Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 329-340

Business Actions Posing Threat to National Security

Violeta Vasiliauskienė
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
violeta.vasiliauskiene@go.kauko.lt

Anželika Banevičienė
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
anzelika.baneviciene@go.kauko.lt

Vykintas Stumbrys
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
vykintas.stumbrys@go.kauko.lt

***Abstract*—This paper explores how business activities can pose risks to national security, with a focus on Lithuania and the European Union. It analyzes how illicit practices, foreign ownership, and technological vulnerabilities contribute to threats in areas such as economic security, cybersecurity, and political influence. The research uses a qualitative approach, reviewing legal frameworks, national strategies, and real-world cases, including the revocation of UAB Foxpay's license and companies with ties to Russia and Belarus. These cases show how business links to authoritarian regimes, when left unchecked, can compromise critical infrastructure and sensitive data, or influence political decision-making. Technological advancements, such as artificial intelligence, digital finance, and global supply chains, increase vulnerabilities. Cases like Huawei and Kaspersky Lab illustrate the persistent risks of espionage, while supply chain attacks show how cyber threats can spread through business networks. The misuse of technology and lack of internal controls in some companies further exacerbate these risks. At the EU level, strategies such as the Security Union Strategy, the Digital Services Act, and the Chips Act aim to strengthen resilience, protect critical sectors, and regulate foreign influence. National measures, including Lithuania's investment screening and cybersecurity policies, complement these efforts by safeguarding strategic infrastructure and enhancing oversight. The study concludes that protecting national security in a digital and globalized economy requires a collaborative approach. Strong legal regulation must be combined with responsible business conduct. Security begins with knowing your partners and addressing indirect ties that may present risks. Ongoing legal development and consistent enforcement are essential to prevent business-related threats and maintain national stability.**

Keywords*— *economic security; national security; foreign influence; cybersecurity

I. INTRODUCTION

In an era marked by increasing geopolitical tensions, rapid technological advancements, and economic globalization, national security concerns extend beyond military and political dimensions to include economic, cyber, and technological threats. Business activities, while essential for economic growth, can pose significant risks to national security through illicit financial practices, strategic sector dependencies, cybersecurity vulnerabilities, and foreign influence. Recent cases, such as financial fraud in digital payment systems, supply chain cyber-attacks, and business ties with foreign entities that threaten state security, highlight the urgent need for stronger regulatory frameworks and oversight mechanisms.

The integration of artificial intelligence, digital financial transactions, and global trade networks has amplified the risks associated with economic security, making it imperative to assess how business actions influence national security. Governments, particularly within the European Union, have adopted legal frameworks and policies to mitigate these threats, but evolving challenges demand continuous adaptation and collaboration between regulatory bodies and businesses. Addressing these issues is critical to ensuring economic stability, protecting strategic sectors, and maintaining national sovereignty in a globalized world.

National security in Lithuania is a multifaceted concept encompassing several critical areas to ensure the country's sovereignty, stability, and resilience against various threats. One of the primary pillars is political security, which safeguards democratic governance, constitutional order, and the country's ability to independently conduct domestic and foreign policy [1]. Another essential area is military security, which focuses

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8505

on defence capabilities, territorial integrity, and cooperation with NATO allies to deter external aggression [2]. Additionally, economic security is important for maintaining stability, with an emphasis on protecting strategic industries, ensuring energy independence, and fostering economic resilience against external shocks [1, Art. 43]. Lithuania's social security involves efforts to strengthen national identity, social cohesion, and demographic sustainability, which collectively contribute to long-term national stability [1]. Cybersecurity measures aim to protect critical infrastructure, government networks, and sensitive data from cyber threats and espionage [1, Art. 37]. The areas of national security are closely related and the breach of one of them may have and has implications for other areas of national security.

The relationship between economics and national security is close and may not be evaluated separately. As A. L. Friedberg notes, "although the relationship may have grown more complex, economics and national security are and will continue to be intimately intertwined. Economic forces are changing not only the structure of the international system but the manner in which it functions. National security policy therefore may come to encompass measures designed to reduce a country's vulnerability to economic influence attempts as well as the more traditional forms of preparation for military defense" [3].

The aim of this study is to analyse specific cases where business activities pose threats to national security, highlighting their economic, technological, and regulatory implications. It seeks to examine the measures implemented at the European Union level to mitigate these risks, focusing on legal frameworks, cybersecurity policies, and economic controls. Additionally, the study evaluates Lithuania's national regulatory strategies, including investment screening, critical infrastructure protection, and measures to prevent illicit business influence on state security.

II. Methods and Materials

This study adopts a qualitative research methodology, focusing on the systematic examination of both national and European Union (EU) legal frameworks and strategic documents. It draws upon a wide range of regulatory texts, including binding and non-binding instruments from the European Commission, the European Parliament, and relevant Lithuanian legislative bodies. Additionally, the study incorporates national security reports published by the State Security Department of the Republic of Lithuania, as well as cybersecurity threat assessments issued by the National Cyber Security Centre. A critical component of the analysis is the review of selected Lithuanian business cases that have been publicly identified as posing potential threats to national security. These include, but are not limited to, cases involving violations of anti-money laundering (AML) and counter-terrorism financing (CTF) obligations, undisclosed ties with entities based in authoritarian regimes, and cybersecurity lapses in firms managing critical infrastructure. By triangulating these legal and empirical sources, the study aims to capture the evolving intersection between commercial activity, regulatory oversight, and national security imperatives in Lithuania within the broader EU legal context.

III. Results and Discussion

The relationship between EU measures on national security and those adopted by individual member states illustrates a complex balance between supranational coordination and national sovereignty. Through legislation, policy strategies, and judicial interpretation, the EU shapes the boundaries within which national governments may act.

Although national security remains primarily a competence of individual member states under Article 4(2) of the Treaty on European Union [4], the EU is increasingly involved in this area. This influence can be seen in sectors such as counterterrorism, cybersecurity, data governance, critical infrastructure protection, and foreign interference. Additionally, the Court of Justice of the EU strengthens the EU's role by ensuring that national security measures adhere to fundamental rights and the principles of the internal market.

The outcome is a legal and policy landscape in which national measures need to be carefully tailored to address both domestic security needs and EU legal obligations. This situation highlights the EU's significant influence in shaping security governance among its member states. The article offers a comprehensive analysis of the measures related to national security adopted by the EU and Lithuania.

A. EU measures against business threats to national security

At the EU level, Article 24 of the Treaty on European Union [4] and Article 72 of the Treaty on the Functioning of the European Union [5], which took effect in 2009, along with the Charter of Fundamental Rights [6], established the foundation for an EU security policy centred on the rule of law, fundamental rights, and solidarity. Member States are free to maintain law and order and safeguard states' internal security, whereas the EU's competence covers the Union's security [7, p. 646-647].

The EU has implemented policy, legal and technical measures to protect internal security while balancing economic interests and business operations. These measures cover areas falling under several EU strategies.

In July 2020, the EU adopted the Security Union Strategy for 2020-2025 to tackle a complex security landscape. This strategy emphasises a holistic approach that integrates various security policies. The strategy outlines key priorities for ensuring EU citizens' physical and digital security over five years. It focuses on priority areas where the EU can help Member States foster security. The strategy lays out the tools and measures to be developed to ensure security. It identifies four strategic priorities: fighting terrorism and organised crime, creating a future-proof security environment, building a strong security ecosystem, and addressing evolving threats [8].

Europeans' protection from terrorism and organised crime focuses on the significant threats posed by terrorism and radicalism, which destabilise society and endanger lives. Organised crime also incurs substantial economic losses, estimated to be between 218 billion and €282 billion annually [8, sec. IV (3)]. Key actions in the strategy include developing a counter-terrorism agenda and enhancing anti-radicalization efforts, improving cooperation with non-EU countries and international organisations, implementing plans against organised crime, migrant smuggling, drug trafficking [9], and firearms trafficking [10], reviewing legislation on asset freezing, confiscation, and environmental crimes.

The EU's new rules aim to combat money laundering and the financing of terrorism, enhancing detection and prevention measures for criminals within the financial system. Private sector operators must now conduct customer due diligence and report suspicious activities [11].

Additionally, Directive 2024/1260 on asset recovery and confiscation [12] will strengthen the fight against serious crime, enabling better confiscation of illicit profits. An upcoming directive on combating corruption will also harmonise penalties across the EU to address corruption risks [13].

Creating a future-proof security environment aims to establish safe and resilient critical infrastructure within the EU and protect against cyberattacks. Key actions include strengthening legislation on critical sectors, enhancing financial resilience, developing a cybersecurity strategy and joint cyber unit, promoting cooperation in safeguarding public spaces and addressing drone misuse [11].

The EU has implemented measures to protect critical infrastructure and enhance the resilience of essential services, notably through Directive 2022/2557 [14] and Directive 2022/2555 [15]. These directives address risks in key sectors such as energy, transport, banking, health, and public administration. Stress tests have been conducted in the energy sector to expedite the implementation of these directives.

A proposed Council Recommendation on a Blueprint setting aims for EU-level coordination against disruptions to critical infrastructure [16] and the Internal Market Emergency and Resilience Act (Regulation 2024/2747) [17] will help maintain market functioning during crises.

In collaboration with Member States and ENISA, the Commission has conducted a risk assessment of the EU's connectivity infrastructure and taken steps to improve the security of submarine cable networks essential for communication [11, p. 3]. The 5G Security Toolbox (2020) recommends mitigating telecom cybersecurity risks [11, p. 5].

The EU Cybersecurity Act [18] establishes a certification framework for ICT products and strengthens the EU Cybersecurity Agency (ENISA). The Digital Operational Resilience Act (DORA) [19] enhances the digital resilience of EU financial sector entities by updating existing rules amidst growing cyber threats. Directive 2022/2555 [15] expands cybersecurity requirements to all medium and large businesses across 18 critical sectors, introducing mandatory incident reporting and a European cyber crisis coordination structure. The Cyber Resilience Act [20] enforces mandatory cybersecurity measures for hardware and software, ensuring products are free of known vulnerabilities. The recently adopted Cyber Solidarity Act [21] creates a European Cybersecurity Alert System with Cyber Hubs for coordinated detection and response, supported by a Cybersecurity Emergency Mechanism and the EU Cybersecurity Reserve for significant incidents. The Digital Europe Programme allocates EUR 84 million for cybersecurity actions, including AI applications and post-quantum cryptography [11, p. 6].

The EU Network Code for cybersecurity rules related to cross-border electricity flows enhances system resilience in the energy sector [22]. The Wind Power Action Plan aims to improve the cyber-resilience of wind installations [23]. In transport, the Commission is advancing aviation and maritime security inspections [11, p. 2]. The Water Security Plan manual addresses measures against threats to water supply systems [24]. The revised EU Maritime Security Strategy [25] aims to protect critical maritime infrastructure from physical and cyber threats. A Common Information-Sharing Environment is being developed to improve information exchange among maritime authorities across borders and sectors [11, p. 3]. The revised Trans-European transport network Regulation [26] introduces new risk-proofing requirements for Member States to safeguard key transport infrastructure. In space, the EU Space Strategy for Security and Defence [27] includes actions to enhance resilience and further develop EU space-based dual-use services.

The EU Chips Act [28] is dedicated to strengthening supply chain security by reducing foreign dependencies in semiconductor supply chains. Meanwhile, the Critical Raw Materials Act [29] seeks to secure critical raw materials necessary for green and digital transitions, such as lithium and rare earth metals. This act focuses on diversifying supply chains and enhancing domestic extraction and recycling capacities.

EU Security Strategy emphasises that to build a strong European security ecosystem, EU governments, law enforcement, businesses, NGOs, and individuals must improve cooperation and sharing of information to combat crime and promote justice. Key actions include creating an EU 'police cooperation code,' enhancing Europol's role, linking Eurojust with judicial bodies, and strengthening ties with Interpol [8].

Artificial intelligence plays a significant role in law enforcement, but fundamental rights must be respected. While generative AI can aid cybercriminals in executing sophisticated attacks, Regulation 2024/1689 on Artificial Intelligence [30] aims to provide guardrails for

responsible AI use in the EU, ensuring the safety and rights of citizens.

The EU Security Strategy regarding tackling evolving threats includes addressing cybercrimes (like identity theft), illegal online content (such as hate speech), and hybrid threats (combining military and non-military activities). It recommends enforcing cybercrime laws and reviewing protocols on hybrid threats [8].

The European Economic Security Strategy [31] enhances the "whole of society approach" proposed in the EU Security Union Strategy by concentrating on protecting the EU, its Member States, and its citizens from economic threats. The strategy aims to achieve economic security by strengthening the EU's economic foundations and competitiveness, safeguarding against risks, and fostering partnerships with various countries to tackle common challenges. This approach will be essential for the EU's future security considerations.

Two key focus areas for economic security are combating market monopolisation and strengthening trade and economic defence.

Combating market monopolisation: Article 101 of the Treaty on the Functioning of the EU prohibits anti-competitive agreements, while Article 102 addresses the abuse of dominant positions. The EC Merger Regulation restricts concentrations that hinder competition [32, Art. 2 (3)]. Regulation 2022/2560 introduces measures to investigate foreign subsidies that distort the internal market [33]. The Digital Markets Act [34] and Digital Services Act [35] regulate tech giants to promote fair competition and prevent monopolisation.

Strengthening trade and economic defence: Regulation 2019/452 [36] enables screening of foreign investments that could threaten security or public order, allowing Member States to block or impose conditions on investments in critical sectors (e.g., energy, telecommunications, defence, etc.) [7, p. 648-650]. Regulation 2021/821 updates export controls on dual-use items, including emerging technologies and cybersecurity tools [37]. Regulation 2023/2675 protects EU businesses from economic coercion by non-EU states and permits trade restrictions against such countries [38].

The analysis of EU instruments demonstrates that they are continually being expanded and improved to address emerging challenges. Considering the Commission's unique role in safeguarding EU internal security, the Commission will undoubtedly provide new initiatives aimed at today's challenges.

2. *B. National measures against business threats to national security*

States employ different measures in order to protect national security from the threats caused by action of businesses.

The National security strategy of the Republic of Lithuania [1] foresees measures aimed at mitigating and removing risks that may be caused by the actions of business entities to national security. It foresees the following related tasks aimed at ensuring economic and energetic security of Lithuania:

1) to develop measures to encourage economic entities of the Republic of Lithuania to shift their business relations from authoritarian states to states that adhere to democratic values;

2) to develop the system of control of transactions and foreign investments in strategic sectors;

3) to reduce the dependence of Lithuanian transport sector from one country and increase diversification;

4) to increase control on import, export and transit of military equipment and dual-use goods;

5) to increase independence of Lithuanian electricity systems [1, Art. 43];

6) to ensure that the digitisation of the state through data opening, digital infrastructure, e-services, digital content or data creation, development and other digitisation initiatives is carried out in accordance with the interests of national security;

7) to ensure the safe use of new technologies for the state and society by employing only reliable equipment in critical information infrastructure and state IT resources; to implement AI, IoT, 5G, and digitalization following top cybersecurity and resilience standards, guaranteeing uninterrupted critical infrastructure operations during crises [1, Art. 37].

Protection of strategic sectors

The system of control of strategic sectors is foreseen in the Law on the Protection of Objects Important for National Security. The Law foresees measures to protect:

1) objects of strategic importance to national security (companies, installations and assets and economic sectors of energy, transport, information technologies and communications, other high technologies, finance and credit and military equipment);

2) assets and territory in protective zones;

3) strategically important cyber security objects [39, Art. 1].

It is foreseen that transactions regarding those objects should be protected from all risks to national security interests, the causes and conditions that give rise to such risks should be addressed. In particular, there is a list drawn up of such objects which are strategically important to national security. A risk assessment is carried out regarding such objects. The managing organs of companies of strategic importance to national security are prohibited from taking decisions that would contravene national security interests. Actions regarding companies in such a list (like reorganization, liquidation of assets and similar) are subject to approval by state institutions (national parliament or government). Investors are also vetted in order to establish their compatibility with national security interests. [39, Art. 6-

10]. One of the key criteria for assessing the compatibility of an investor or a party to a transaction with national security interests is the existence of past or present relations with foreign authorities, natural or legal persons of foreign countries that pose a risk or threat to national security [40]. Furthermore, the government may limit, stop or abolish contracts, investments or economic commercial activities [39, Art. 1]. There are requirements for persons who take up positions in governing bodies of strategically important companies [39, Art. 17].

The decisions are taken by the Coordination Commission for the Protection of Objects Important for National Security established by the Law. "The Commission is chaired by the Chancellor of the Government and includes representatives from various ministries, the Bank of Lithuania, the General Prosecutor's Office, the Police Department, the Special Investigation Service and the State Security Department" [41]. The subjects providing their opinions on the compliance with the national security interests are the Ministry of Foreign Affairs of the Republic of Lithuania, the Ministry of the Interior, the Police Department, the Prosecutor General's Office, and by request of the Commission - other bodies.

3. Restrictions of influence of business on politics

Speaking about business influence in politics, a tool to control the level of influence is the criminalization of influence peddling under Article 226, which serves as a safeguard against illicit business interference in political and administrative decision-making, thereby protecting national security interests [42, Art. 226]. This crime encompasses offering, promising, giving, or accepting bribes in exchange for using one's real or perceived influence over public institutions, officials, or international organizations to affect their lawful or unlawful actions. By penalizing such conduct, this measure upholds the integrity of public institutions, ensures transparency, and strengthens public trust in governance.

The transparency of influence of businesses and other entities on legislative processes is ensured by the regulation of lobbying in the Law on lobbying activity. The law indicates that persons aiming to influence politicians and their decisions need to register in the list of lobbyists and indicate in which area of legal regulation they aim to act. The lobbyist must complete a Transparent Legislative Declaration for each act that they aim to change and after the meeting with politicians. The Chief Official Ethics Commission keeps the list of the lobbyists and oversees their activities [43]. The information about lobbyists and all Transparent Legislative Declarations is public [44].

The regulation of the financing of political organisations also aims to limit the influence of business entities on political processes. According to the Law on Political Organisations of the Republic of Lithuania, businesses may not finance the political organisations, only donations from natural persons are allowed to finance the political campaign by their donations [45, Art. 19(1)(7)].

4. Ensuring cybersecurity of businesses

Specific measures are aimed at ensuring the resilience of business entities to cyber threats. National Cyber Security Centre of Lithuania (NCSC) pays special attention to cyber protection and resilience to threats in in organisations managing Critical Information Infrastructure [46, p. 12]. The Centre encourages such organisations to establish cybersecurity policy and implementing standards and other measures and monitors their progress regularly. In 2023 NCSC coordinated and carried out 17 thorough cyber security checks on such companies, together with the European Union Agency for Cybersecurity [46, p. 12].

The Centre also encourages other organisations to voluntarily adopt organisational and technical cyber security measures in their operations as they significantly reduce the risk of cyber-attacks, ensure business continuity for the organisation and reduce the damage caused by cyber incidents, thus minimising risks to national security that could arise [46, p. 12]

In order to ensure the resilience of organisations and companies, the NCSC carried out trainings and practical exercises in order to increase the ability of cyber security subjects to manage risks, to recognize cyber security incidents and react to them properly. In 2023, more than 11,500 people from public administration sector bodies, non-governmental organisations and small and medium-sized enterprises completed the various types of theoretical training organised by the NCSC [46, p. 37] In order to strengthen the resilience of the country's critical infrastructure to cyber threats, the NCSC, in cooperation with the US Naval Postgraduate School, organised for the first time the Industrial Control Systems Cybersecurity Course. The course was attended by 39 participants from Lithuania and Ukraine [47].

To effectively mitigate these risks, a collaborative approach combining strong state regulation with vigilant business practices is essential, ensuring appropriate measures are in place to protect economic and national security. As shown in examples, in an increasingly digital world, security begins with conscious efforts to mitigate risks. In both the business world and cyberspace, the key advice is to know service partners and the partners they work with. Enhancing legal regulation by the state is a must in these conditions

C. Case studies of businesses actions posing threat to national security

At their national level, states deal with influence in different fields. Here are cases discussed that reached courts and formed some precedents, and also cases that were presented by Lithuanian, Latvian, Estonian state security institutions. Authors also draw attention to the most known worldwide examples.

The relationship between economic factors and the threats businesses may pose to state security is a complex interplay. Economic security also serves as a foundation for national stability, and threats arising from business

activities can undermine state security, contributing to various vulnerabilities. Additionally, the interplay between technological advancements and security cannot be overlooked. As states increasingly rely on technology, the risks associated with cyber threats escalate, particularly as criminal enterprises exploit vulnerabilities in digital systems. Business activities may pose security threats, particularly when inadequate regulations lead to illicit practices, contributing to vulnerabilities that affect state security.

The role of state regulation is pivotal in mitigating these risks. As states seek to ensure their security, they must balance facilitating business operations with enforcing regulations that prevent illicit financial activities jeopardizing public welfare [48]. The lack of robust regulatory frameworks can lead to the proliferation of shadow economies and businesses operating outside legal boundaries, posing threats to economic security [49]. Inadequate regulation not only allows for financial crimes, such as money laundering and tax evasion, but also opens the door to corruption, further eroding public trust and state legitimacy [48]. In order to understand the nature of this relationship, some examples may be needed.

In the case of UAB Braitin (formerly UAB Lewben Investment Management), the company intended to acquire an investment company registered in Vilnius, UAB Prosperus Real Estate Fund II. In order to carry out this transaction, they needed the permission of state institutions. The Commission for Assessment of Compliance of Potential Participants with National Security Interests refused to grant such permission on the basis of information provided by the State Security Department of Lithuania (further – SSD). The SSD provided information to the Commission that the sole shareholder of the company had relations with individuals from non-EU and non-NATO countries that posed a risk to national security. Publicly available information provided by the SSD indicated that one of the persons was a suspect in criminal activity and was arrested in Belarus, and the other person, a businessman, had been under the EU sanctions for support, via his company, to the Lukashenko regime. [50, para. 12]. The threat had been addressed before becoming a breach of national security. The Vilnius Regional Administrative Court and Supreme Administrative Court of Lithuania upheld the authorities' decision, emphasizing that even minimal risks to national security justify state intervention over private business interests. The European Court of Human Rights also ruled that the company's rights had not been violated. It noted that while fair trial rights are important, they are not absolute—especially in cases involving national security where states enjoy a significant margin of appreciation. What matters is that the courts put in place enough safeguards to protect the interests of the company, even if some information had to be kept secret. [50, para. 60]

In another case, Lithuanian authorities raised national security concerns about a planned data storage facility that would connect to the Internet and local telecommunications networks, linking it to EU countries and Russia. The companies AmberCore DC and Arcus Novus which were registered at a technology park in Liepiškės near Vilnius. Arcus Novus was founded in 2003 and deals with the implementation and development of technological projects, including the transmission of information by satellite telecommunication. In 2009 Arcus Novus established a subsidiary company, later renamed AmberCore DC, which deals with the construction and development of data centres. The companies initiated a project to build a data storage facility near Vilnius, for which they required a permission from the abovementioned Commission for Assessment of Compliance of Potential Participants with National Security Interests. The permission was denied in 2016 due to the potential risks to national security. On the basis of report of SSD, the Commission indicated that Arcus Novus, through intermediary companies was owned and controlled by four citizens of the Russian Federation. The risk posed by Arcus Novus to Lithuanian national security was increased by the fact that "one of these owners, V.A., had previously worked in Russian companies directly linked with the Russian State and law enforcement authorities. Those companies "were overseen" by the Federal Security Service of the Russian Federation ("the FSB"). More specifically, from 2006 to 2009 V.A. had worked as a director of the Russian gas corporation's subsidiary company Gazprom Komplektacija in the Kaliningrad region, and from 2009 to 2014 had been the founder and deputy director of Gazinvest Group, another company operating in Kaliningrad and dealing in customs brokerage" [51, para. 10]. In Lithuania, the data storage facility was to be connected to the Internet and local telecommunications networks, linking it to EU countries and Russia. According to the SSD, this connection could enable Russia's FSB to access the facility through its intelligence centre, which conducts cyber spying against Lithuania, NATO, and the EU. The SSD warned that the FSB could intercept sensitive data, influence Lithuanian networks, use Lithuanian territory for cyberattacks, and, if key institutions became clients, disrupt the functioning of the State and its economy [51, para. 10]. As in the previous case, the threat had been addressed via legal and judicial means, by refusing permit for the planned activity. The Lithuanian courts upheld this decision, and the European Court of Human Rights found no violation of the companies' rights. It confirmed that national authorities had struck a fair balance between public interests and the companies' procedural rights, and that the use of some confidential material had not undermined the fairness of the hearing. [51, para. 117].

In another important case the Constitutional Court of Lithuania analysed the case involving the Lithuanian President committing severe national security breaches by unlawfully granting Lithuanian citizenship to J.B., a businessperson, in return for substantial financial and material support provided through his enterprises. J.B., through his business enterprises, provided significant financial and material assistance to the presidential campaign of the candidate for President in 2002. Such extensive financial backing created undue influence, allowing J.B. to leverage his enterprise's economic power for political advantage [52]. This created a

scenario where private enterprise interests directly influenced state decisions and presidential actions. This established a concerning precedent, demonstrating how economic power from enterprises could compromise governmental integrity, potentially exposing decision-making processes to external manipulation or foreign influence, thus directly threatening national security. The breach was addressed through the constitutional impeachment procedure, as defined in Article 74 of the Lithuanian Constitution. The Constitutional Court of Lithuania conducted an examination and concluded that the Lithuanian President had gravely violated the Lithuanian Constitution. This impeachment case exposed significant regulatory gaps in the national security framework, particularly concerning the intersection of enterprises and political power. It showed that there was no adequate conflict-of-interest prevention. The legal framework for preventing private enterprise influence or economic contributions from improperly affecting state decision-making was not sufficiently robust. To remove this gap, the legal regulation was changed, prohibiting enterprises from giving material support to politicians and political parties [52]. In addition, the Constitutional Court declared the President Decree on granting citizenship to the J.B. as unconstitutional [53].

In the case No. eI2-3776-1114/2024 [54], the national security breach was centered around the Lithuanian aviation company Aviabaltika, which was found non-compliant with Lithuania's national security interests. The breach occurred due to the company's long-standing commercial relationships and historical ties with entities from Russia and Belarus, countries officially considered hostile by Lithuania. Specifically, concerns were raised due to former shareholder and owner J. B., a Russian citizen with significant business ties to the Russian military-industrial complex, association with entities enhancing Russia's defence capabilities. Aviabaltika continued commercial activities involving entities from Russia and Belarus, including organisations directly involved in their military-industrial sectors, thereby indirectly supporting the strategic capabilities of adversarial states. Aviabaltika operated facilities within Kaunas International Airport's strategically important protection zone, a critical infrastructure site essential for Lithuania's national defense and security. The breach was directly addressed through formal regulatory actions. The Lithuanian Government, through the Commission on Coordination of Protection of Objects Important to National Security, conducted a thorough security review and declared Aviabaltika non-compliant with national security interests, effectively prohibiting further extension of the company's land lease within the critical security zone. The Vilnius Regional Administrative Court upheld the government's position, validating the proportionality and legitimacy of the security-based restrictions applied. The case revealed significant regulatory gaps regarding national security oversight. Existing procedures lack a proactive and systematic mechanism to monitor or review enterprises with sensitive foreign ties operating within national security zones. The regulatory framework did not clearly define how indirect or past ties with adversarial states should be assessed and at what thresholds they constitute a national security risk. Therefore, there is a need to clearly define regulatory criteria and thresholds specifying what constitutes unacceptable indirect business relationships or historical ties, ensuring consistent application across similar enterprise assessments [54].

Similarly, Supreme Administrative court case No. eA-393-520/2023 [55] shows that the Lithuanian Government and the National Security Coordination Commission determined that the enterprise seeking to expand its operations within a strategically sensitive security zone had ownership structures indirectly connected to individuals and entities affiliated with foreign state institutions, special services, and corporations closely related to the military-industrial complex of a foreign state, particularly Russia. A significant concern was the indirect control exercised by individuals associated with Russian state corporations, thereby creating vulnerabilities in critical national infrastructure protection due to potential foreign influence and espionage risks. Due to these foreign links, the enterprise's planned infrastructure expansion and reconstruction within the security-sensitive area adjacent to critical Lithuanian national security infrastructure was deemed incompatible with Lithuanian national security interests. The Lithuanian Government adopted a resolution based on the Commission's assessment, officially prohibiting the enterprise's planned activities (expansion and reconstruction) within the security-sensitive zone. The Supreme Administrative Court confirmed the government's decision as legitimate, proportional, and consistent with national security requirements. This case revealed that the existing regulatory frameworks did not clearly define how to monitor and transparently disclose foreign links or beneficial ownership in corporate structures, particularly when involving complex ownership chains and offshore entities. Therefore, there is a need to establish clear statutory definitions and objective criteria regarding the national security implications of indirect corporate ownership and beneficial interests, especially those involving entities or individuals affiliated with foreign state institutions or special services [55].

In another one case, the Vilnius Regional Administrative Court found serious threats to national security involved in a procurement contract between Lithuanian Airports and Nuctech, a Chinese enterprise, for the acquisition of baggage inspection systems — equipment integral to the operation and security of national critical infrastructure (airports) [56]. The main national security concern was that Nuctech was found to have ties to the Chinese government, including affiliations with Chinese military and intelligence services. This raised red flags about potential risks of surveillance, data interception, and system manipulation through hardware/software embedded in critical national infrastructure. By allowing a company with such affiliations to supply systems for airport security, Lithuania risked exposing sensitive data and operational

integrity to a foreign government with competing geopolitical interests. The Lithuanian Government took action to address the threat. An investigation was carried out by the Commission for Coordination of Protection of Objects of Importance to Ensuring National Security, which concluded that Nuctech's connections made it ineligible to operate within sensitive Lithuanian infrastructure. Based on these findings, the Government annulled the contract, citing national security grounds. The court upheld the Government's action, validating the national security rationale and procedural legality [56].

In the Vilnius Regional Administrative Court case No I-4964-764/2016 [57], the breach concerned potential threats to Lithuania's national security arising from the relationships between private enterprises and foreign state-affiliated entities. Specifically, UAB "FL Technics" was determined not to meet Lithuania's national security requirements due to its corporate association with AB "Avia Solutions Group", a company engaged in close commercial relations with Russian state-controlled entities. AB "Avia Solutions Group," the parent company of FL Technics, maintained significant commercial relations with the Russian state-owned enterprise "Rostec," whose CEO, S. C., was closely affiliated with Russian security services and sanctioned by the U.S. and EU for actions undermining Ukrainian sovereignty (specifically, Crimea's annexation). The association with S.C. and Rostec presented an indirect yet tangible risk of foreign intelligence influence due to S.C.'s known past involvement with KGB and high-ranking positions within Russian state structures. The identified national security risk was addressed by Lithuania's special commission, which is responsible for evaluating enterprises' compliance with national security interests. The Commission concluded in 2015 that FL Technics did not meet the required national security criteria, primarily because of its indirect ownership link to Russian entities considered hostile or detrimental to Lithuanian, EU, and NATO interests. This decision resulted in the Denial of the right for FL Technics to lease strategically important land within Vilnius International Airport. The decision revealed the lack of clarity in criteria defining connections that threaten national security (e.g., indirect ownership or commercial collaboration with foreign state enterprises). FL Technics challenged the criteria for being vague, unclear, and overly broad. Therefore, the court decision revealed the need to provide regulatory guidance clarifying what constitutes unacceptable national security risks stemming from corporate relationships or indirect ownership, specifying thresholds and conditions [57].

The Department of National Security of Lithuania likewise mentions example of such risks. The company operating in the transport sector had links with Belarusian companies – the state institute Belželdorprojekt and the company Želsviazprojekt BR. As part of the strategically important project, the company resumed contacts with the employees of these Belarusian entities and used them to carry out the tasks of the project, trying to hide it from the project developer. In this way, Belarusian entities gained access to information about the ongoing project and part of its engineering solutions. After the identification of the company's cooperation with Belarusian entities, its participation in strategically important projects was prevented. It is very likely that Russian and / or Belarusian entities, in order to interfere with the work of strategically important infrastructure facilities or obtain non-public information about it, will try to use cyber capabilities or take advantage of the vulnerabilities of personnel of strategically important companies [40, p. 71].

Almost all Lithuanian companies that previously cooperated with Russian Rosatom companies and their representatives did not break these ties. The main motives for cooperating with Rosatom are financial interests, opportunities to get jobs in projects carried out by Rosatom and the desire to maintain cooperation based on personal loyalty and friendship. Lithuanian companies with contacts with Rosatom, in order to participate in Ignalina atomic power station projects, use various tools, often act in a non-transparent manner and try to conceal the contacts they maintain, realizing that they are likely to be assessed as risky or threatening. The most popular ways of acting: creating a new name – setting up or acquiring a new shelter company; attempts to recruit specialists in projects by concluding individual contracts with them, who often try to conceal links with a company whose participation in the project would not be in the interests of national security. Lithuanian companies cooperating with Rosatom companies are not able to claim a large number of applications [40, p. 72].

The Latvian State Security Service notes that Latvian business cooperation with Russia to circumvent sanctions poses a great risk. Direct and indirect cooperation of local businesses with Russia remained the main source of risks to Latvia's economic security and international reputation. Security and other responsible services continuously assessed suspicious transactions by Latvian companies to detect and prevent violations of international sanctions. At the same time, Latvia continued to gradually move towards severing economic ties with Russia [58, p. 50].

It is likely that rapid development of AI and the wider-ranging use of the tools it provides have created a situation where national legislation and regulation have not been able to keep pace. Estonian National security report states that as such, easy access to ever more powerful resources is being accompanied by the misuse of AI: increasingly, false information is being spread through deepfake images, videos and audio clips, and large-scale, quick-learning language models are making it easier for cybercriminals to engage in social manipulation and phishing. In the last decade, the number of incidents involving the misuse of AI has increased and this trend is expected to continue in the near future, with the scope of incidents likely to grow as the quality of AI improves. Misuse of artificial intelligence appears in different ways. Use of deepfake in election campaigns in Poland and Slovakia was aimed to cause loss of trust in institutions. AI-generated image of an explosion near the Pentagon or similar spreads disinformation, deterioration in media literacy, reduced

threat perception. Use of deepfake to hold fake calls with Western politicians may cause loss of trust in institutions, undermining, influencing public opinion. Use of AI by Russia to produce disinformation aimed at loss of trust in institutions, influencing public opinion and outcome of elections [59, p 16].

Well known example of such a technological threat in 2020 is Huawei products related to the threat of espionage. Although Huawei has claimed that the Chinese government does not legally have the authority to compel it to build backdoors into its telecommunication system and that its subsidiaries and employees outside of China are not subject to the territorial jurisdiction of the National Intelligence Law, many legal experts have disputed this interpretation [60]. And a lot of countries even banned Huawei products in its institutions [61].

Some other examples of cybercrime-related cases revealing business vulnerabilities include a Moscow-based antivirus firm Kaspersky Lab was banned on the grounds of national security concerns. It is purportedly alleged that Kaspersky's products constituted a threat to national security and could be used to facilitate espionage by the Russian government [62, p. 279].

Over the past decade a long-term process of digitization of finance has increasingly combined with datafication and new technologies including cloud computing, blockchain, big data and artificial intelligence in a new era of FinTech. One of the recent and most highlighted cases in Lithuania was the Foxpay case. In 2024 Central Bank of Lithuania revoked the electronic money institution licence of UAB Foxpay for serious and systematic breaches of legal acts regulating the prevention of money laundering and terrorist financing, safeguarding of client funds and other legislation. Following the decision, Foxpay can no longer provide financial services. The Central Bank of Lithuania noted that Foxpay's operational shortcomings and breaches of legislation were identified in all areas inspected [63].

Foxpay infringed the following key requirements for the prevention of money laundering and terrorist financing (AML/CTF):

- Failed to ensure that its internal control system for AML/CTF was effective and sound. AML/CTF processes implemented in practice were not in line with internal procedures.
- Failed to ensure adequate identification of clients, their representatives and beneficiaries, including enhanced client identification.
- Failed to establish sufficient measures for monitoring client's business relationships and operations/transactions. Failed to ensure that clients' individual ML/TF risks were properly identified and assessed [63].

Allegations of money laundering, fraud and corruption dominated the narrative, and, pre-trial investigations led to the detention of seven individuals, including Ieva Trinkunaite, Foxpay's owner; her partner Vilhelmas Germanas; and Mindaugas Navickas, the husband of former Social Security Minister Monika Navickienė [64].

Examples of supply chain attacks attributed to state cyber capabilities made public in 2021: The French National Cyber Security Agency publicly accused the Sandworm group, which was affiliated with the Russian GRU, of carrying out attacks on the networks of French organizations in 2017-2020. The group gained access to the target systems by exploiting a vulnerability in software sold by the local IT company Centreon. The APT29 group, which was affiliated with Russian intelligence, which carried out a large-scale attack against the IT management systems manufacturer SolarWinds and its customers in 2019-2020, had launched a new supply chain attack campaign. It is likely that companies providing IT solution management services were chosen as the initial targets of the new attacks due to their access to their customers' information systems. The North Korean-backed Lazarus group's attacks were exposed, with the group carrying out malicious activities using software from South Korean and Latvian IT companies [58, p. 47].

In conclusion from these cyberspace related examples, states may consider new technological and legal vulnerabilities. 1. The reliance on emerging technologies such as blockchain, AI, and IoT in digital payments introduces new vulnerabilities that can be exploited by sophisticated attackers. 2. With lack of comprehensive legal frameworks to address the unique risks posed by digital payments, leaving gaps that cybercriminals can exploit. 3. Payment system security gaps, while used for bribery and money laundering, can cause significant moral and structural damage to societies and economies.

Concluding, all examples above we can state that technological advancements further complicate the landscape, increasing the potential for threats as companies face challenges in maintaining effective internal controls. Notable instances, such as the revocation of UAB Foxpay's license by the Central Bank of Lithuania for serious regulatory breaches, exemplify the repercussions of failing to uphold adequate regulations. Additionally, connections between companies and foreign entities, like those with Belarusian or Russian companies, pose risks by potentially compromising sensitive project information. Companies have been found to maintain ties with Russian state-operated entities, driven by financial interests and personal loyalties, despite the associated risks to national security. Businesses collaboration with Russia and China to circumvent sanctions presents a significant threat to economic security, and there is a continuous assessment of suspicious transactions to prevent violations. Cases like Huawei or Kaspersky Lab illustrate ongoing concerns regarding espionage and national security linked to technology firms. Supply chain attacks, attributed to state-backed cyber groups, reveal vulnerabilities exploited in the digital landscape.

To effectively mitigate these risks, a collaborative approach combining strong state regulation with vigilant business practices is essential, ensuring appropriate measures are in place to protect economic and national security. As shown in examples, in an increasingly digital world, security begins with conscious efforts to mitigate risks. In both the business world and cyberspace, the key advice is to know service partners and the partners they work with. Enhancing legal regulation by the state is a must in these conditions.

V. CONCLUSIONS

The relationship between business activities and national security is increasingly complex, with economic and technological factors playing a critical role in maintaining state stability. This paper shows that business actions—especially those involving critical infrastructure, foreign ownership, or influence in politics—can pose significant threats to national security. Lithuania has faced several real-world examples, such as the revocation of UAB Foxpay's license due to regulatory breaches and multiple cases involving business ties to entities from Russia and Belarus. These instances highlight how business interests, if unregulated, can compromise sensitive sectors and even influence political decisions.

Technological advancements further complicate the landscape, increasing the potential for threats as companies face challenges in maintaining effective internal controls. The growing use of artificial intelligence, digital finance, and global supply chains introduces new vulnerabilities. Cases like Huawei and Kaspersky Lab underscore persistent concerns about espionage and data security. Supply chain attacks by state-backed actors further reveal how weaknesses in business ecosystems can be exploited.

European Union initiatives, such as the Security Union Strategy, Digital Services Act, and the Chips Act, provide a multi-layered framework aimed at addressing these evolving threats. These policies stress collaboration across sectors, improved investment screening, and enhanced cybersecurity standards. National efforts, including Lithuania's strategic legislation and oversight mechanisms, reinforce this approach by protecting critical infrastructure, regulating foreign influence, and monitoring business activities in sensitive sectors.

To effectively mitigate these risks, a collaborative approach is essential—combining strong state regulation with responsible and transparent business practices. Regulatory bodies must ensure legal clarity, enforce compliance, and adapt to rapid technological change. As shown in the examples, in a digitalized and globalized world, national security starts with awareness—knowing service providers, their partners, and potential foreign connections. Enhancing legal frameworks and enforcing them consistently remains a necessary condition for safeguarding both economic interests and state security.

REFERENCES

[1] Republic of Lithuania, Seimas, "National Security Strategy," Resolution No. IX-907, May 28, 2002. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr. [Accessed: Mar. 3, 2025].

[2] Republic of Lithuania, Seimas, "Programme for the Strengthening and Development of the National Defence System," 2022. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e3acb430e78f11ee9fdedfc979ae62a9?jfwid=oizvypq8. [Accessed: Mar. 3, 2025].

[3] A. L. Friedberg, "The changing relationship between economics and national security," in *Power, Economics, and Security: The United States and Japan in Focus*. Routledge, 2019. [E-book]. Available: https://doi.org/10.4324/9780429302831.

[4] European Union, "Treaty on European Union" (Consolidated version 2016), Official Journal of the European Union, OJ C 202, Jun. 7, 2016.

[5] European Union, "Treaty on the Functioning of the European Union (Consolidated version 2016)", Official Journal of the European Union, OJ C 202, Jun. 7, 2016.

[6] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union, OJ C 364/01, Dec. 18, 2000.

[7] A. Banevičienė, "The regulation of non-horizontal concentrations in the context of EU economic security," in Transformations, Challenges and Security: Collective Monograph, Ž. Simanavičienė, Ed. Vilnius: Mykolas Romeris University, Public Security Academy, 2024. [Online]. Available: https://cris.mruni.eu/cris/handle/007/49074. [Accessed: Mar. 4, 2025].

[8] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions on the EU Security Union Strategy, COM(2020) 605 final, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605. [Accessed: Mar. 4, 2025].

[9] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: EU Agenda and Action Plan on Drugs 2021-2025, COM(2020) 606, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0606. [Accessed: Mar. 4, 2025].

[10] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: 2020-2025 EU Action Plan on Firearms Trafficking, COM/2020/608 final, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0608. [Accessed: Mar. 4, 2025].

[11] European Commission, Communication from the Commission to the European Parliament and the Council on the Seventh Progress Report on the Implementation of the EU Security Union Strategy, COM(2024) 198 final, May 15, 2024. [Online]. Available: https://commission.europa.eu/publications/seventh-progress-report-implementation-eu-security-union-strategy_en. [Accessed: Mar. 4, 2025].

[12] European Parliament and Council, "Directive 2024/1260 (EU) of 24 April 2024 on Asset Recovery and Confiscation, Official Journal of the European Union", OJ L 2024/1260, May 2, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2024/1260/oj/eng. [Accessed: Mar. 4, 2025].

[13] European Commission, Proposal for a Directive of the European Parliament and of the Council on Combating Corruption, Replacing Council Framework Decision 2003/568/JHA and the Convention on the Fight Against Corruption Involving Officials of the European Communities or Officials of Member States of the European Union and Amending Directive (EU) 2017/1371 of the European Parliament and of the Council, COM/2023/234 final, May 3, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0234. [Accessed: Mar. 4, 2025].

[14] European Parliament and Council, Directive 2022/2557 (EU) of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC, Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng. [Accessed: Mar. 4, 2025].

[15] European Parliament and Council, Directive 2022/2555 (EU) of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng. [Accessed: Mar. 4, 2025].

[16] European Commission, Proposal for a Council Recommendation on a Blueprint to Coordinate a Union-Level Response to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance, COM/2023/526 final, Sep. 6, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=celex%3A52023DC0526. [Accessed: Mar. 4, 2025].

[17] European Parliament and Council, Regulation (EU) 2024/2747 of 9 October 2024 Establishing a Framework of Measures Related to an Internal Market Emergency and to the Resilience of the Internal Market and Amending Council Regulation (EC) No 2679/98 (Internal Market Emergency and Resilience Act), Official Journal of the European Union, OJ L 2747, Nov. 8, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2747/oj/eng. [Accessed: Mar. 4, 2025].

[18] European Parliament and Council, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union, OJ L 151, Jun. 7, 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881. [Accessed: Mar. 4, 2025].

[19] European Parliament and Council, Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng. [Accessed: Mar. 4, 2025].

[20] European Parliament and Council, Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Official Journal of the European Union, OJ L 2847, Nov. 20, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. [Accessed: Mar. 4, 2025].

[21] European Parliament and Council, Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), Official Journal of the European Union, OJ L 38, Jan. 15, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng. [Accessed: Mar. 4, 2025].

[22] European Commission, Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 Supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by Establishing a Network Code on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, Official Journal of the European Union, OJ L 1366, May 24, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng. [Accessed: Mar. 4, 2025].

[23] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: European Wind Power Action Plan, COM/2023/669 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0669&qid=1702455143415. [Accessed: Mar. 4, 2025].

[24] R. Teixeira, O. Carmi, P. Gattinesi, and P. Hohenblum, *Water Security Plan Implementation Manual for Drinking Water Systems*, JRC Publications Repository, Jan. 11, 2022. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC126684. [Accessed: Mar. 4, 2025].

[25] European Commission, Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and its Action Plan: "An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats", JOIN/2023/8 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0008. [Accessed: Mar. 4, 2025].

[26] European Parliament and Council, Regulation (EU) 2024/1679 of 13 June 2024 on Union Guidelines for the Development of the Trans-European Transport Network, Amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and Repealing Regulation (EU) No 1315/2013, Official Journal of the European Union, OJ L 1679, Jun. 28, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1679/oj/eng. [Accessed: Mar. 4, 2025].

[27] European Commission, *Joint Communication to the European Parliament and the Council: European Union Space Strategy for Security and Defence*, JOIN(2023)9, Mar. 10, 2023. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en. [Accessed: Mar. 4, 2025].

[28] European Parliament and Council, Regulation (EU) 2023/1781 of 13 September 2023 Establishing a Framework of Measures for Strengthening Europe's Semiconductor Ecosystem and Amending Regulation (EU) 2021/694 (Chips Act), PE/28/2023/INIT, Official Journal of the European Union, OJ L 229, Sep. 18, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.229.01.0001.01.ENG. [Accessed: Mar. 4, 2025].

[29] European Parliament and Council, Regulation (EU) 2024/1252 of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials and Amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724, and (EU) 2019/1020, Official Journal of the European Union, OJ L 1252, May 3, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1252&qid=1720020986785. [Accessed: Mar. 4, 2025].

[30] European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), PE/24/2024/REV/1, Official Journal of the European Union, OJ L 1689, Jul. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. [Accessed: Mar. 4, 2025].

[31] European Commission, "Joint Communication to the European Parliament, the European Council, and the Council on "European Economic Security Strategy"," JOIN/2023/20 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020. [Accessed: Mar. 4, 2025].

[32] Council of the European Union, Regulation (EC) 139/2004 of 20 January 2004 on the Control of Concentrations Between Undertakings (the EC Merger Regulation), Official Journal of the European Union, OJ L 24, Jan. 29, 2004. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2004/139/oj/eng. [Accessed: Mar. 4, 2025].

[33] European Parliament and Council, Regulation (EU) 2022/2560 of 14 December 2022 on Foreign Subsidies Distorting the Internal Market, PE/46/2022/REV/1, Official Journal of the European Union, OJ L 330, Dec. 23, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2560/oj/eng. [Accessed: Mar. 4, 2025].

[34] European Parliament and Council, Regulation (EU) 2022/1925 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), PE/17/2022/REV/1, Official Journal of the European Union, OJ L 265, Oct. 12, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925. [Accessed: Mar. 4, 2025].

[35] European Parliament and Council, Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1, Official Journal of the European Union, OJ L 277, Oct. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065. [Accessed: Mar. 4, 2025].

[36] European Parliament and Council, Regulation (EU) 2019/452 of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments into the Union, PE/72/2018/REV/1, Official Journal of the European Union, OJ L 79I, Mar. 21, 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/452/oj/eng. [Accessed: Mar. 4, 2025].

[37] European Parliament and Council, Regulation (EU) 2021/821 of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit, and Transfer of Dual-Use Items, PE/54/2020/REV/2, Official Journal of the European Union, OJ L 206, Jun. 11, 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821. [Accessed: Mar. 4, 2025].

[38] European Parliament and Council, Regulation (EU) 2023/2675 of 22 November 2023 on the Protection of the Union and Its Member States from Economic Coercion by Third Countries, PE/34/2023/REV/1, Official Journal of the European Union, OJ L 2675, Dec. 7, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2675/oj/eng. [Accessed: Mar. 4, 2025].

[39] Republic of Lithuania, Seimas, "Law on the Protection of Objects Important for Ensuring National Security," No. IX-1132, Oct. 10, 2002. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr. [Accessed: Mar. 3, 2025].

[40] Republic of Lithuania, State Security Department and Second Operational Services Department under the Ministry of National Defence, "National Threat Assessment", Feb. 15, 2024. [Online]. Available: https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-LT-1-1.pdf. [Accessed: Mar. 3, 2025].

[41] Lex Mundi, *Global Foreign Investment Restrictions Guide: Lithuania*, 2024. [Online]. Available: https://www.lexmundi.com/guides/lex-mundi-global-foreign-investment-restrictions-guide/jurisdictions/europe/lithuania. [Accessed: Mar. 3, 2025].

[42] Republic of Lithuania, Seimas, "Criminal Code of the Republic of Lithuania," No. VIII-1968, Sep. 26, 2000. [Online]. Available: https://e-

seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555. [Accessed: Mar. 3, 2025].

[43] Republic of Lithuania, Seimas, "Law on Lobbying Activities," No. VIII-1749, Jun. 27, 2000. [Online]. Available: http://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.104674/asr. [Accessed: Mar. 3, 2025].

[44] Chief Official Ethics Commission of the Republic of Lithuania, "Transparency Information System, 2025". [Online]. Available: https://skaidris.vtek.lt/public/home/main. [Accessed: Mar. 3, 2025].

[45] Republic of Lithuania, Seimas, "Law on Political Organizations," No. XIV-1450, Dec. 20, 2022. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a81b677034fa11edbf47f0036855e731. [Accessed: Mar. 3, 2025].

[46] Republic of Lithuania, Ministry of National Defence, "National Cybersecurity Report," 2023. [Online]. Available: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf. [Accessed: Mar. 3, 2025].

[47] Republic of Lithuania, National Cyber Security Centre, "Lietuvos ir Ukrainos atstovai sėkmingai baigė pirmą kartą surengtą pramoninių technologijų kibernetinio saugumo kursą," 2025. [Online]. Available: https://www.nksc.lt/naujienos/lietuvos_ir_ukrainos_atstovai_sekmingai_baige_pirm.html [Accessed: Mar. 3, 2025]

[48] T. Akimova, O. Akimov, Y. Mihus, *et al.*, "Improvement of the methodological approach to assessing the impact of public governance on ensuring the economic security of the state," ФКДПТП, 2021. [Online]. Available: ResearchGate www.researchgate.net [Accessed: Mar. 4, 2025]. http://dx.doi.org/10.18371/fcaptp.v4i35.221969

[49] V. Franchuk, Z. Zhyvko, and A. Kuzior, "The impact of criminal revenue legalization on economic security," Proceedings of the International Conference on Business, Accounting, Management, Banking, and Economics (BAMBEL-21), 2021. [Online]. Available: https://www.atlantis-press.com/proceedings/bambel-21/125960308. [Accessed: Mar. 4, 2025] 10.2991/aebmr.k.210826.013

[50] European Court of Human Rights, UAB Braitin v. Lithuania, Application No. 37944/19, Judgment of 6 February 2024. [Online]. Available: https://hudoc.echr.coe.int/?i=001-225221. [Accessed: Apr. 13, 2025].

[51] European Court of Human Rights, UAB Ambercore DC and UAB Arcus Novus v. Lithuania, Application No. 37943/19, Judgment of 6 February 2024. [Online]. Available: https://hudoc.echr.coe.int/?i=001-225220. [Accessed: Apr. 13, 2025].

[52] Constitutional Court of the Republic of Lithuania, Case No. 14/04, Conclusion on the compliance of the actions of the President of the Republic of Lithuania R. P., against whom impeachment proceedings have been initiated, with the Constitution of the Republic of Lithuania, 31 March 2004. [Online]. Available: https://lrkt.lt/en/court-acts/search/170/ta1263/content [Accessed: Apr. 13, 2025].

[53] Constitutional Court of the Republic of Lithuania, Case No. 40/03, Decision on the compliance of the Decree No. 40 of 11 April 2003 by the President of the Republic of Lithuania 'On the granting of citizenship of the Republic of Lithuania by way of exception', insofar as it provides that citizenship of the Republic of Lithuania by way of exception is granted to J. B., with the Constitution of the Republic of Lithuania and paragraph 1 of Article 16 of the Law on Citizenship of the Republic of Lithuania, 30 December 2003. [Online]. Available: https://lrkt.lt/en/court-acts/search/170/ta1245/content. [Accessed: Apr. 13, 2025].

[54] Lithuania, Regional Administrative Court, Administrative Case No. eI2-3776-1114/2024, 2 May 2024.

[55] Supreme Administrative Court of Lithuania, Administrative Case No. eA-393-520/2023, 8 November 2023

[56] Ministry of National Defence of the Republic of Lithuania, Press Release, "The Court heard the MoD legal team: complaint from a company that is not safe for Lithuania's national interest was dismissed," 8 December 2021. [Online]. Available: https://kam.lt/en/the-court-heard-the-mod-legal-team-complaint-from-a-company-that-is-not-safe-for-lithuanias-national-interest-was-dismissed/. [Accessed: Apr. 13, 2025].

[57] Lithuania, Vilnius Regional Administrative Court, Administrative Case No. I-4964-764/2016, 4 November 2016.

[58] Republic of Latvia, Latvian State Security Service, "Annual Report 2024". [Online]. Available: https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf. [Accessed: Mar. 4, 2025].

[59] Republic of Estonia, Government Office, "Horisondiseire 2024". [Online]. Available: https://www.riigikantselei.ee/sites/default/files/documents/2024-06/Horisondiseire%202024_EN.pdf. [Accessed: Mar. 4, 2025].

[60] C. E. Wallace, Testimony before the Senate Judiciary Committee, "Dangerous Partners: Big Tech and Beijing," 116th Congress, Mar. 4, 2020. [Online]. Available: https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing. [Accessed: Mar. 4, 2025].

[61] Statista, "Which Countries Have Banned Huawei?", 2020. [Online]. Available: https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/. [Accessed: Mar. 4, 2025].

[62] Q. Bu, "Behind the Huawei sanction: national security, ideological prejudices or something else?" China International Strategy Review, 2024. [Online]. Available: https://link.springer.com/article/10.1365/s43439-024-00112-6. [Accessed: Mar. 4, 2025].

[63] Lietuvos Bankas, "Lietuvos bankas revoked UAB Foxpay licence due to serious and systematic breaches", 2024. [Online]. Available: https://www.lb.lt/en/news/lietuvos-bankas-revoked-uab-foxpay-licence-due-to-serious-and-systematic-breaches. [Accessed: Mar. 4, 2025].

[64] Fintechnews Baltic, "Fintech in Lithuania in 2024: Foxpay Collapses, Kevin Declares Bankruptcy, AML Compliance Remains a Challenge," Jan. 6, 2025. [Online]. Available: https://fintechbaltic.com/10118/fintechlithuania/fintech-in-lithuania-in-2024-foxpay-collapses-kevin-declares-bankruptcy-aml-compliance-remains-a-challenge/. [Accessed: Apr. 13, 2025].