#79 - POLICY PAPER

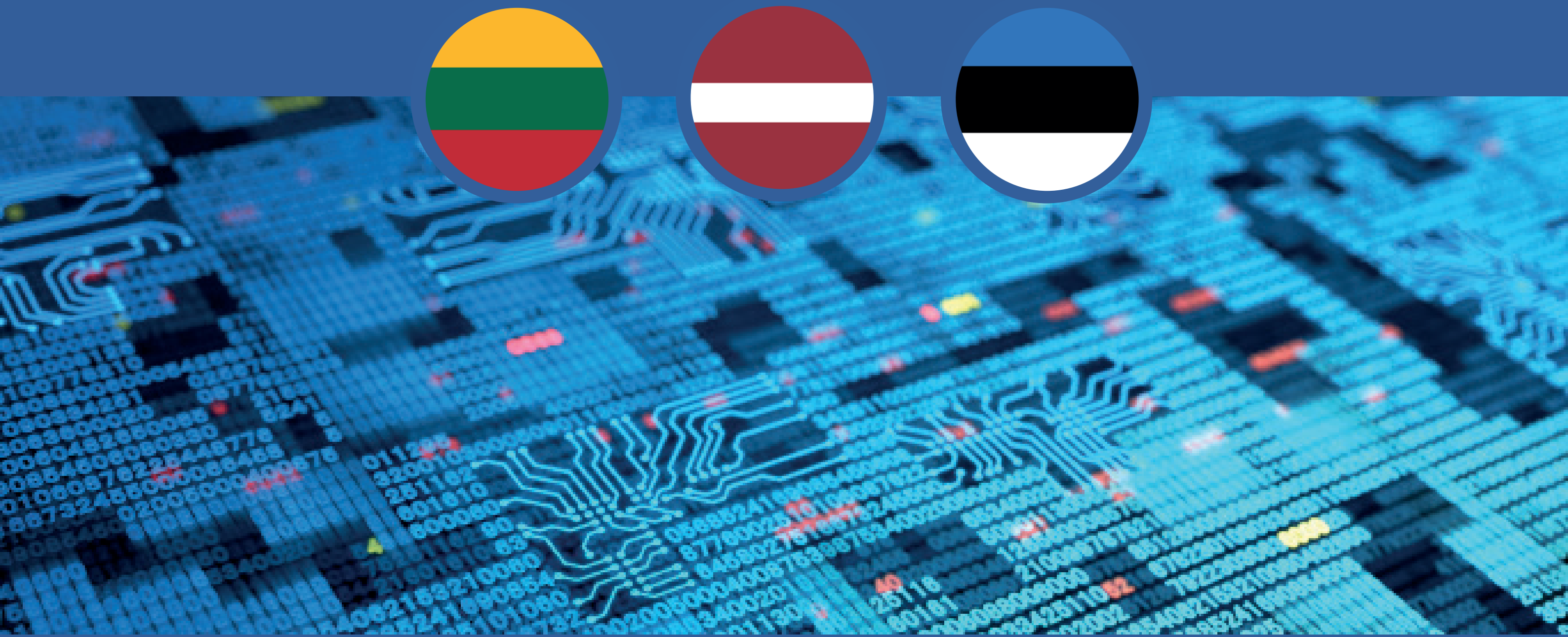
ARES
Armament Industry
European Research
Group

CRITICAL TECHNOLOGIES AND INDUSTRIAL CAPABILITIES: NATIONAL DEFINITION AND POLICY IMPLICATIONS

The case of Baltic States

Prof. Margarita Šešelgytė / Director of the Institute of International Relations and Political Science, Vilnius University
Emilė Indrašiūtė / PhD student at the Institute of International Relations and Political Science, Vilnius University

January 2023



The views expressed here are solely those of the authors. They do not reflect the views of any organisation.

ABOUT THE AUTHORS

Prof. Margarita Šešelgytė / Director of the Institute of International Relations and Political Science, Vilnius University

Emilė Indrašiūtė / PhD student at the Institute of International Relations and Political Science, Vilnius University

ARES
Armament Industry
European Research
Group

The Armament Industry European Research Group (Ares Group) was created in 2016 by The French Institute for International and Strategic Affairs (IRIS), who coordinates the Group. The aim of the Ares Group, a high-level network of security and defence specialists across Europe, is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.

CONTACT [PILOTS]
Jean-Pierre Maulny, Federico Santopinto, Olivier de France, Sylvie Matelly
ares@iris-france.org
+33 (0)1 53 27 60 60

iris-france.org/ares
#ARESGroup

@AresGroup_EU

ARES Group - EU

ABSTRACT

The way the Baltic States define, assess and develop critical technologies and their industrial capabilities is very much affected by their smallness in terms of capabilities and the size of the defence industrial sector as well their security environment. Critical technologies are inextricably linked to ensuring the security and operability of critical infrastructure. The development of critical technologies in Lithuania, Latvia and Estonia, therefore, depends on the identified vulnerabilities of critical infrastructure. All three Baltic states have limited defence industries which are mostly focused on dual-use products. The main players in the industries are private small and medium-sized enterprises which have slim chances of competing with France or Germany's counterparts. Key challenges for all three Baltic states mostly derive from the external security environment rather than natural disasters or other threats such as terrorism (apart from frequently occurring cyberterrorism). Russia's war of aggression against Ukraine has reinforced the aspiration to increase defence capabilities and ensure the security of the critical infrastructure.

This paper focuses on five main questions: how the Baltic States define their critical technologies, what monitoring mechanisms are in place, how they tackle potential dependencies, how national mechanisms are coordinated with the EU, and finally, how the war in Ukraine has impacted the understanding of the security of the critical infrastructure.

Keywords: Baltic States / Critical Technology / Critical infrastructures / Defence Industrial Policy / European Union / Foreign Direct Investments regulation / Innovation

DEFINITION OF CRITICAL TECHNOLOGIES IN THE BALTIC STATES

Although Baltic States perceive their security environment in the same way,[1] they tend to define their critical technologies in a somewhat different manner: while Lithuania has elaborated its own national definitions, Latvia and Estonia follow the definition set by the EU.

The main document defining critical technologies in Lithuania is a resolution on the Methodology of identifying objects of critical security (2018). It obliges various ministries and other government institutions to identify objects of the highest importance for the security of Lithuania.[2] Critical technologies as a whole are broadly defined as "a service whose inactivity or disruption would have a significant negative impact on national security, the national economy, or the national or public interest."[3] On a more particular note, the National Security Strategy (NSS) sets the goal of independence from Russia in the energy sector and mentions threats related to transformative technologies, particularly cybersecurity.[4] Civil-military cooperation in the area of military innovation is defined as key in order to 'create conditions for enhancing the competitiveness of the sector and fostering innovation'.[5]

Building on the NSS, as well as military priorities identified by the institutions, guidelines for the development of defence industrial capabilities are set. The current list of priorities include cybersecurity, energy security, military mobility and drone development, with a strong emphasis on dual-use products. [6,7]

The Latvian National Security Law sets a list of physical infrastructure objects defined as critical infrastructure; it also identifies cybersecurity systems and counterterrorism activities as important areas. The current definition mostly relies on a Directive on European critical infrastructure, as well as the concept of "services," in order to constitute a comprehensive,

[1] Masha Hedberg and Andres Kasekamp, "Baltic States," in *The Handbook of European Defence Policies and Armed Forces,* ed. Hugo Meijer and Marco Wyss, Oxford University Press, 2018, 214-230.

[2] Seimas of the Republic of Lithuania, Regarding the Government of the Republic of Lithuania in 2018 August 13 resolution no. 818 "On approval of the National Cyber Security Strategy" amendment, 2018. [retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce]

[3] Ibid.

[4] Resolution regarding the Seimas of the Republic of Lithuania Resolution of May 28, 2002 NO. Amendment IX-907 On the Approval of the national Security Strategy, 2021. [retrieved from: https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=124aazcfpq&actualEditionId=zDQFzPCLKi&documentId=TAIS.167925&category=TAD]

[5] Ibid.

[6] Interview with the director of the Defence Materiel Agency under the Ministry of National Defence of Lithuania Sigitas Dzekunskas and head of Department of Research and Technologies of the Defence Materiel Agency under the Ministry of National Defence of Lithuania Laurynas Mockaitis, November, 2022.

[7] The Minister of Defence of Lithuania Arvydas Anušauskas, "Gynybos pramonės ir krašto apsaugos sistemos bendradarbiavimo perspektyvos", 7 November, 2022. [retrieved from: https://www.lrt.lt/naujienos/pozicija/679/1814302/arvydas-anusauskas-gynybos-pramones-ir-krasto-apsaugos-sistemos-bendradarbiavimo-perspektyvos]

EU-aligned notion of critical infrastructure.[8] Strengthening the defence industrial sector is specified as one of the most important aims of defence policy in the Latvian National Defence Concept for 2020-2024.[9] The priorities are set largely taking into account the needs of the military and are mostly concentrated in the areas of electronic warfare, cyber capabilities, communications, and machine building, which includes manufacturing machine components, electrotechnical articles, steel and other metal structures. These military needs are closely interconnected with the development of national defence technologies, and are the main factor for further development direction.[10]

Estonia also employs the EU definition, outlined in the Council Directive 2008/114/EC, to define its critical infrastructure, which is reiterated by the Estonian Information System Authority (RIA). According to the directive, 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the main-tenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[11] The Estonian National Security Concept (NSC), published in 2017, expands this definition, mostly concentrating on military readiness and cybersecurity.[12] Arguably, the document does not entirely correspond to the latest changes in the security environment as it was released 5 years before the war in Ukraine took place, therefore, in Estonia, understanding of the security of the critical infrastructure is situational.

Although the three Baltic have more or less similar threat assessments,[13] their definitions of critical technologies slightly differ, Latvia and Estonia tend to rely more on the EU directive, whereas Lithuania has developed a national one. The guidelines on critical technologies both in Latvia and Lithuania are closely connected to the needs of the national defence forces, thus providing a basis for consistent capability development planning, whereas the Estonian National Security Concept has not been updated recently and therefore fails to connect critical infrastructure challenges with capability development progress.

[8] Evija Djatkoviča and Maris Andžans, "Latvia: Entangled system-in-progress amidst terrorism, Russia and cyberthreats", in *Critical infrastructure in the Baltic states and Norway: Strategies and practices of protection and communication*, ed. Maris Andžans, Andris Sprūds and Ulf Sverdrup (Latvian Institute of International Affairs, 2021), 39-41.

[9] The Ministry of Defence of Latvia, "Saeima approves the National Defence Concept," 2020. [retrieved from: https://www.mod.gov.lv/en/news/saeima-approves-national-defence-concept]

[10] Ministry of Defence of the Republic of Latvia, Military capabilities. [retrieved from: https://www.mod.gov.lv/en/nozares-politika/comprehensive-defence/military-capabilities]

[11] Information System Authority of the Republic of Estonia, Critical Information Infrastructure Protection CIIP. [retrieved from:https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html]

[12] Estonian Ministry of Defence, National Security Concept, 2017. [retrieved from: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf]

[13] Masha Hedberg and Andres Kasekamp, "Baltic States," in *The Handbook of European Defence Policies and Armed Forces,* ed. Hugo Meijer and Marco Wyss, Oxford University Press, 2018, 214-230.

MONITORING CRITICAL TECHNOLOGIES AND INDUSTRIAL CAPABILITIES, AND TACKLING POTENTIAL DEPENDENCIES

Monitoring processes related to the critical technologies and industrial capabilities in Baltic states are somewhat similar in the field of cyber and information security, however, slightly differ in the domain of physical systems of critical infrastructure.

A critical infrastructure protection system in Lithuania has been developing while Lithuania was preparing for the EU and NATO membership.[14] In the top-down approach, the Government of Lithuania designates specific sectors to related ministries (e.g. Ministry of National Defence) or other national institutions (e.g. National Cyber Security Centre), which then occasionally monitor the previously listed objects of strategic importance. At most, every two years, the responsible institutions must review the operation of objects of critical infrastructure unless the operators of the objects inform the responsible institutions of any changes regarding the object. The objects of strategic importance fall into sectors of energy, transport, information technologies, telecommunications and other high technologies, finance and credit, and military equipment.[15] The war in Ukraine, as well as earlier Russian acts of aggression in Georgia and Ukraine, has brought to attention several dependencies on Russia in the domain of critical energy infrastructure, for instance, connection to the Russian Federation-run BRELL electricity grid.[16] Another area that has attracted increased attention is information security. In 2021 Lithuanian policymakers almost doubled the number of critical infrastructure service providers which were obliged to implement cybersecurity-oriented and other organisational compliance requirements.[17] Monitoring of industrial capabilities in Lithuania is ensured through regular communication between the Ministry of National Defence and defence industry. The Ministry of National Defence collects information on what resources are available and coordinates cohesion between the needs of the military and the products and services provided by private enterprises, including SMEs. Lithuania has quite a rigid scrutiny related to the defence procurement, particularly when it involves Foreign direct investments (FDI). A stiff list of requirements regarding the acquisition of security and

[14] Ramūnas Vilpišauskas, "Lithuania: Regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences", in *Critical infrastructure in the Baltic states and Norway: Strategies and practices of protection and communication*, ed. Maris Andžans, Andris Sprūds and Ulf Sverdrup (Latvian Institute of International Affairs, 2021), 60-62.

[15] Ibid, 71-80.

[16] The Ministry of National Defence of the Republic of Lithuania, "Baltic power supply grid resilience against hybrid attack rehearsed in Vilnius", 2021. [retrieved from: https://kam.lt/en/baltic-power-supply-grid-resilience-against-hybrid-attack-rehearsed-in-vilnius/]

[17] The government office of the Republic of Lithuania, "Vyriausybei išplėtus ypatingos svarbos informacinės infrastruktūros sąrašą, daugiau įmonių privalės skirti ypatingą dėmesį savo kibernetinio saugumo užtikrinimui," 2021. [retrieved from: https://lrv.lt/lt/naujienos/vyriausybei-ispletus-ypatingos-svarbos-informacines-infrastrukturos-sarasa-daugiau-imoniu-privales-skirti-ypatinga-demesi-savo-kibernetinio-saugumo-uztikrinimui]

defence-related products is set out in the Law of the Republic of Lithuania on public procurement,[18] which the Lithuanian Ministry of National Defence has to follow.

In Latvia, a system of critical infrastructure protection is specified by several laws,[19] and the processes of monitoring and protection involve multiple ministries (e.g. Ministry of Interior, Ministry of Defence), as well as security agencies and other institutions, such as Defence Intelligence and Security Service, Financial and Capital Market Commission, CERT.LV and others. It also overlaps with the civil protection system and makes it dependent on other national security and state defence sub-systems like the Emergency planning process which includes 13 Latvian ministries.[20] The responsibilities are clearly divided amongst various actors involved in the process, namely the Latvian Cabinet of Ministers, Ministry of Interior, State Security Service, Defence Intelligence and Security Service, Constitution Protection Bureau, CERT. LV, Ministry of Defence and certain sectoral ministries manage Critical infrastructure and European critical infrastructures, while CERT.LV and Digital Security Supervisory Committee under the Ministry of Defence manages Essential services and Financial and Capital Market Commission together with the Bank of Latvia are involved in managing the Critical financial services.[21] However, the system is a bit cumbersome which might affect the speed of response in a crisis: it is supervised by numerous state institutions, regulated by several laws and the components of the critical infrastructure maybe subject to several regulatory frameworks, such as civil protection system.[22] While the attention to specific objects, systems or parts of critical infrastructure allows monitoring and assessing concrete objects, considerable focus on the details might hamper the ability to grasp the broader picture. While protecting objects and systems, it also risks leaving behind the procedures of services these objects operate.[23] The protection system also includes private owners.[24] The security of the privately owned objects relies on the limited budgets of these private companies which might undermine the critical infrastructure protection system as a whole. NATO and the EU defence planning processes - NATO Defence Planning Process (NDPP) and

[18] The law of the Republic of Lithuania on Public procurement in the field of defense and security, 2011. [retrieved from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.402795/ZxtOdsEYSC]

[19] These laws include The National Security Law, Regulation No. 508 „Procedures for the Identification of Critical Infrastructure, Including European Critical Infrastructure and Planning and Implementation of Security Measures and Operational Continuity,“ The Law on the Security of Information Technologies, as well as Regulation No. 100 „Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies.“ The National Security Concept also addresses critical infrastructure and its protection.

[20] Evija Djatkoviča and Maris Andžans, "Latvia: Entangled system-in-progress amidst terrorism, Russia and cyberthreats", in Critical infrastructure in the Baltic states and Norway: Strategies and practices of protection and communication, ed. Maris Andžans, Andris Sprūds and Ulf Sverdrup (Latvian Institute of International Affairs, 2021), 49.

[21] Ibid, 44-49.

[22] Ibid.

[23] Ibid, 49-52.

[24] National Security Law of Republic of Latvia, United Nationas, Investment Policy Hub. [retrieved from: https://investmentpolicy.unctad.org/investment-laws/laws/237/latvia-national-security-law]

EU's Coordinated Annual Review on Defence (CARD) plays a strong role in Latvia in the field of critical technologies as understood from an interview with a Latvian defence industry expert,[25] as anticipation in the European Defence Fund (EDF), as well as The European Defence Industrial Development Programme (EDIDP) initiatives allows Latvian ministry of defence and other institutions to review the state of critical systems, as well as what local enterprises may provide for the security and defence of the country. At the national level, the government uses a closely supervised licensing process to track the developments in the defence industry.[26]

In the case of Estonia, the system of critical infrastructure protection is quite decentralised and does not have cohesive planning and monitoring mechanisms, but the Ministry of Interior plays a central role at the top of the policy planning level. Protection of privately-owned elements of critical infrastructure is to be ensured by their owners, and there is a lack of strong inter-institutional ties in order to provide security of the state-owned infrastructure.[27] However, despite a decentralised approach toward the protection of critical infrastructure, different actors, both public and private, responsible for particular sectors are well-informed and prepared to ensure security within the scope of their responsibility. Quite comprehensive strategy though exists in the domain of cybersecurity. The extensive, 22 day-long cyber attacks on commercial and government servers,[28] and the Estonian ID card crisis in 2011[29] have provided the impetus for building resilience in cyberspace. This resulted in ongoing high readiness to counter cyber threats, avert any harmful dependencies in cyberspace, and in establishing The NATO Cooperative Cyber Defence Centre of Excellence. Further monitoring of objects of strategic importance falls under the authorities organising the continuity of vital services (ETKA) and providers of vital services (ETO).[30] The ETKAs are to supervise and coordinate the continuity of vital services, while the ETOs notify ETKAs of interruptions and other information, implement measures preventing interruptions, and ensure the capabilities

[25] Interview with Elīna Egle-Ločmele, Chairperson of the Board of Federation of Security and Defence Industries of Latvia (FSDI Latvia), November 2022.

[26] Ibid.

[27] Interview with Tomas Jermalavičius, Head of Studies and Research Fellow at the International Centre for Defence and Security (ICDS), Estonia, October 2022.

[28] Rain Ottis, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2018. [retrieved from: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf]

[29] Mihkel Kärmas, "Declassified documents reveal ID-card crisis from decade ago," ERR News, 2021, [retrieved from: https://news.err.ee/1608415676/declassified-documents-reveal-id-card-crisis-from-decade-ago]; Interview with Tomas Jermalavičius, Head of Studies and Research Fellow at the International Centre for Defence and Security (ICDS), Estonia, October 2022.

[30] Ivo Juurvee and Ramon Loik, "Estonia: building resilience through vital service providers", in *Critical infrastructure in the Baltic states and Norway: Strategies and practices of protection and communication*, ed. Maris Andžans, Andris Sprūds and Ulf Sverdrup (Latvian Institute of International Affairs, 2021), 27-30.

to guarantee quick restoration of services in case of emergencies.[31] However, this monitoring system includes only a short list of vital services indicated in the Emergency Act,[32] and omits a large lump of other critical security objects (e.g. national railways).

Small defence budgets and defence industries force Baltic states to thoroughly prioritise and to rely both on the private sector, as well as on international formats in order to ensure the safety of the infrastructure connected, which will be further explained in the next section of this paper. While the priorities in all three states for the last years were oriented towards cybersecurity, information, and energy security, the rising scope of hybrid threats requires constant re-evaluation and coordination both with national and private defence enterprises, as well as with the EU and NATO.

ALIGNMENT OF THE NATIONAL AND EU MECHANISMS, AND THE ROLE OF SMES

While the smallness of the Lithuanian, Latvian and Estonian defence budgets requires coherent planning and coordination with both the private sector and international formats. The critical infrastructure development and security is also closely connected to national and private defence companies and small and medium enterprises (SMEs) in the industry. For the three countries, developing critical infrastructure and technologies means a complex process, where on the one hand states have to cooperate and coordinate with local defence enterprises, and on the other hand, states must coordinate processes with international partners and alliances in order to achieve a better access to additional funding and projects. According to Elīna Egle-Ločmele, Chairperson of the Board of Federation of Security and Defence Industries of Latvia, even symbolic state grants for SMEs allow the enterprises to test their products in militaries and thus contribute to the development of critical technologies and defence capabilities. Furthermore, these defence enterprises may then enter the European arena and be involved in larger consortiums, thus strengthening the production of the defence capabilities even further. All three Baltic countries are members of both the EU and NATO, and take part in security and defence initiatives, such as the EDF, CARD, Capability Development Plans (CDP), Permanent Structured Cooperation (PeSCo), NDPP and others. Baltic states see new value added in PeSCo and also EDF, in particular as a framework to

[31] Ibid, 28.

[32] The Parliament of Estonia, *Emergency Act,* Riigi Teataja, 2017. [retrieved from: https://www.riigiteataja.ee/en/eli/513062017001/consolide]

develop new capabilities needed to address hybrid threats.[33] For instance, Lithuania participates in PeSCo projects related to military mobility and cybersecurity, the areas that have a direct impact on Lithuanian defence. Latvia, together with Estonia, also participates in the military mobility PeSCo project, as well as the Estonian-led "Integrated Unmanned Ground System" project. In the Call for Proposals for EDF in 2021, as a participant Latvia was listed in 5 projects, as opposed to Lithuanian involvement in 9 projects and Estonian - in 12.[34] The increasing involvement and overall positive response to the EU defence initiatives of all three Baltic states are to a large extent influenced by the changing security situation in the region, as well as increased defence needs and expanded defence budgets. Since 2017, Lithuania increased its military expenditure from 812.1 million USD to 1240.5 million USD in 2021,[35] Latvia - from 482.5 million USD to 826.6 USD,[36] and Estonia - from 537.4 million USD to 764 million USD in 2021.[37] Regional security environment however results in prioritisation of NATO planning processes over the EU.

Lithuanian Ministry of National Defence is involved in supporting local enterprises, including SMEs both participating in the EU defence industry and R&T development projects as well in national programs such as the Ministry of National Defence's Defence technology development program.[38] Both the Lithuanian government and the armed forces are actively involved in defence research. One of the priorities of The Ministry of National Defence of Lithuania is to integrate the Lithuanian defence industry into the EU initiatives by supporting local enterprises for them to take part in larger European consortiums. The main aim of this action is to firstly ensure the development of national security systems, and only secondly to bring profits.[39] The involvement of Lithuanian enterprises in the EU programs allows to better

[33] Margarita Šešelgytė, "Armament and Transatlantic Relationships: The Baltic States Perspective," Armament industry research group, 2019. [retrieved from: https://www.iris-france.org/wp-content/uploads/2019/11/Ares-47.pdf]

[34] Donatas Palavenis, "The Baltic States and the European Defence Fund: results for the first call available," The European Sting, 2022. [retrieved from: https://europeansting.com/2022/08/09/the-baltic-states-and-the-european-defence-fund-results-for-the-first-call-available/]

[35] Lithuanian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/lithuania/military-expenditure]

[36] Latvian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/latvia/military-expenditure]

[37] Estonian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/estonia/military-expenditure]

[38] The Ministry of National Defence of the Republic of Lithuania, "Krašto apsaugos ministro A. Anušausko komentaras: Gynybos pramonės ir krašto apsaugos sistemos bendradarbiavimo perspektyvos," 2022. [retrieved from: https://kam.lt/krasto-apsaugos-ministro-a-anusausko-komentaras-gynybos-pramones-ir-krasto-apsaugos-sistemos-bendradarbiavimo-perspektyvos/]

[39] The Minister of Defence of Lithuania Arvydas Anušauskas, "Gynybos pramonės ir krašto apsaugos sistemos bendradarbiavimo perspektyvos", 7 November, 2022. [retrieved from: https://www.lrt.lt/naujienos/pozicija/679/1814302/arvydas-anusauskas-gynybos-pramones-ir-krasto-apsaugos-sistemos-bendradarbiavimo-perspektyvos]

coordinate national supply with European demand, as well as to ensure faster advancement of Lithuanian SMEs in terms of developing new technologies.

There is close cooperation between the Latvian defence industry and the Ministry of Defence, which provides comprehensive aid for Latvian defence industries including SME's to participate in the EDIDP and EDF calls. The Latvian government plans to enhance the involvement of Latvian enterprises, research centres, and universities in the EU-funded mechanisms in the future.[40] The war in Ukraine has shed more light on the defence sector in Latvia which has opened more opportunities for SMEs to get financial assistance, thus allowing them to produce new technologies and get involved in more projects.[41] Even though Latvia currently does not lead any projects under the EU defence initiatives, it has high ambitions for increasing participation in projects regarding producing semiconductors and lasers, and enhancing cyber security and communication systems.

The EU initiatives, especially the EDF and the EDIDP are also well integrated in the Estonian defence industrial development action. The government co-funds and participates in various industry projects, the success of such involvement can be seen as the Estonian companies enrol in European defence R&D funding systems.[42] The Estonian defence budget has lately increased just as in other two Baltic countries,[43] allowing for more investment in research and defence industry development. The Estonian Ministry of Defence has been consistently contributing to national defence R&D in order to both promote innovation and increase export potential.[44]. The government itself has also increasingly contributed to the R&D activities.

[40] Interview with Elīna Egle-Ločmele, Chairperson of the Board of Federation of Security and Defence Industries of Latvia (FSDI Latvia), November 2022.
[41] Ibid.
[42] Defence Estonia, "The projects of Estonian defence industry companies received EUR 6 million from Europe," 2021. [retrieved from: https://defence.ee/news/the-projects-of-estonian-defence-industry-companies-received-eur-6-million-from-europe/]
[43] Estonian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/estonia/military-expenditure]; Latvian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/latvia/military-expenditure]; Lithuanian military expenditure, Trading Economics, source: SIPRI. [retrieved from: https://tradingeconomics.com/lithuania/military-expenditure]
[44] The ministry of Defence of the Republic of Estonia, Defence research and development. [retrieved from: https://riigikaitsareng.ee/en/defence-research-and-development/]

CONCLUSION AND STATE OF THE SECURITY ENVIRONMENT

Even though Lithuania, Latvia and Estonia have many similarities in how they define, monitor and develop critical technologies and how they cooperate with their defence industries, there are considerable differences among them related to the different architecture and different evolution of the infrastructure in each country. While Lithuania has the most updated national security strategy which encompasses hybrid threats and the need to secure critical infrastructure, Latvian and Estonian strategies still rely on older documents. The current geopolitical crises have enlightened some of the weak parts not only of the critical infrastructure itself, but also those of policies and crisis management processes. These weaknesses should be addressed in updated or reviewed strategies of securing the critical infrastructure in all three states, especially Latvia and Estonia. The development of critical technologies is directly linked to the definition of critical infrastructure and naming of its vulnerabilities, thus, a further investigation of current challenges in critical infrastructure may prompt advancements of critical technologies.

All three states have a top-down approach with government-designed lists of objects of critical infrastructure. Latvia stands out as one which has only objects and not services listed as critical for national security, and the Estonian list of objects and services is quite limited, whereas the Lithuanian list of critical infrastructure objects is relatively very extensive. The monitoring processes in Lithuania and Latvia seem to be similar, with both owners of objects of critical infrastructure, and certain government bodies, such as ministries or other institutions involved. In the Estonian case, even though there are agencies responsible for monitoring, the system is quite decentralised and lacks cohesion as a result of a large number of actors involved.

Table : Critical technologies : key findings : comparison Estonia, Latvia, Lithuania

	Estonia	Latvia	Lithuania
Definition of critical technologies What is considered critical technologies?	“Critical infrastructure” means an asset, system or part thereof located in Member States which is essential for the main-tenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.”	“Critical infrastructure” means an asset, system or part thereof located in Member States which is essential for the main-tenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.”	“A service whose inactivity or disruption would have a significant negative impact on national security, the national economy, or the national or public interest.”
Monitoring critical technologies and industrial capabilities: actors involved	Ministry of Interior, owners of the critical infrastructure elements, NATO Cooperative Cyber Defence Centre of Excellence, authorities organising the continuity of vital services (ETKA), providers of vital services (ETO).	The Latvian Cabinet of Ministers, Ministry of Interior, State Security Service, Defence Intelligence and Security Service, Constitution Protection Bureau, CERT. LV, Ministry of Defence and certain sectoral ministries, Digital Security Supervisory Committee under the Ministry of Defence, Financial and Capital Market Commission, the Bank of Latvia.	Specific sectors are designated to related ministries or other national institutions (e.g. National Cyber Security Centre).
Alignment of the national and EU mechanisms, and the role of SMEs	EU and NATO mechanisms well integrated in defence industrial development action. Estonia leads 1 PeSCo project. The government co-funds defence industry projects, Estonian enterprises actively enrol to European defence R&D funding systems.	Active involvement in EU and NATO mechanisms. Close cooperation between MoD and defence enterprises; the government provides comprehensive aid for local enterprises to participate in EDIDP and EDF calls. Latvia does not lead any projects under EU defence initiatives, but has ambitions for increasing participation.	Active involvement in both EU and NATO processes and mechanisms; the government supports SMEs in taking part in EU consortiums in order to strengthen the development of new technologies. Lithuania leads 1 PeSCo project.

Key texts / legislation / strategies	The Estonian National Security Concept (NSC) (2017), The Emergency Act (2017).	The Latvian National Security Law (2001, ed. 2022); the Latvian National Defence Concept for 2020-2024 (2020); Regulation No. 508 „Procedures for the Identification of Critical Infrastructure, Including European Critical Infrastructure and Planning and Implementation of Security Measures and Operational Continuity" (2021), The Law on the Security of Information Technologies (2013), Regulation No. 100 „Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies" (2011).	Resolution on the Methodology of identifying objects of critical security (2018); the National Security Strategy (NSS) (2021).

The war in Ukraine have had a major impact on threat assessment in all three Baltic states and affected several defence policy areas. It has also increased governmental support to the local defence industries and visibly raised private investment flows.[45] Importantly the war has also drawn attention to the specific technologies which might be developed locally, e.g drones.[46] These and other less sophisticated and relatively inexpensive, often dual-use products and systems might become a window of opportunity for relatively small defence industry companies of Baltic states which were facing a lot of limitations competing with vast defence industries of larger states. However, it should be noted that in general as defence planning is a long-term process the impact of the war in Ukraine on the main priorities of the development of industrial capabilities was not strongly influential.

Factors that will impact the future development of critical technologies in the Baltic states in include: the developments in the security environment, lessons learned from the war in Ukraine, increasing defence budgets and international programs, such as the EU's EDF, PeSCo,

[45] Interview with Elīna Egle-Ločmele, Chairperson of the Board of Federation of Security and Defence Industries of Latvia (FSDI Latvia), November 2022.

[46] Interview with Tomas Jermalavičius, Head of Studies and Research Fellow at the International Centre for Defence and Security (ICDS), Estonia, October 2022.

as well as NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the newly launched Innovation Fund. The three Baltic states, located in both EU and NATO's Eastern flank, seek not only more funding for innovations and the development of new technologies, but also put a strong emphasis on the current military and critical infrastructure-related needs. Even though both governments and local enterprises look forward to participating in various EU and NATO defence initiatives, in light of the war in Ukraine, the priorities remain on tackling the immediate threats to national security.[47]

[47] Interview with Elīna Egle-Ločmele, Chairperson of the Board of Federation of Security and Defence Industries of Latvia (FSDI Latvia), November 2022.

The Armament Industry European Research Group

ARES
Armament Industry
European Research
Group

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
ares@iris-france.org

iris-france.org/ares

The Armament Industry European Research Group (Ares Group) is a high-level network of security and defence specialists across Europe. Its aim is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.