovation ecosystem and facilitate communication with partner organizations such as NATO DIANA, key armaments working groups NAAG, NNAG, NAFAG, centers of excellence COE, STO, and NIAG. In addition, the NATO Innovation Fund (NIF) and the European Defense Fund (EDF) finance those ecosystems that can operate together as platforms rather than as individual institutions. Lithuania has a unique opportunity to become part of such a model, but this requires **a national coordinator** capable of integrating Lithuania's R&D potential into NATO's innovation and armaments development and standardization networks.

Regional cooperation is another critical component. Joint pilot projects with Estonia, Latvia, Poland, and Finland would accelerate testing, reduce unit costs, and create a Baltic defense innovation cluster – a practice already used by the Nordic countries and Israel. Cooperation between science, innovation, and industry can also encourage deeper cooperation in the development of defense technologies and capabilities, as well as joint procurement.

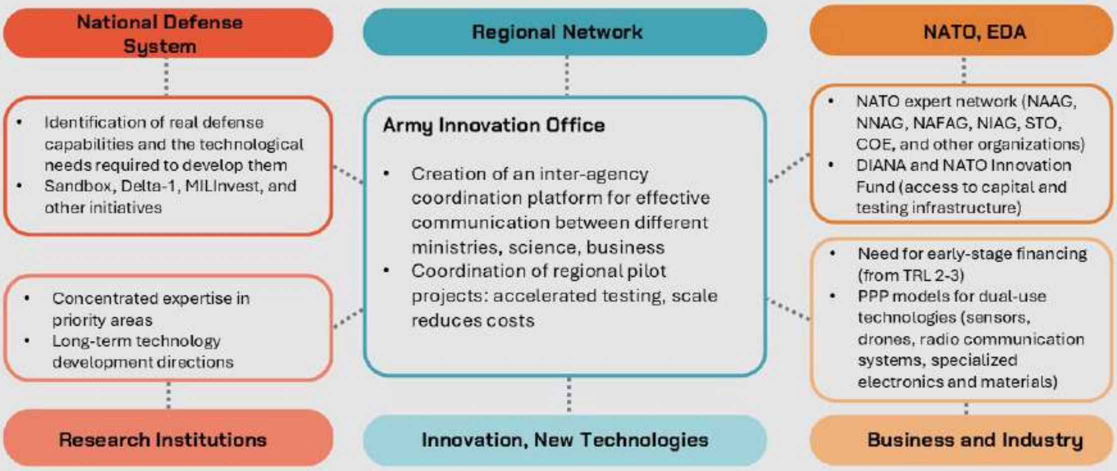

National Defense System
Identification of real defense capabilities and the technological needs required to develop them
Sandbox, Delta-1, MILInvest, and other initiatives
Concentrated expertise in priority areas
Long-term technology development directions
Research Institutions
Regional Network
Army Innovation Office
Creation of an inter-agency coordination platform for effective communication between different ministries, science, business
Coordination of regional pilot projects: accelerated testing, scale reduces costs
Innovation, New Technologies
NATO, EDA
NATO expert network (NAAG, NNAG, NAFAG, NIAG, STO, COE, and other organizations)
DIANA and NATO Innovation Fund (access to capital and testing infrastructure)
Need for early-stage financing (from TRL 2-3)
PPP models for dual-use technologies (sensors, drones, radio communication systems, specialized electronics and materials)
Business and Industry

Fig. 1. Scheme of strategic cooperation and coordination in the defense innovation ecosystem

1

AUTHORS AND EXPERTS

Prof. Dr. Edita Gimžauskienė	Vice-Rector for Strategic Partnerships, Kaunas University of Technology
Prof. Dr. Monika Petraitė	Principal Investigator, Innovation and Entrepreneurship Research Group, Faculty of Economics and Business, Kaunas University of Technology
Prof. Dr. Šarūnas Grigaliūnas	Head of the Cyber Security Competence Center, Kaunas University of Technology
Dr. Artūras Medeišis	Dean of the Faculty of Electronics, Vilnius Gediminas Technical University
Dr. Andrius Vilkauskas	Senior Researcher at the Mechatronics Institute, Faculty of Mechanical Engineering and Design, Kaunas University of Technology
Paulius Vaitkevičius	Head of Innovation and Products in the Programming Division at Novian
Peter Nielsen	Independent Member of the Board of Lithuanian Railways
Dr. Simona Pūkienė	Science and Innovation Advisor at the Ministry of National Defense of the Republic of Lithuania
Tadas Gudėnas	Innovation Expert at the Lithuanian Armed Forces
Dr. Una-May O'Reilly	Head of the Anyscale Learning for All (ALFA) Group at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)
Dr. Kevin P. O'Brien	MIT Electrical Engineering and Quantum Technologies Expert

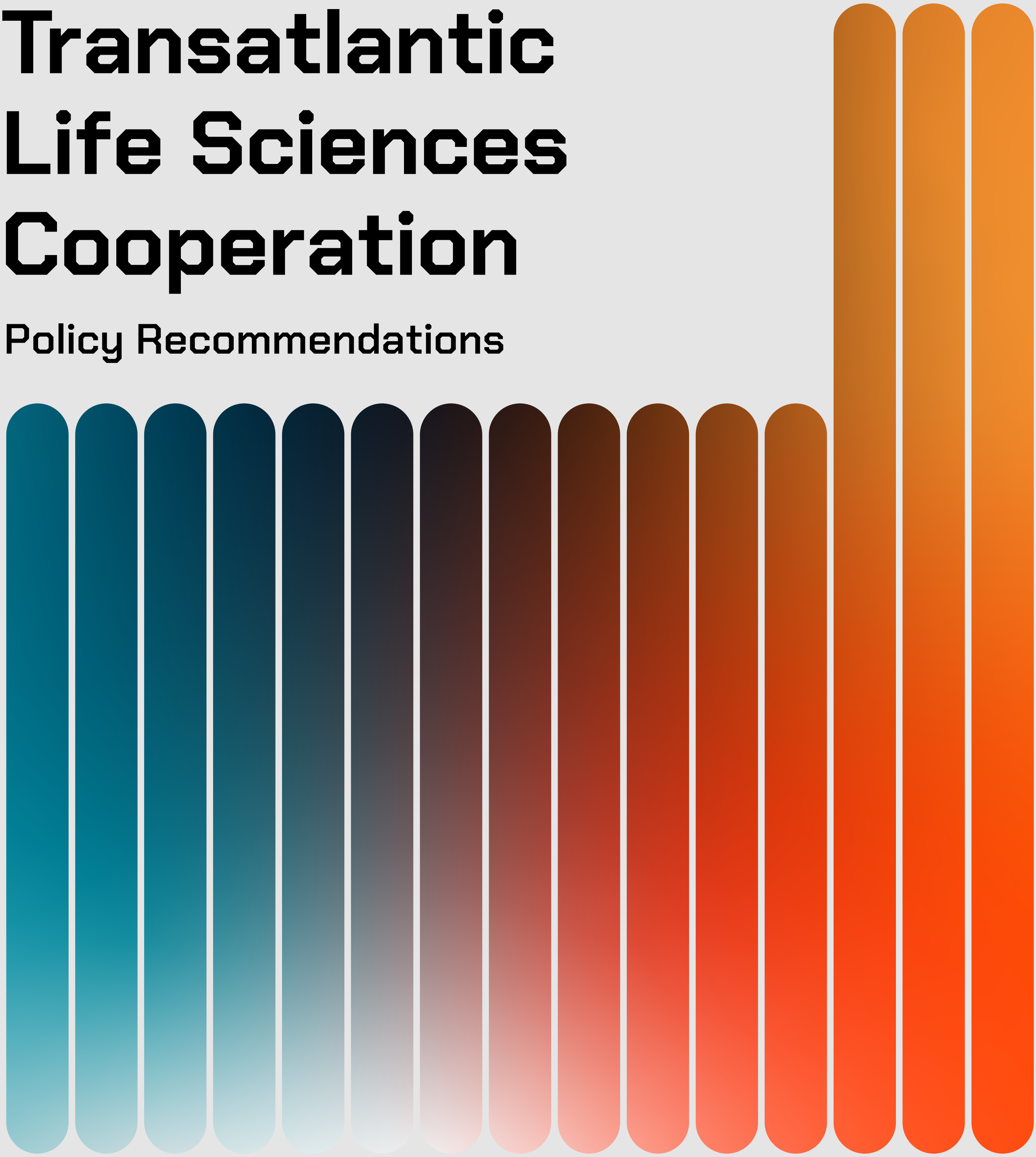
Human and More-Than-Human Futures: Innovating Technologies for Coexistence

Together with MISTI Lithuania

Vilnius University

Transatlantic Life Sciences Cooperation

Policy Recommendations



Prepared by the MISTI Lithuania consortium for Lithuania’s cooperation with MIT, with the participation of representatives from Lithuanian business, academia, venture capital, and the public sector

ABSTRACT

This white paper outlines a strategic framework for strengthening transatlantic collaboration in the life sciences, drawing on insights from the CiLSC introductory document, group discussion outputs, and a comparative analysis of EU–US research environments. The recommendations aim to accelerate innovation, enhance mobility and institutional openness, and create sustainable mechanisms for long-term cooperation.

STRATEGIC CONTEXT

Cooperation between Lithuania, the EU, and the United States is shaped by significant structural differences: EU research funding remains predominantly top-down and highly regulated, whereas US systems tend to be bottom-up, faster, and more flexible. Collaboration often relies on personal networks rather than stable, institutional frameworks. Meanwhile, technology development—especially in areas such as GMO and NGT—is significantly more dynamic in the US, creating both opportunities and asymmetries.

To bridge these gaps, Lithuania requires instruments that support agile, researcher-driven initiatives, institutional alignment, and strong international partnerships, enabled by modern funding, mobility, and talent-attraction mechanisms.

STRATEGIC THEMES

- Creating stable EU–US collaboration pathways through diversified funding (BAFF, MISTI-Lithuania, ILTE, NATO programs).
- Supporting bottom-up, researcher-led cooperation rather than exclusively institutional agreements.
- Facilitating rapid seed funding, mobility schemes, and private co-investment to accelerate innovation.
- Reducing regulatory and cultural barriers to collaboration, including increasing visibility of EU institutions.
- Establishing shared digital tools and platforms for scientific partnering, visibility, and mission-driven projects.

SCIENCE COOPERATION PLATFORM

The Science Cooperation Platform is a digital environment designed to match researchers, students, and industry partners based on research interests, available infrastructure, methods, and collaboration needs. It creates structured and transparent opportunities for cooperation, reducing reliance on sporadic personal contacts.

Key functions include:

- profiles detailing expertise, facilities, and collaboration interests;
- algorithm-based partner recommendations;
- integrated access to calls, seed grants, and joint programs;
- institutional contact-point support and science managers facilitating collaboration;
- mission-oriented project spaces aligned with Lithuanian, EU, and global priorities.

POLICY RECOMMENDATIONS

A. Diversified and Flexible Funding Models

1. Establish fast-turnaround LT–US Seed Grants enabling early-stage collaboration, shared-use of infrastructure, and exploratory research.
2. Strengthen cooperation through existing programs such as BAFF, MISTI, ILTE, and NATO by developing co-funded calls focused on high-impact life sciences.
3. Create public–private mechanisms for pilot projects, including spin-off scholarships and risk-tolerant grants for ambitious interdisciplinary ideas.
4. Incentivize private-sector co-investment in early-stage biotechnology and deep-tech innovations.

B. Strengthening Institutional Cooperation Frameworks

1. Appoint institutional science cooperation officers responsible for coordinating collaborations, building networks, and supporting applications.
2. Develop a national database of life science research topics, infrastructures, and expertise to facilitate strategic matchmaking.
3. Expand joint doctoral programs, mission-driven research clusters, and parallel laboratory models to strengthen long-term collaboration.
4. Promote long-term internships, research rotations, and infrastructure-sharing agreements with US institutions.

C. Kultūra, talentas ir matomumas

1. Strengthen support for commercialization through patenting assistance, IP management training, and institutional patent funds.
2. Create talent-attraction packages such as funded PhD positions, tenure-track schemes, and start-up research packages for returning scientists and international recruits.
3. Recognize diverse forms of academic achievement (e.g., internationalization, education contributions, business collaboration) alongside traditional metrics.
4. Encourage student-driven innovation through mission-based challenges, hackathons, and virtual conferences.

LONG-TERM VISION (5–10 YEARS)

- Institutionalized EU–US co-funded collaboration frameworks with stable annual calls.
- Mission-based research clusters addressing climate resilience, synthetic biology, and health.
- Fully operational Science Cooperation Platform integrated across Lithuanian institutions.
- Strong spin-off ecosystem supported by coordinated patenting, mentoring, and investment pathways.

FIRST-MILE STEPS (12–18 MONTHS)

- Launch the Science Cooperation Platform (alpha version) and host initial matchmaking events.
- Appoint institutional cooperation officers and begin developing the topic database.
- Organize a student-driven mission challenge with MIT partners.

AUTHORS AND EXPERTS

Prof. Dr. Eglė Lastauskienė	Director of the Institute of Biosciences at the Life Sciences Center of Vilnius University, Professor, Chair of the VU Senate
Prof. Dr. Arvydas Lubys	Director of the Life Sciences Center of Vilnius University
Prof. Dr. Hadley Sikes	Willard Henry Dow Professor of Chemical Engineering, Massachusetts Institute of Technology (USA)
Dr. Gytis Dudas	Chief Researcher at the Life Sciences Center of Vilnius University
Dr. Gintaras Brazauskas	Director of the Lithuanian Research Centre for Agriculture and Forestry, Chief Researcher
Assoc. Prof. Dr. Viktorija Vaštakaitė-Kairienė	Deputy Director for International Relations at the Bioeconomy Research Institute, Agriculture Academy of Vytautas Magnus University
Dr. Vidmantas Bendokas	Deputy Director for the Institute of Horticulture at the Lithuanian Research Centre for Agriculture and Forestry, Senior Researcher

The Lithuanian Consortium

Euromonitor International

ignitis grupė

ktu 1922 kauno technologijos universitetas

Klaipeda University

LAMMC LITHUANIAN RESEARCH CENTRE FOR AGRICULTURE AND FORESTRY

LITHUANIAN ENERGY INSTITUTE

LTG

NOVIAN

Vilnius Academy of Arts

VILNIUS TECH Vilnius Gediminas Technical University

VILNIAUS UNIVERSITETAS · 1579 · UNIVERSITAS VILNENSIS · Vilnius University

VYTAUTI MAGNI CAUNAE UNIVERSITAS VYTAUTAS MAGNUS UNIVERSITY MCMXXII

The activities of the Lithuanian consortium are supported by

RCL

Research Council of Lithuania