UDC 355.02:004.056.5(474) UDC 005.334:004(474)

RESILIENCE BUILDING AGAINST CYBER INSECURITIES IN THE BALTICS

Öncel Sençerman[16]
Aydın Adnan Menderes University, Faculty of Political Sciences, Department of International Relations

Abstract: The Global Risk Report of the World Economic Forum has been defining cyber insecurity as one of the severe global risks since 2023. The Global Risk Report 2024 ranked cyber insecurity as the eight global risk by severity over a ten-years-period. The peaceful environment the cyberspace had provided for almost two decades ended with the release of the Morris Worm, the first harmful malware, in 1988. Since then cyber threats and cyber-attacks have been posing serious dangers to national security. The cyber-attacks on Estonia in 2007 owing to the Bronze Soldier event are considered as an important milestone in cybersecurity studies. These were followed by the cyber-attacks on Georgia in 2008 and on Iran in 2010, which created a serious need for cyber policies, actions, strategies and norms at national and international level like the efforts of the UN, NATO and OECD to overcome the unwanted results of the cyber domain. This study will deal with the Baltic states' cyber capabilities, cyber capacity building, security concerns and cybersecurity challenges from the perspective of small states' security considering the latest developments in Eastern Europe since 2022, the fast advancements in information technology and artificial intelligence. The study will be a desk research focusing on the national strategies, policies and action plans of the Baltic states to fight with the insecurities of cyberspace by using case study analysis as a research method. This study aims to shed light on the vulnerabilities and resilience of the Baltic states facing with cyber insecurities. The scholarship will contribute into Baltic and cyber security studies.

Keywords: Baltics, Cybersecurity, Cyber Insecurity, Small States.

Introduction

Cyberspace is no more safe and it is anarchic. Cyber insecurities are increasing day by day with the fast improvement in information technologies. Artificial Intelligence is another issue worrying the states. The number of cyber-attacks is on the rise. Conventional wars have been transformed into hybrid warfare. Information war utilizing the cyberspace is a popular way of fighting with the enemies these days. These all are enough to make states concern more than ever about their national securities.

Cybersecurity has been a national security issue since the beginning of the 1990s when the peaceful times of cyber arena was over with the first cyber-attacks between the super powers of two blocs and the release of the first harmful malware the 'Morris worm'. The Bronze Night event in Estonia in 2007 and the following cyber-attacks rang a bell for states to think about cybersecurity more seriously because these attacks were directly affecting

[16] Contact Address:osencerman@adu.edu.tr

the national security. For the last two decades the states together with the regional and international organizations have been taking necessary measures to fight with the insecurities cyber arena brought along to the faces of the states. The recent Global Risk Reports of the World Economy Forum (WEF) underlines the important risks waiting for the states in the future and cyber security is one of them.

This study is a descriptive desk research handling with the scholarly literature basically on Baltic cybersecurity, websites of Baltic states' cybersecurity institutions and agencies, governmental data, cyber insecurities, cyber power and information-technology-related international indexes like the Global Cybersecuirty Index of the International Telecommunications Union (ITU), the National Cyber Security Index and E-Government Knowledgebase of the United Nations (UN). This study enjoys international indexes regarding cybersecurity trying to evaluate the cyber power of the states in terms of cyber insecurities. The study focuses on the national strategies, policies, situation reports of the Baltic states to fight with the insecurities of cyberspace by using case study analysis as a research method. It aims to shed light on the vulnerabilities and resilience building of the Baltic states facing with cyber insecurities with the perspective of small states studies in the literature and benefits mostly from the authors from the Baltic region.

Case study and process tracing analysis methods were preferred for this descriptive study. The main aim of this study is to detect the main the risks for Baltic cybersecurity using the definition of cyber insecurity of the latest WEF Global Risks Reports. The Baltic states have vulnerabilities in terms of cyber insecurities owing to being small states, for this reason the study aims to understand the methods these states use for resilience building against cyber insecurities with the perspective of small states studies. This study tries to give an answer to this central research question: What are the methods the small Baltics states use for resilience building against cyber risks prevailing in the region?

The scholarship will contribute into Baltic and cyber security studies. The studies about both of the topics, Baltic states and cyber insecurities, mostly focus on Estonia, the pioneer country in the field of cyber security. However, same importance should be given to Latvia and Lithuania since they are also small Baltic countries which are under pressure of their bigger and stronger neighbor Russia especially for the last decade with the increased cyber threats owing to Russia's alleged hybrid warfare in the neighborhood following the Ukranian war in 2022.

This study consists of four main parts. The first part deals with the cybersecurity and cyber insecurity definitions, the second part gives briefly the perspective of small states studies regarding security concerns and their characteristics in making foreign policy. The third part deals with the vulnerabilities of the Baltic states in terms of cyber insecurities and the final part discusses the methods the Baltic states use for fighting with the cyber insecurities stemming from their vulnerabilities for cyber resilience building.

Cyber Insecurity, A New Challenge for the Baltic States

The concept of cyberspace was first introduced by William Gibson in his famous 1984 science fiction novel *Neuromancer*, where he described it as a complex global network of computers, used by billions worldwide (Akyeşilmen, 2022: 112). The importance of cybersecurity has grown since the 1990s with the widespread use of computers and the

internet, becoming a significant issue for nations to secure their cyberspace. Cavelty simply defines cybersecurity as "the measures taken to protect a computer or computer systems (as on the Internet) against unauthorized access or attack" (2010: 157). According to the International Telecommunication Union (ITU), cybersecurity involves a range of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, and technologies designed to protect the cyber environment and the assets of organizations and users (ITU, 2024).

The evolution of cybersecurity in international relations has been shaped by significant cyber-attacks and conflicts, leading to the development of cybersecurity measures at both national and international levels (Akyeşilmen, 2022: 114). Initially, cyberspace was designed for information sharing, with transparency as a key feature from 1969 until 1988; however, this changed with the emergence of the 'Morris worm,' the first harmful malware, marking the end of an era where the internet was largely free from such threats (116). After major incidents like the 2007 cyber-attacks on Estonia and the Stuxnet attack on Iran in 2010, significant efforts to establish national and international cybersecurity measures began (119). Organizations like the ITU, the North Atlantic Treaty Organization (NATO), the Organization for Economic Cooperation and Development (OECD) and the European Union Agency for Cybersecurity (ENISA) started creating programs and guidelines to help their members secure cyberspace; as a result, states began developing their own national cybersecurity strategies, which include policies, tools and applications aimed at securing national cyberspace (119).

The 9/11 attacks in the USA shifted the definitions of security, threats and priorities in the international system, bringing national security back to the forefront and leading to discussions about the possibility of a "Digital Disaster" against a NATO member (Bıçakçı, 2014: 119). Cyber discussions were overshadowed by the global focus on the war on terrorism after the 9/11 attacks and it wasn't until 2007 when Estonia, a NATO member, experienced cyber-attacks, that the situation shifted (Schmitt, 2019: 269). The political securitization of cyberspace gained momentum after several notable cyber-attacks, such as attacks on the USA in 2006, on Estonia in 2007 and the Stuxnet attack on Iran in 2010 (Aydındağ, 2021). Among them the attacks on Estonia drew widespread international attention to cybersecurity, which also led NATO to initiate a research project aimed at exploring the implications of international law concerning cyber warfare (Schmitt, 2019: 269).

The Estonian case was followed by a similar incident during the Georgian War in 2008, even though the Estonian case was never thoroughly investigated and no state was officially blamed, though Russia was suspected due to the involvement of agents in the cyberattacks following the removal of a Soviet-era statue in Tallinn in 2007, which led to riots known as the Bronze Night (Delerue, 2011). Following the above-mentioned cyber incidents, other well-known cyber-attacks occurred worldwide, including the Sony Entertainment hacking in the USA in 2014, the hacking of the Democratic National Committee during the Presidential Election campaigns of the USA in 2015 and 2016, attacks on Ukraine between 2015-2017, Saudi Arabia in 2017 and the hacking of Macron's campaign during the 2017 French election (Delerue, 2011). Considering these important cyber-attacks, according to Nikers et. al., cybersecurity is a relatively recent field, emerging in the 1980s, nevertheless, for the Baltic states it only became a national priority more recently, particularly following the cyber-attacks on Estonia in 2007 (2019: 171).

Cyber insecurity was first clearly defined in the World Economic Forum's (WEF) Global Risks Report 2023. Cyber insecurity, identified as a severe risk factor, was introduced alongside other global risks like natural resource shortages, extreme weather events and economic downturns. It includes threats like cyber espionage, cybercrimes, loss of privacy, data fraud and theft. In the 2023 report, cyber insecurity is considered one of the top 10 global risks in both the short and long term (WEF, 2024). Previous reports from 2021 and 2022 did not mention cyber insecurity as a global risk, while the 2020 report only highlighted it as a significant risk related to digital fragmentation (WEF, 2024). Cybersecurity was ranked as the 4th most severe global risk over a two-year period and the 8th over a ten-year period. Among stakeholders, including civil society, international organizations, academia, government and the private sector, cyber insecurity poses a significant global risk, particularly for governments and private sectors over a two-years-period (WEF, 2024).

Cyber insecurity arises from vulnerabilities in the cyber environment due to flaws in hardware and software infrastructure often caused by the misconduct of individuals, organizations, or nations (Cavelty, 2010: 157). Cyber insecurity can manifest as cyber warfare, cybercrime or cyber-attacks leading to serious damages and losses for individuals, institutions, organizations, sectors like healthcare and states. As information technology advances, the potential for cyber-attacks increases, leading states to develop doctrines in this area and enhance their cyber defense capabilities (Gündoğdu, 2023: 1332). The absence of physical boundaries in cyberspace means that cyber threats can originate from anywhere, posing a constant threat to cybersecurity. These attacks can range from simple cybercrimes to more significant threats like cyber terrorism or cyber warfare (1334-1335). Cyber-attacks are carried out by using various cyber weapons and methods, such as viruses, spyware, trojans, keyloggers, worms, and botnets. When directed at states, these attacks are often referred to as cyber warfare (1334-1335).

The transition from the peaceful use of cyberspace to its exploitation for malicious purposes in the 1990s has brought about various insecurities, including cyber threats, cyber-attacks, human and financial losses, threats to critical infrastructure and national security, cyber terrorism and cyber warfare resulting in increased global risks in recent years that affect the small Baltic states as well. Baltic states confronting with the insecurities in cyberspace had to take necessary measures to strengthen their resilience against them using different methods small states benefit from.

Small States Perspective for the Baltics

Different types of member states exist in harmony within the United Nations (UN). Among these states, there are large and small states, but there are various approaches regarding how and according to what criteria these definitions should be made. Some states are defined as large or small based on their area, population or Gross Domestic Product (GDP) size. These definitions are, of course, mostly made qualitatively or quantitatively within the framework of certain academic approaches. Therefore, it is not possible to find a universally accepted, established and clear definition of a small state in the international relations literature. For example, in his 1976 study on small states, Amstrup mentions that there are six different approaches to defining these states including the ones that avoid the burden of establishing a fixed definition for small states; attempt to relate the issue of size

to the measurable characteristics of states; stress the factors such as the political internal systems of small states, their geopolitical position and the structure of the international system in their definition; take a perceptual approach; analyze the behavior of small states by focusing on specific conditions and mention the necessity of differentiating the concept of size by incorporating different approaches into the definition (Amstrup, 1976: 165-167). In a manner similar to Amstrup's grouping, Tür and Salık also bring together approaches to these definitions under three different models: quantitative, qualitative and perceptual ones (Tür and Salık, 2017: 7).

Jazbec emphasizes, small states, particularly after World War I, sought ways to integrate into the international community in some manner and following the World War II they became members of the UN and specialized in certain areas or joined regional organizations (2001). NATO under its famous Article 5th provides member states with a standard security umbrella making itself attractive to small states since the primary aim of small states seeking to increase their visibility in the international community is security as they consider themselves disadvantaged in terms of security due to their relative smallness and limited access to resources (Jazbec, 2001). As Cesnakas and Jakstaite suggest since small states have limited capacity to use force in international politics, they often respond to processes initiated by larger states and the foreign policy of small states is less dependent on internal factors such as institutions and the positions of leaders (2019: 24).

Vandenbosch notes that both large and small states have certain shortcomings and since small states have weaker military and economic power, they find it difficult to impose their will on other states, as a result, they are particularly interested in the development of international law, the establishment of international courts and the promotion of institutions, organizations, and tools that ensure a peaceful environment (1964: 304). This interest stemming from their weaknesses leads small states to exhibit certain standard behaviors in their foreign policies and to assume specific roles (304). Tür and Salık summarize the behaviors exhibited by small states in foreign policy as follows: low-profile participation in world affairs; placing importance on participation in international and multinational organizations; pursuing limited foreign policy objectives; limiting policies to their nearby geographical region; preferring diplomatic and economic tools over military ones; following a policy of neutrality in global matters; relying entirely on major powers (alliances) for security; avoiding conflicts with powerful states; supporting international law, norms, principles, and values; promoting cooperation in international matters (2017: 12).

Small states show a limited involvement in global affairs, focus on a narrow range of foreign policy issues, restrict their activities to their nearby geographic region, prefer diplomatic and economic tools over military ones in their foreign policy, advocate for internationalist principles, international law and other morally driven ideals, seek to secure multinational agreements and participate in international institutions whenever possible, often adopt neutral stances, rely on superpowers for protection, partnerships, and resources, strive to cooperate and avoid conflicts with other nations, devote a disproportionate share of their foreign policy resources to ensuring their physical and political security and survival (Hey, 2003: 5). They use various strategies to enhance their stability, security and influence relative to other actors: they may engage with great powers, balance against potential threats, develop hedging strategies or remain neutral and they seek shelter through alliances (Vaicekauskaite, 2017: 10). These strategies share the common goal of increasing security

while reflecting the specific circumstances and vulnerabilities of small states encountering numerous challenges, some of which are vital to their survival like terrorism, environmental disasters, hybrid threats, cyber-attacks and economic and social vulnerabilities (9). Baltic states reflect the basic vulnerabilities of small states especially regarding their security policies. Cyber insecurities pose significant threats for the national security concerns of the Baltic states.

Vulnerabilities of the Baltic States

Estonia, Latvia and Lithuania had to maintain their national identities under the Tsarist Empire and following a short period of independence under the Soviet Union. Following the restitution of their independence at the start of the 1990s these Baltic states searched ways to re-integrate with the Western world especially by becoming members of the European Union (EU) and the NATO considering their security and identity concerns. The eastern and bigger neighbor, Russia was one of the main security concerns regarding the past. The Baltic states envisaged Russia as a threat. The Russian speaking communities and Russian minorities living in the Baltics turned into a foreign policy tool by the Russian compatriot policies starting from the early 2000s. Russia wanted to influence these people living in the region using different methods including cyberspace usage for conducting an information war. The recent developments in the neighborhood that started with the Crimean annexation by Russia in 2014 and continued with the Russian invasion of Ukraine in 2022 increased Russian activities in the region including hybrid warfare that has been deepening the vulnerabilities of the Baltic states.

Fraszka asserts that the Baltic Sea is a key focus of Russia's foreign and security policies, where Moscow actively pursues its vital interests and in the northern Baltic, St. Petersburg sits at the head of the Gulf of Finland, while to the south lies Kaliningrad Oblast, a Russian military exclave and strategic window to the West (2020). These locations allow Russia to strengthen its military presence in the region and the energy sector in the Baltics remains a target for Russian cyber-attacks (Fraszka, 2020). Nyemann thinks that Russia still views the Baltic states as part of its natural sphere of influence, driven by nostalgia for its imperial past and this view persists partly due to the significant Russian-speaking populations in Estonia, Latvia and Lithuania; besides, the Baltic states perceive Russia as a primary threat (2020: 198). In line with these claims, Medvedev also mentioned that there are certain regions where Russia has 'privileged interests' particularly those with which Russia shares 'special historical relations' and maintains friendly ties (President of Russia, 2008). President Putin's efforts to unify ethnic and cultural Russians abroad are also particularly troubling for Baltic nations like Estonia, which view their cities as potential conflict zones (Watson, 2021: 10). Stitilis et. al. assert that the Russkiy Mir Foundation, an institution that promotes Russian language and culture in over 100 countries including NATO nations particularly those bordering Russia, has built a network of influencers in these regions, which can potentially engage in activities hostile to their host nations and exacerbate societal divisions and considering these risks emphasize that the national cybersecurity strategies should address such threats, incorporating measures to ensure the security of cyberspace in the broader context of national security (2020: 2346). Russia's growing assertiveness and the annexation of the Crimea, marking the first forcible change of European borders in decades,

have also renewed focus on traditional security concerns (Vaicekauskaite, 2017: 7). As a result, small European states are reassessing their security strategies in response to a significantly altered strategic environment and to address these new challenges, countries in the Baltic Sea region and Central Europe have started revising their security policies and implementing new measures to address emerging threats (7).

Russia has played a pivotal role in shaping the regional identity and very existence of the Baltic States: Estonia, Latvia, and Lithuania gained independence from the Tsarist Empire around the end of the World War I, however, their brief interwar independence was abruptly ended by the Soviet annexation just before the World War II (Jurkynas, 2014: 116). As to Jurkynas, deep-rooted Baltic-Russian antipathy stems from a significant power imbalance and a clash of identities: while Russia's national identity is built on the victorious and expansive Soviet legacy, this legacy is viewed as a political threat in Lithuania, Latvia and Estonia (2014: 116). According to Nyemann, since 1991 Russia has tried to influence the Baltic states, particularly targeting the large Russian minorities in the region, yet the Baltic states made different political choices, culminating in their 2004 accession to NATO and the EU, which strained relations with Russia and significantly reduced Russia's ability to exert military and economic pressure on these former Soviet republics (2020: 197). As to Jurkynas, recent foreign policy statements by the Baltic politicians have centered around three key pillars: energy security, the EU's Eastern neighborhood and Russia and Europe–US relations; each of these areas is tied to the post-Soviet states' relations with Russia and continues to influence current political dynamics (2014: 114).

The Baltic states feel particularly vulnerable given their small size and proximity to Russia, which pursues an expansionist policy using overt and covert methods, including disinformation campaigns and cyber-attacks as part of hybrid warfare (Gorka, 2024: 4). Watson claims that the Baltic states are confronted with numerous threats in cyberspace, including cybercrime, cyber espionage and disinformation and adds that the concerns about hybrid warfare from Russia, similar to the tactics used in Ukraine, are still prevalent (2021: 10). Gorka states that security threats from Russia have been a significant concern for military strategists and international policy analysts, especially regarding the Baltic states and they have already warned of a high probability of future Russian actions against the Baltic States due to their strategic position at the intersection of Russian and NATO interests (2024: 4-5). Facing these threats, Watson asserts that the Baltic States have bolstered their defensive capabilities to avoid becoming targets of such attacks and Estonia has traditionally been the leading force in cyberspace, while Latvia and Lithuania have been slower to develop their defenses. (2021: 10). As a consquence, protecting against the Russian threat to their territorial integrity and sovereignty has become central to the Baltic states' national security agendas and following the Russian aggression in Ukraine in 2022, these countries have accelerated efforts to strengthen their digital defense capabilities (Gorka, 2024: 5). While membership in organizations like the EU and NATO offers some protection, new security threats such as cyber-attacks and disinformation challenge their defenses (5).

Lithuania's national computer emergency response team recorded 4,088 cyber incidents, with many being of "medium or high impact" in 2021 and after Russia's invasion of Ukraine the focus shifted toward data theft and DDoS attacks, with DDoS incidents making up over 75% of global cyber-attacks (Kaltreider and Bell, 2023: 48-49). In 2022, Lithuania was hit by a wave of DDoS attacks affecting railways, airports, media companies and government

ministries which followed Lithuania's partial restriction on cargo transit to Kaliningrad in line with EU sanctions and were claimed by the Russian hacker group *Killnet*. Between the start of the war and the first quarter of 2023 Lithuania faced 45 DDoS attacks making it the sixth most targeted country in Europe (48-49). On May 16, 2022, the pro-Russian hacker group *KillNet*, along with the volunteer group *Legion* declared a cyber war against ten countries including Lithuania (Warren et. al., 2023: 520). Following Russia's invasion of Ukraine, cyberattacks on Latvia increased by 40% and the Russian state-backed hacking group *Killnet* launched a DDoS attack against Latvia's public broadcasting center in July 2022. In February 2023, the Russian cyber espionage group *Gamaredon* conducted a phishing attack on Latvia's Ministry of Defense (Kaltreider and Bell, 2023: 57-58). Cyber incidents surged ahead of the NATO 2023 Summit in Vilnius with the number of attacks increasing by up to three times and these attacks targeted a Lithuanian regional radio station and a shopping center by spreading anti-NATO messages together with DDoS attacks affecting websites of various companies and news agencies (Janeliunas, 2023: 17). The rising cyber-attacks on the Baltic states especially starting from 2022 increased the cyber vulnerabilities of these states resulting in more serious demands for resilience building against cyber insecurities affecting their national securities.

Cyber Resilience Building of the Baltic States

After regaining independence Lithuania, Latvia and Estonia opted not to remain neutral, but instead pursued integration into Euro-Atlantic institutions, specifically NATO and the EU (Vaicekauskaite, 2017: 14). The Baltic states' security-policy decisions were motivated by the need for 'strategic shelters' to ensure their security and independence from their large neighbor to the East, so the NATO was viewed as their main security guarantor (14). To enhance their security, the Baltic states sought to break away from the Soviet framework and integrate into Western institutional, economic and socio-political structures. Understanding that the security of small states heavily relies on cooperative engagements, the Baltic countries joined or established numerous regional and global organizations in the 1990s including the Baltic Council, the Council of Baltic Sea States, the UN, the EU and NATO. Throughout this process, Lithuania, Latvia and Estonia developed strong institutionalized collaboration among themselves and with the Nordic countries (Jurkynas, 2014: 116). NATO and EU, which the Baltic states managed to become members of, took steps to overcome the vulnerabilities the cyberspace created for its member countries. NATO recognized cyber-attacks as a security risk in its strategic concept in 2010 and acknowledged that cyber-attacks could have impacts similar to conventional attacks and included cyber defence in its collective defence mandate by the 2014 Wales summit and declared cyber space as a military operations domain requiring defence capabilities at the 2016 Warsaw summit. Meanwhile, the European Parliament adopted a cybersecurity directive in 2016, requiring all member states to develop national cybersecurity strategies. In 2017, under the Estonian EU Presidency, the European Commission updated its cybersecurity policy, including the EU Cybersecurity Strategy (Estonian Cybersecuirty Strategy, 2019: 22).

Gromilova thinks that Estonia and Latvia have high rankings when it comes to cyber capabilities according to ITU and it is clear that both countries have deep security concerns about its eastern neighbor, Russia, especially in light of the ongoing hybrid war in Ukraine and

former Russian cyber activities during its war in Georgia and its possible involvement in 2007 Estonian events (2017: 131). It is clear that both countries promote cyber norms internationally and Estonia even provides cyber security trainings to and hosting NATO's cyber-defence exercises (Gromilova, 2017: 131). Lithuania and Latvia have already increased their defense spending to reach the NATO benchmark of 2% of GDP following Estonia's example which has consistently maintained this level (Gorka, 2024: 8-9). Between 2017 and 2022, Estonia led with EUR 140 million allocated, followed by Lithuania with EUR 54 million and Latvia with EUR 16 million and each country plans to allocate an additional EUR 10-16 million to bolster their cybersecurity efforts for 2021-2027 (Gorka, 2024: 8-9). Nikers et. al. state that at the political level, cooperation among Estonia, Latvia and Lithuania in the field of cybersecurity is highly active and the related topics are addressed in various official settings such as the Baltic Council of Ministers and the Baltic Assembly (2019: 167). Similarly, cybersecurity is a key subject in discussions between the Baltic and Nordic countries and these discussions often take place within the larger context of regional resilience against hybrid threats (167). Tumkevic mentions that countries differ in how they approach cybersecurity based on how they define what needs protection, how they perceive primary threats and risks and how they identify the sources of those threats and risks and asserts that Estonia, Lithuania and Latvia view cybersecurity as a top national security issue militarizing cybersecurity issues by focusing on protecting ICT and government information resources (2016: 85). In these countries, cybersecurity challenges are seen as threats to state functionality, with foreign state attacks identified as the most dangerous, so military and defense institutions are responsible for addressing cyber threats (86). Below, resilience building processes of each Baltic states will be discussed.

Estonia

Estonia has been a pioneer in digital innovation, being the first and sometimes the only, country to introduce Internet voting, digital signatures, X-Road, e-taxation, e-Health and numerous other online services (Kaljurand, 2023: 238). This extensive digitalization effort, known as E-Estonia, is one of the most ambitious technological statecraft projects globally and has earned international acclaim (238). In response to extensive hacking attacks in 2007 and this event, dubbed the first cyberwar led Estonia to develop robust cybersecurity policies including the Digital Agenda 2020 and the establishment of the Cyber Security Council (Tumkevic, 2016: 77-78). Some Estonians believe that the attacks were, in a way, a blessing in disguise, serving as a crucial wake-up call that drove significant changes in the Estonian government's approach to cybersecurity (Robinson and Hardy, 2021: 212). Nevertheless, since the 1990s, the Estonian government initiated several IT programs to promote its digital vision and the government-funded Tiger Leap Program, launched in 1997 aimed to equip Estonian schools with ICT infrastructure and as part of this program nearly 4.000 teachers received basic computer training with thousands more trained in the following years (Kaljurand, 2023: 239).

Estonia adopted its first National Cybersecurity Strategy in 2008 motivated by the clear and pressing need highlighted by the large-scale cyber-attacks in 2007 (Kaljurand, 2023: 245). Estonia established the National Cyber Defense League, an organization dedicated to protecting the nation's cyberspace in 2010 and it consists of IT security experts, programmers,

lawyers and management specialists from various sectors who voluntarily assist during cyber-attacks (Gromilova, 2017: 131). The Estonian Information Systems Authority (RIA) was founded in 2011 as the primary hub for cyber security expertise and coordination in Estonia, operating under the Ministry of Economic Affairs and Communications whose duties include developing and managing state information systems, creating relevant policies and strategies, overseeing the application of security standards, organizing cyber security initiatives and addressing security incidents on Estonian networks (Osula, 2015: 7). Within the RIA, the Estonian Computer Emergency Response Team (CERT-EE) handles security incidents within Estonian computer networks (8). The Ministry of Defence is responsible for coordinating national cyber defense, managing the Defence Forces and overseeing related agencies with key functions including developing national defense policies, organizing cyber defense activities. The Ministry also organizes cyber exercises, such as NATO's Cyber Coalition and has offered its cyber range for NATO training, which is currently under discussion (8). Additionally, the Estonian Internal Security Service (KAPO) focuses on detecting and preventing cyber threats through intelligence and investigations, while the Estonian Defense League operates a Cyber Unit dedicated to cyber defense (8-12).

Estonia has also emerged as a key player in shaping global cyberspace policies within the UN framework. Thus, following the 2007 cyberattacks, Estonia used its experience to revive the UN Group of Governmental Experts (GGE) and advocate for stronger efforts against cybercrime at the UN General Assembly (Goa, 2023: 167). Through active promotion of cybersecurity norms across the EU, NATO and the UN, Estonia has built a strong reputation as a leader in cyberspace governance and this reputation has made Estonia a crucial contributor to shaping EU cybersecurity policies: Estonia's long-standing focus on resilience is reflected in the EU's cybersecurity strategy, which emphasizes enhancing Europe's collective defense against cyber threats (Goa, 2023: 167).

Cyber insecurity has become a growing global issue, impacting economic, humanitarian and national security spheres, leading to the development of a new ecosystem of "cyber norm" processes in various forums and formats. These norms, championed by state and non-state stakeholders, aim to enhance the stability of cyberspace; for instance, the United Nations (UN) and organizations like the Shanghai Cooperation Organization, the G7 and the G20 have all worked on establishing cyber norms (Ruth et. al., 2020: 1). The importance of norms and international law is a common theme in the rhetoric of small states, for instance, Lennart Meri, who served as Estonia's president from 1992 to 2001, emphasized this when responding to nuclear tests in Southeast Asia in 1998, stating "the nuclear weapon of small states is international law" and that statement was rooted in Estonia's own national experience (Lupel and Malksoo, 2019: 3). As norm entrepreneurs are typically small states that focus on advancing and reinforcing international norms, Estonia seeks to act as an advocate and facilitator of collaboration among nations with similar values and goals (Kohler, 2020: 17). Hence, Estonia has significantly contributed to shaping and advancing cyber norms at both international and regional levels and actively participated in the UN GGE during the periods of 2009–10, 2012–13, 2014–15, 2016–17, and 2019–21 (Osula, 2021: 25).

Done thinks that Estonia also regards itself as a credible and strong global partner in cybersecurity, so its cybersecurity strategy emphasizes that cyber issues are an integral part of Estonia's foreign policy, particularly in terms of international cooperation on cyber norms and international law recognizing that global discussions on the application of

international law in cyberspace are both crucial and complex (2022: 35). Pernik states that given Estonia's status as a small state with limited human and financial resources, it would be wise to maximize these assets through international collaboration to achieve broader benefits, so the most notable advancements have occurred in two areas: safeguarding critical infrastructure and fostering international cooperation, while the most significant hurdles persist in developing legislation and regulation (2013). Estonia is notable for its efforts in raising awareness and delivering training on various aspects of state behavior in cyberspace, so beside the extensive training provided by NATO's Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, the Estonian Ministry of Foreign Affairs organizes high-level summer and winter schools for diplomats worldwide (Osula, 2021: 25). Moreover, the RIA leads the EU-wide network of cybersecurity experts, CyberNet and partners with the EU's Cyber for Development Project (Cyber4Dev), which aims to enhance cybersecurity in Africa, Asia, Latin America, and the Caribbean through various training initiatives (Osula, 2021: 25). The five-year Cyber4Dev project marked a significant achievement in executing international projects where Estonian experts played a key role in developing national cybersecurity strategies for Botswana, Ecuador, Mauritius, the Dominican Republic, Costa Rica, Mozambique and Cambodia and they also contributed to establishing national Computer Emergency Response Teams (CERTs) in Botswana, Mauritius, Sri Lanka and the Dominican Republic (Information System Authority, 2024: 5051).

The 2007 cyber-attack on Estonia, however, became a pivotal moment, significantly increasing the country's participation in the EU's cyber policy efforts (Gao, 2023: 165). This attack provided Estonia with a unique opportunity to gain more influence in the cyber domain, which was largely because the conventional understanding of violence and force was disrupted, allowing Estonia to challenge the status-quo and help shape new norms, policies and institutions within this policy area (Gao, 2023: 165). Goa claims that Estonia leveraged this attack to establish itself as a leader in cyberspace governance and to prioritize cybersecurity on the EU agenda (2023: 166). Through its 2008 Cybersecurity Strategy, Estonia emphasized the importance of cybersecurity and cooperation among EU member states, so advocated for enhanced collaboration on cyber-attack investigations and the promotion of international projects aligned with EU cybersecurity policies (166). Estonia has closely collaborated with the EU to establish an IT center within the country and has been actively involved in promoting cyber defense across various international organizations championing cyber defense in the Council of Europe, working with the Association of Southeast Asian Nations (ASEAN) to harmonize laws on cybercrime and contributing as an expert to the UN task force on developments in ICT (Crandall, 2014: 37).

Along with the regional and international cooperation, Estonia benefited from bilateral cyber relations as well. The USA and Estonia completed their third cyber dialogue in 2019 during which they initiated a collaboration to develop a joint platform for securely sharing cyber threat intelligence between the US Department of Defense and the Estonian Ministry of Defense. (Kohler, 2020: 16). Estonia has actively involved in cyber-related bilateral discussions, cooperation or agreements with several countries and organizations that include the Organization of American States (2014), the Netherlands (2015), Japan (2016), the Republic of Korea (2017), Iceland (2017), the Republic of Mauritius (2017) and Singapore (2018) (16). The Nordic-Baltic Cooperation is a regional collaboration established in 1992 involving five Nordic countries (Finland, Sweden, Norway, Iceland, Denmark) and three Baltic countries (Estonia,

Latvia, Lithuania) which focuses on discussing regional and international issues including holding an annual roundtable on cybersecurity topics since 2014 (16).In 2017 Estonia chose to partner with Luxembourg to create the world's first data embassy, which enables the country to store its data in a dedicated section of data centers under Estonian jurisdiction (Kohler, 2020: 6). In addition, one year later Estonia appointed Heli Tiirmaa-Klaar, formerly head of cyber policy coordination as its first Ambassador at Large for Cyber Security. The following year, in September 2019, the Ministry of Foreign Affairs established the Cyber Diplomacy Department under the Undersecretary for Political Affairs (Kohler, 2020: 9). Estonian cyber diplomacy focuses on state behavior in cyberspace, establishing rules and norms for states, combating international cybercrime and safeguarding a free and open internet (Ministry of Foreign Affairs of the Republic of Estonia, 2024).

The National Strategy Document of Estonia (Estonian Cybersecuirty Strategy, 2019: 24-25) states five strenghts in cyber sector: Establishing a Secure Framework for Estonia's Digital Society: Estonia's digital infrastructure is built on secure electronic identities issued by the government and the X-Road data exchange layer, which has facilitated rapid digital innovation and ensures that security is seamlessly integrated into citizens' daily lives. A Proven Level of Maturity: Estonia's cybersecurity is supported by a well-functioning digital society, a robust digital identity system, mandatory security protocols for government institutions and critical service providers, a centralized system for monitoring, resolving, and reporting cybersecurity incidents, a supportive legal framework, and effective cooperation structures. Efficiency and Agility of a Small Nation: Estonia's cohesive cybersecurity community and strong interpersonal communication enable effective responses to pressing issues, leveraging the efficiency typical of a smaller nation. Estonia's International Influence: Estonia has earned a high international reputation by maintaining its leadership in cybersecurity over the past decade, often introducing and adopting innovative cybersecurity concepts. High Trust Among Citizens: Public trust in Estonia's digital state and services, as well as a general societal awareness of cybersecurity's importance, have been significantly bolstered by the successful handling of past cyber-attacks. Estonia also follows its vision through four key principles: protecting and promoting fundamental rights and freedoms in cyberspace is just as important as in the physical world; cybersecurity is viewed as a crucial driver of Estonia's rapid digital growth, which underpins its socioeconomic progress; security should foster innovation and innovation should enhance security; ensuring the security of cryptographic solutions is vital for Estonia, as they form the backbone of its digital ecosystem (Estonian Cybersecuirty Strategy, 2019: 10).

Latvia

The National Cybersecurity Centre formulates Latvia's cybersecurity policy, oversees its implementation, ensures compliance with the EU's directives and supports the European Cybersecurity Competence Centre, also responsible for preventing cyber incidents and raising public awareness. The Ministry of Foreign Affairs supports international cybersecurity cooperation while the Data State Inspectorate handles tasks related to personal data protection under EU regulations. The Military Intelligence and Security Service monitors ICT for the Ministry of Defence and its institutions, including the National Armed Forces. The NAF and National Guard Cyber Defence Unit assist in managing IT security incidents and

their consequences. Non-governmental organizations contribute by providing support and consultation, while the State Security Service focuses on anti-espionage and internal security (Latvian Cybersecuirty Strategy, 2023: 14-15). The Ministry of Defence is primarily responsible for developing and implementing national cybersecurity policy, but the governance model involves collaboration among various government institutions, private sector companies and cooperation platforms like the National Information Technology Security Council. On June 20, 2024, the Parliament adopted the National Cyber Security Law to strengthen Latvia's cybersecurity and align with the EU directive, which aims for a high level of cybersecurity across the European Union (Ministry of Defence of the Republic of Latvia, 2024).

The cybersecurity policy for 2023 to 2026 aims to enhance the security of Latvia's cyberspace by advancing cyber defense capabilities, increasing resilience to cyber attacks and raising public awareness of cyber threats. The policy is centered around three main priorities: protection, deterrence and development. The five objectives of the national strategy are: strengthening cybersecurity management; advancing cybersecurity and building resilience; promoting public awareness, education, and research; fostering international cooperation and upholding the rule of law in cyberspace; preventing and combating cybercrime (Latvian Cybersecuirty Strategy, 2023).

Lithuania

The National Cyber Security Centre is Lithuania's primary cybersecurity institution, responsible for managing cyber incidents, monitoring cybersecurity compliance and accrediting information resources with missions of serving as a center of expertise for effective incident response and prevention (NKSC, 2024). Since 2018 the NCSC follows a one-stop-shop approach, assisting state institutions, businesses, and residents with cybersecurity issues (NKSC, 2024)In 2023, the Ministry of National Defence (MoND) decided to create the Cyber Defence Command as a new structural unit within the Lithuanian Armed Forces to enhance the planning and execution of cyber defence operations within the National Defence System and facilitate integrated military planning across all operational domains, including cyberspace coordination (Ministry of National Defence of Republic of Lithuania, 2023: 5). In 2023, the MoND strengthened its cooperation with strategic partners, particularly the US by signing the Defense Cooperation Roadmap 2024-2028, which prioritizes cybersecurity and defense. Specialists from the US Pennsylvania National Guard and the Lithuanian National Cyber Security Centre (NCSC) participated in joint training and shared information on cyber threats (Ministry of National Defence of Republic of Lithuania, 2023: 5).

Lithuania expanded its cyber defense collaboration with the Indo-Pacific countries, such as Japan, Australia, South Korea, Singapore and Taiwan (Ministry of National Defence of Republic of Lithuania, 2023: 6). Lithuania advocates for closer and more coordinated cooperation with NATO and the European Union in the cybersecurity field to avoid overlapping functions and activities. In addition, Lithuania aims to strengthen bilateral political and technical cooperation with other democratic countries with a particular focus on the United States. (Lithuanian National Cyber Security Strategy, 2018: 18) The Regional Cyber Defence Centre (RCDC) operates as a branch of the National Cyber Security Centre under the Ministry of National Defence of the Republic of Lithuania. The main operational goals of the RCDC include enhancing collaboration with strategic partners such as the USA, Ukraine and Georgia

in the field of cyber security, conducting joint cyber threat analysis with partner nations, organizing training programs for cyber security professionals, leading international scientific research in the area of cyber security. (NKSC, 2024)

The Australian-Lithuanian Cyber Research Network (ALCRN) is a joint initiative established in 2022 aiming to bring together cybersecurity researchers, students, and industry and government professionals focused on or interested in Australia and Lithuania between the RMIT University and Mykolas Romeris University, whose first initiative is to establish the Hybrid Threat Centre to conduct joint research on how hybrid threats affect Australia and Lithuania, evaluate the impact of such threats on societies and organizations, investigate the effects on critical infrastructure, including democratic institutions, organize a series of seminars to explore these issues, and produce thought leadership content on the consequences of hybrid threats (RMIT University, 2024).

The national cybersecurity strategy has five key targets: 1. Strengthen the country's cybersecurity and develop cyber defence capabilities, 2. Ensure the prevention and investigation of cyber crimes, 3. Promote a culture of cybersecurity and encourage innovation, 4. Foster close cooperation between the private and public sectors, 5. Enhance international cooperation and ensure the fulfillment of international cybersecurity obligations (Lithuanian National Cyber Security Strategy, 2018). The strategy focuses on strengthening the state's cybersecurity and cyber defence capabilities, preventing and investigating cybercrimes, promoting a cybersecurity culture and innovation, enhancing private-public partnerships (PPP) and boosting international cooperation (2018). To enhance cybersecurity culture, it's important to provide children and students with fundamental cybersecurity knowledge through nursery, preschool, primary, and secondary education programs, as ICT plays a crucial role in educational processes. To ensure effective public-private partnerships the Cyber Security Information Network is used to facilitate the sharing of information, exchange of cybersecurity recommendations, instructions, technical solutions, and other measures that help ensure the cybersecurity of its members (2018: 13).

Cybersecurity Scores of the Baltic States

This study deals with the results of several international indexes in the fields of cybersecurity, cyber power, start-up ecosystems and e-government systems such as the Global Cybersecurity Index, the National Cyber Security Index, the National Cyber Power Index, the UN E-Government Development Index and the Global Startup Ecosystem Index to better understand the strengths and weaknesses of Baltic states' cybersecurity while comparing it with other nations regarding the rankings.

According to the Global Cybersecurity Index (GCI) 2020, an initiative of the International Telecommunications Union (ITU), Estonia's score is 99.48 and its rank is 3, Latvia's score is 97.28 and its rank is 15, Lithuania's score is 97.93 and its rank is 6. Estonia's rank in its region, Europe, is 2 and it comes after the UK, Latvia's is 9 and Lithuania's is 4. The GCI is authorized by the ITU Plenipotentiary Resolution 130, whose primary objectives include monitoring the type, level, and progression of cybersecurity commitment within and among countries; tracking global and regional advancements in cybersecurity commitment; identifying disparities in cybersecurity commitment among countries (GCI, 2020).

However, as different from the data offered by the ITU GCI Index, the National Cyber Security Index (NCSI, 2024) shows Estonia as the 3rd country, Latvia as the 25th country and Lithuania as the 2nd country on its ranking list regarding the national cybersecurity depending on the data between the years of 2016 and 2023 (NCSI, 2024). The objective of the NCSI is to offer an index that measures the countries' readiness to thwart cyber threats and handle cyber crises and it also functions as a repository containing accessible evidence materials and serves as a resource for enhancing national cybersecurity capabilities (NCSI, 2024). The NCSI indicators are designed based on the national cybersecurity framework and at the core of this framework are the primary cyber threats: (1) Disruption of e-services – hindrance in service accessibility, (2) Compromise of data integrity – unauthorized alterations, (3) Breach of data confidentiality – exposure of secrecy (NCSI, 2024).

According to the Cyber Project titled 'National Cyber Power Index 2022' conducted by the Harvard Kennedy School Belfer Center for Science and International Affairs, Estonia and Lithuania have ranked as 25 and 29, respectively among 30 other countries. According to the same index, Latvia is not among the first 30 countries. The Top 10 Cyber Powers are the USA, China, Russia, the UK, Australia, the Netherlands, Korea, Vietnam, France and Iran, respectively. The 'National Cyber Power Radar' shows cyber powers of Estonia and Lithuania in terms of meeting multiple objectives like financial, surveillance, intelligence, commerce, defense, information control, offense and norms and it points out that these two countries radars diagrams are closer to the defense and surveillance zones (Voo et. al., 2022).

The E-Government Development Index rankings of Estonia, Latvia and Lithuania are 8, 29 and 24, respectively among 193 UN member states (The World leader is Denmark with a score of 0.9717). The E-Participation Index rankings of Estonia, Latvia and Lithuania are 3, 29 and 67, respectively among UN member states (UN E-Government Knowledgebase). According to the Global Startup Ecosystem Index 2024 for 100 countries and 1000 cities that has been issued by the StartupBlink since 2017, Lithuania's ranking is 10 in Europe and 16 among 100 other countries. The report deals with eleven different industries including software and data, which also covers cybersecurity. The countries with 'cybersecurity' top industry rankings are Lithuania, Ireland, Hungary, Israel, Canada, Spain and Switzerland in 2024. The report also draws attention to the rising importance of Artificial Intelligence sector. Vilnius city's rating among the cities is 11th in terms of cybersecurity (StartupBlink, 2024).

Conclusion

Estonia, Lativa and Lithuania are small Baltic states. Like every small state they have weaknesses and vulnerabilities. In terms of cyber security, their vulnerabilities originate mostly from the threats coming from the neighborhood in the shape of close interest of the Eastern neighbor Russia, instabilities started in their region with the annexation of the Crimea, the Ukranian war in 2022, cyber threats, cyber-attacks, information war and compatriot policies. Recognizing the weakness they have, the Baltic states have found different methods to build resilience against cyber insecurities within the last couple of decades, in particular following the 2007 Estonian case. The first one was to create necessary national cybersecurity strategies, action plans and responsible instutitions like every other

country immediately after the first cyber-attack on the Baltics. The second method was to pay attention to get the cover of a shelter alliance, which is offered by the regional and international organizations like the EU, UN and NATO. The third one was not to restrict themselves only into their regions and to have international cooperations with other countries acknowledging their weakness coming from limited involvement capabilities in world matters. This included several cooperations around the world in the field of cybersecurity. The fourth method was to use diplomacy as a successful tool, for this reason, especially Estonia paid a lot of importance and attention on diplomatic moves to open the first data embassy and to influence the EU in creating the necessary cybersecurity directives for the members. The fifth method was to pay a great importance on the internationalist principles as a small state to contribute into the creation of norms and international law especially within the EU and UN again with the leadership of Estonia.

The Baltic states chose to integrate with the Western world following the restitution of their independence in the early 1990s and became members of the EU and NATO. NATO with its popular Article 5 gifted them a protective 'shelter alliance', the most important aim of these small states for strengthening their national securities. The 2007 cyber-attacks on Estonia triggered the Baltic states to recognize cybersecurity as an important issue for their national security and without losing time they started to build resilience against the insecurities of cyberspace. Like other small states, the Baltic states used international and regional organizations like the UN, NATO, the Baltic Council and EU to involve into international matters to make their voices heard and to influence the policies for cybersecurity. Among them Estonia helped norm making processes within the UN and EU thanks to its fame in the field of cybersecurity because Estonia had already started to invest in the field in the 1990s with the 'Tiger Leap Program' for the school teachers.

International cooperation and especially cooperation with super powers are also vital for small states and it is obvious for the Baltic states that after rejoining the Western world they closely work with the USA in cybersecurity matters, Estonia and Lithuania in particular. Regarding international cooperation, Estonia and Lithuania are so active to get into cooperation with other nations of the world like Japan, Australia, Sri Lanka, Dominican Republic and Cambodia. Lithuania's RCDC pays significant importance to work closely with the USA and its close neighbors Ukraine and Georgia in cybersecurity. Diplomacy is another method for small states for resilience building and Estonia here again was a pioneer to open the first Data Embassy of the world in Luxembourg and only one year later to appoint an Ambassador at large for cybersecurity paying great importance to cyber diplomacy. The international indexes also show the Baltic states are among the strongest in the world in terms of cybersecurity, yet Latvia seems to be a bit slower than her sister states. Estonia has been pioneering in cybersecurity field especially in creating a 'niché' for herself to contribute into the development of international law.

This study dealt with the three small Baltic states and their resilience building against the cyber insecurities considering their vulnerabilities. The literature on the Baltic states mostly focus on Estonia, maybe because of Estonia's status as norm maker and frontrunner within the field, but further studies are also needed for the two other sister countries: Lithuania and Latvia.

References

- Akyeşilmen, N. (2022) 'Türkiye in the Global Cybersecuirty Arena', Insight Turkey, Vol. 24., No. 3, 2022, pp. 109-134.
- Amstrup, N. (1976) 'The Perennial Problem of Small States: A Survey of Research Efforts', Cooperation and Conflict, Vol. XI, pp. s. 163-182.
- Aydındağ, D. (2021) 'Copenhagen School and Securitization of Cyberspace in Turkey', Propósitos y Representaciones, Vol. 9.
- Bıçakçı, S. (2014) 'NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik', Uluslararası İlişkiler, Vol. 10, No. 40, 2014, pp. 100-130.
- Cavelty, M. N. (2010) 'Cyber-Security', The Routledge of Handbook of New Security Studies, J. Peter Burges (Ed.) Taylor and Francis Group, pp. 166-174.
- Cesnakas, G. and Jakstaite, G. (2019) 'Lithuania's Foreign Policy in the Public Policy Cycle: Efficient Evaluation is Still Missing', Policy and Administration, Vol. 18, No. 1, pp. 22-35.
- Crandall, M. (2014) 'Soft Security Threats and Small States: the Case of Estonia', Defence Studies, Vol. 14, No. 1, pp. 30-55,
- Done, L. (2022) 'Applicability of International Law in Cyberspace: Positions by Estonia and Latvia', RSU Elektroniskais Juridisko Zinatnisko Rakstu Zurnals, Vol. 3, No. 24, pp 30-40.
- Estonian Cybersecurity Strategy (2019) https://www.mkm.ee/media/703/download, (Accessed, 01 August 2024).
- Latvian Cybersecuirty Strategy (2023) https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20(1).pdf, (Accessed, 01 August 2024).
- Lithuanian National Cybersecurity Strategy (2018) https://kam.lt/en/cyber-security, (Accessed, 01 August 2024).
- Fraszka, B. (2020) Baltic States Versus Russian Hybrid Threats, Special Report of Warsaw Institute.
- GCI (2024) Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, (Accessed, 01 August 2024).
- Goa, X. (2023) 'Challenges and opportunities: Estonia's role in shaping EU cybersecurity policy', Small States in EU Policy Making, Högenauer, A. and Misik, M. (Ed.), London, Routledge, pp. 159-174.
- Gorka, M. (2024) 'Baltic States Cyber Security Policy: Development of Digital Capabilities in 2017-2022', Stosunski Miedzynarodowe International Relations, Vol. 3, No. 15, pp. 1-20.

- Gromilova, A. (2017) 'Promoting Cyber Security: Estonia and Latvia as Norm Setters', Analele Universitatii din Craiova, Vol. 1, No. 31, pp. 127-139.
- Gündoğdu, S. (2023) 'Cyber Security as an Influencer in International Politics and Türkiye's Cyber Security Policy Implementation: National Cyber Incident Response Center (TR-CERT)', Journal of Social Sciences, Vol. 3, No. 3, pp. 1325-1337.
- Hey, A.K.J. (2003) Small States in World Politics, London, Boulder.
- Information System Authority (2024) Cyber Secuirty In Estonia, 2024.
- ITU, International Telecommunication Union, https://www.itu.int/en/Pages/default.aspx (Accessed, 01 August 2024).
- Janeliunas, T. (2023) Index of Russia's Influence on Lithuania 2022-2023, Eastern Europe Studies Centre.
- Jazbec, M. (2001) The Diplomacies of New Small States, New York, Routledge.
- Jurkynas, M. (2014) 'Security Concerns of the Baltic States in the Twenty-First Century', Small States and International Secuirty-Europe and Beyond, Archer, C., Bailes, A.J.K. and Wivel, A. (Ed.), New York, Routledge.
- Kaljurand, M. (2023) 'Taking stock of Estonia's multistakeholder cyber diplomacy', Building an International Cybersecuirty Regime, Johnstone, I., Sukumar, A. and Trachtman, J. (Ed.), USA, Edward Elgar Publishing, pp. 238-257.
- Kaltreider, J. and Bell, T. (2023) 'Hybrid Warfare and the NATO Response', The Donald C. Hellmann Task Force Program.
- Kohler, K. (2020) 'Estonia's National Cybersecurity and Cyberdefense Posture', Cyberdefense Report, Center for Secuirty Studies ETH Zurich, Switzerland.
- Lupel, A. and Mälksoo, L. (2019) 'A Necessary Voice: Small States, International Law, and the UN Security Council', International Peace Institute, April.
- Ministry of Defence of the Republic of Latvia (2024) Cybersecurity https://www.mod.gov.lv/en/cybersecurity, (Accessed, 01 August 2024).
- Ministry of Foreign Affairs of the Republic of Estonia (2024) Cyber Diplomacy, https://www.vm.ee/en/activity/digital-and-cyber-diplomacy/overview-cyber-diplomacy, (Accessed, 01 August 2024).
- Ministry of National Defence of Republic of Lithuania (2023) Overview of the Cybersecurity Status in Lithuania: Key Information.
- NCSI (2024) National Cyber Security Index, https://ncsi.ega.ee/, (Accessed, 01 August 2024).

- Nikers, O., Tabuns, O., Pernik, P. and Poga, E. (2019) 'Cybersecurity', Baltic Security Strategy Report, Nikers, O. and Tabuns, O. (Ed.), Washington, Jameson Foundation, pp. 167-182.
- NKSC (2024) National Cyber Secuirty Centre of the Republic of Lithuania https://www.nksc.lt/en/structure.html, (Accessed, 01 August 2024).
- Nyemann, D. B. (2021) 'Hybrid warfare in the Baltics', Hybrid Warfare: Security and Asymmetric Conflict in International Relations, Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (Ed.), London, Bloomsbury Collections, pp. 195–213.
- Osula, A. (2015) National Cybersecuirty Organization: Estonia, NATO CCDCOE, Tallinn.
- Pernik, P. (2013) 'Cyber Space in Estonia: Greater Security, Greater Challenges', International Centre for Defence and Security, Tallinn, Estonia.
- President of Russia (2008) 'Interview given by Dimitri Medvedev to Television Channels Channel One, Rossia, NTV', http://en.kremlin.ru/events/president/transcripts/48301 (Accessed, 01 July 2024).
- RMIT University (2024) Australian-Lithuanian Cyber Research Network, https://www.rmit.edu.au/research/centres-collaborations/cyber-security-research-innovation/australian-lithuanian-cyber-research-network, (Accessed, 15 August 2024).
- Robinson, N. and Hardy, A. (2021) 'Estonia: from the Bronze Night to cybersecurity pioneers', Routledge Companion to Global Cybersecurity Strategy, Romaniuk, S.N. and Manjikian, M. (Ed.), New York, Routledge, pp. 211-226.
- Ruhl, C., Hollis, D., Hoffman, W. and Maurer, T. (2020) Cyberspace and Geopolitics: Asssesing Global Cybersecurity Norm Processes at a Crossroads, Carnegie Endowment for International Peace, USA.
- Schmitt, M. N. (2014) 'The Law of Cyber Warfare: Quo Vadis', Stanford Law and Policy Review, Vol. 25, pp. 269-300.
- StartupBlink (2024) Global Startup Ecosystem Index, https://www.startupblink.com/startupecosystemreport2024.pdf, (Accessed, 01 August 2024).
- Stitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S. and Khorunzak, N. (2020) 'National Cyber Security Strategies: Management, Unification and Assessment', Independent Journal of Management and Production, Vol. 11, No. 9, pp. 2341-2354.
- Tumkevic, A. (2016) 'Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats', Baltic Journal of Political Science, No. 5, pp. 73-87.
- Tür, Ö. and Salık, N. (2017) 'Uluslararası İlişkilerde "Küçük Devletler": Gelişimi, Tanımı, Dış Politika ve İttifak Davranışları', Uluslararası İlişkiler, Vol. 14, No 53, pp. 3-22.

- UN E-Government Knowledgebase (2024) E-Government Development Index, https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index, (Accessed, 01 August 2024).
- Vaicekauskaite, Z. M. (2017) 'Secuirty Strategies of Small States in a Changing World', Journal on Baltic Secuirty, Vol. 3, No. 2, pp. 7-15.
- Vandenbosch, A. (1964) 'The Small States in International Politics and Organization', The Journal of Politics, Vol. 26, No. 2, 1964, pp. 293-312.
- Voo, J., Hemani, I. and Cassidy, D. (2022) National Cyber Power Index, Cyber Project for Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Warren, M. Stitilis, D. and Laurinaitis, M. (2023) 'Cyber Lessons that the World Can Learn From Lithuania', Proceedings of the 22nd European Conference on Cyber Warfare and Secuirty, ECCWS 2023, pp. 517-524.
- Watson, W. (2021) 'Baltics and NATO in cyberspace', Baltic Cyber Resilience, Nikers, O. and Tabuns, O. (Ed.) Baltic Security Foundation.
- WEF (2024) World Economic Forum, https://www.weforum.org/ (Accessed, 01 August 2024).