University of Twente
Faculty of Behavioral Management and Social Sciences

Universität Münster
Institut für Politikwissenschaften

Summer Semester 2024
1st Supervisor: Dr. Ringo Ossewaarde (UT)
2nd Supervisor: Dr. Hendrik Meyer (UM)

The New Baltic Way
–
Baltic Identity amidst the Geopolitics of Digital Transformation

Executive summary

This thesis explores the geopolitics of digital transformation in the Baltic states - Estonia, Latvia, and Lithuania - through the lens of constructivist identity theory. It investigates to highlights how these states, often perceived as a homogenous bloc, uniquely integrate emerging technologies into their foreign policies, defense strategies, and national identities. This study aims to answer three sub-questions: the extent to which digital transformation is visible in Baltic foreign policies, the differences and similarities in their approach, and how the political control of emerging technologies, particularly AI, can be explained through their geopolitical strategies. The key findings reveal distinct national approaches. Estonia is recognized as a pioneer in e-governance, leveraging its digital identity to influence global standards and policies with a focus on cybersecurity, digital public services, and international cooperation. Latvia prioritises combating disinformation and propaganda, emphasizing communication and defense to protect national security from external threats, particularly from Russia. Lithuania focuses on comprehensive cybersecurity and strategic economic growth, integrating AI and fostering robust IT infrastructure to enhance national security. The term “new Baltic Way” describes the collaborative yet distinct approaches of the Baltic states in navigating the geopolitics of emerging technologies. Each state finds its niche, reinforcing its national identity while enhancing security within the broader European context. All three states, exemplify how small states can leverage digital technologies to enhance national security, economic growth, and international influence, offering a valuable lesson to the emerging geopolitics of digital transformation.

Table of Contents

1. Introduction

1.1. The Rise of Geopolitics of Identity

The tumultuous 20th century was that of ideologies, one in which national identity was built upon pre-formed archetypes (Oswald, 2000). Thus, the rupture of the collapsed Soviet Union led scholars like Francis Fukuyama to believe we would see the "end of history" as the ideology-driven world suddenly lost its divide, resulting in a peaceful global community (Fukuyama, 1989). However, the resurgence of 15 new states was formerly known as one, showed that identity was suddenly multi-faceted and scattered, as overnight, states like Estonia, Georgia, or Kyrgyzstan stood in front of the challenge to re-form a national identity, frantically decoupling themselves from the heralded archetype of the *homo sovieticus* and inventing their own (Oswald, 2000). The optimism to undergo this transformation has however been repeatedly diminished and challenged by the self-proclaimed USSR-successor-state Russia, visible in the resurgence of aggressive foreign policies and neo-imperial ambitions, since the presidency of Vladimir Putin, as he repeatedly trivializes and questions their sovereignty and separate identity (Hodunova, 2024). "As an international actor, Russia is at a point where it recognizes all former borderland republics as *separate countries*, even if it does not yet see all of them as *foreign states*" (Trenin, 2011, p. 14), casting a long shadow over the quest to create their own archetypes.

While 'the West' is still the proclaimed 'Other' for Moscow, other post-Soviet states have re-negotiated their identity and alliances, slowly transforming Russia into the 'Other` (Neumann, 1998). Seeing its sphere of influence dwindling, the Kremlin incessantly repeats that "the enemy is on our doorsteps, [and] we have to defend every Russian and every household against the West" (Thom, 2023, p. 1), now directly targeting its former allies, as these 'households' are scattered around all former SSRs, being the remnants of old Russification policies. As countries like Moldova, Georgia, and Ukraine a moving closer to their European neighbors, they have become victims of the Kremlin's 'defense against the West, using compatriots[1] as means and justification for its actions. Living with this echo of their post-Soviet societies, especially since Vladimir Putin's presidency, has been grounds for conflicts over the last 20 years, making their search for identity more

[1] Term to describe Russians living abroad.

complex than anticipated. In Moldova, this led to the separation of Transnistria in the early 1990s, while in 2008 Georgia lost Abkhazia and South Ossetia, resulting in numerous pro-Russian (not internationally recognized) autonomous republics mostly populated by ethnic Russians (Tsereteli, 2014). The latest event where a similar tactic can be seen is the regions of Donbas, Luhansk, and Crimea in 2014, currently culminating in an already two-year-long full-scale invasion, inter alia targeting Ukrainian identity and autonomy (Flockhart & Korosteleva, 2022; Pieper, 2018). Therefore, Putin's concern about Russia's 'near abroad' is based on Russian self-identification, constantly coming at the expense of the sovereignty and autonomy of its neighboring states, as soon as they try to diversify their foreign policy approaches.

A special place in this newly formed geopolitical dynamic is occupied by the Baltic states, Estonia, Latvia, and Lithuania, which never considered themselves accessor states to the USSR but occupied by it (Taagepera, 1990). To remind the world of their fate of being involuntary Soviet states resulting from the Molotov-Ribbentrop-Pact, in 1989 a 690km-long human chain from Vilnius, over Riga to Tallinn was formed, known as the Baltic Way (Wright & Tambur, 2021). This Way marked the start of the USSR's dissolution, quickly leading to the Baltic's sovereignty and quest to find its new position in the global arena. Thus, it is no surprise that they not only re-formed their identities but actively aligned them with the European identity policies and positioned their security juxtaposed to Russia by joining NATO in 2004 (NATO, 2023). This distinguishes them significantly from their post-Soviet counterparts, as their sovereignty is guarded by their international alliances, having prevented events similar to that of Moldova, Georgia, and Ukraine.

However, their situation resembles a proxy conflict, as they are used as leverage against various other (Western) actors, knowing well they cannot be returned to Russia's sphere of influence (Galeotti, 2019). This is done by making the Balics' foreign policy a Russian national matter (Loh, 2024) best seen when in 2023, Vladimir Putin reached out to criticize Latvia's new resident policies, claiming it wanted to "simply throw out ethnic Russian people from their [Latvia's] borders" (Whyte, 2024, p.1). The trivialization and undermining of the Baltics' separate identity have become a constant since their independence, with the former Russian general staff officer openly claiming that "the trouble with the Baltic States is that they are full of Balts." (Galeotti, 2019, p.2). Not being new to the questioning of their sovereign identity, the Baltic states quickly decided to not only align their identity with the West but also make themselves future-proof by understanding that digitalizing their societies is the way to approach it in the 21st century. Only 33 years after their independence and merely 14 years after they acceded to EU, NATO, and the Nordic-Baltic Cooperation (NB8) they are recognized for their digital transformation, exemplified by the Estonian e-government, the Latvian digital innovation hubs, and Lithuanian fintech start-up infrastructure (The Baltic Times, 2023a). All three states have comparably fast Internet connections, advanced digitalized public sectors, or even made access to the World Wide Web a fourth-generation human right, standing out as their history and size would suggest otherwise (Song & Changshan, 2022; The Baltic Times, 2023b).

As the Baltic states are once again navigating the treacherous waters of Moscow's geopolitical strategies, Russia is seeking political, economic, and social influence on domestic issues (Epp, 2012). Thus, it comes as no surprise that digital transformation plays a crucial role not only in building but also in safeguarding the Baltic's identity, trying to find and secure their places in the Western identity, international partnerships, and security alliances.

1.2. The Emergence of the Geopolitics of Digital Transformation

The Baltic states were able to foresee the digital transformation, deciding to prepare in advance by digitalizing their societies and joining international alliances. When the geopolitics of digital transformation officially made its entrance on February 4th, 2022, as the Xi-Putin "no limits" pact[4] was declared, it did not come as a surprise (Ciuriak, 2023). Paired with the simultaneous disruption by the large language model (LLM) ChatGPT, Artificial Intelligence (AI) was officially introduced into our everyday lives as well as geopolitics. As the Soviet Union [Moscow] has historically waged a non-kinetic political, economic, and social war of ideologies (called: active measures) against the West, taking the step to use new emerging technologies to intensify this strategy was only logical. (Ciuriak, 2023) The Baltics now belonging to the proclaimed 'Other' but also being a former ally, catapulted them into a precarious situation, being targets that cannot be touched. Thus, it is the digital transformation that has allowed Moscow to continue its war with the West (and thus the Baltics) opting for economic coercion, disinformation,

[4] A new strategic partnership also including technological cooperation in disruptive technologies.

propaganda, and cyber disruption, to subsequently challenge our ideas of sovereignty and war (Flockhart & Korosteleva, 2022; Herdt & Zublic, 2022).

New emerging technologies of the digital transformation such as AI, or 5G are now able to do, what could not be done before: attacking crucial structures such as power grids, water systems, or communication networks without physically being present – leading to gray zones of international law and order (Chahal, Fedasiuk, & Flynn, 2020; Crosby, 2020). These new so-called grey zone operations are feeding off of revisionist states, seeking to push the limits of hybrid warfare, using vast amounts of data for economic and military advantage (Ringhof & Torreblanca, 2022). AI offers to bring conflicts and wars beyond the physical into the digital battlefield, involving civilians and policymakers alike, as the automation and vast capacities allow them to act faster and achieve higher outcomes (Urbina, Fabio, et. al., 2022). This rings a new era resulting in the blurring of lines between traditional understandings of war and peace and threats challenge the notion of territorial sovereignty in the digital realm, where borders are not as clearly defined as in the physical world, or rather practically absent (Boyle, 2020; Martin et al., 2023).

The Baltic states are frequent targets as the large-scale use of these technologies allows circumventing direct physical attacks, which in their case would alert their NATO partners and lead to unforeseeable conflicts. Therefore the Baltics must be considered simultaneously a crucial but also weak link within the construct of Western foreign policies and security, ultimately posing a security threat in the mid-to-long term (Sytas, 2023). Increasingly using AI-enabled automated exploitation of websites and malware leads to phishing and swarm attacks aimed at its critical infrastructures, intending to influence, distort, and sow distrust in Baltic civil societies which means, that they are already amid conflicts (Dov Bachmann, Putter, & Duczynski, 2023; Priyono, 2022). Digital political warfare via e.g., denial of service attacks (DDoS)[5] is actively used to target Baltic identity by using new digital tools. This can be seen as the Estonian e-government experienced such attacks in 2007, when it actively denounced Soviet identity by demounting tank monuments, whereas Lithuania is frequently targeted as a 'troublemaker' in separating mainland Russia from its exclave Kaliningrad, undermining

[5] Malicious attempt to disrupt normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate requests, rendering its unavailable to legitimate users

Russian unity (Higgins, 2022; Roussi, 2022). The verbal and physical threats targeting the Baltic's identity, however, can mostly be seen in Latvia, encountering countless attacks not only aiming at DDoS but actively addressing its population including the 37% ethnic-Russian minority. While Estonia and Lithuania also have a sizable number of compatriots (24% and 6% respectively) it is in Latvia where Kremlin-hackers capered the Facebook-like social media website Draugiem, inserting a Russian flag and a message saying "Fellow Latvians, this concerns you. The Russian border has no limits!" (Antoniuk, 2022, p. 3). Hence, "information warfare can be perceived as 'identity warfare' where the domestic-international divide is challenged, the borders are blurred and the identity of the nation-state is contested but there is also the possibility that nations will adapt and not crash under the new identity paradigm formed by cyberspace and its tendency to blur lines and borders" (Ciolan, 2014, p. 2). Thus, digital warfare is becoming a new key component against the identity-building of the Baltic states, certainly crossing lines but not borders.

Given the comeback of Russian aggression, some scholars now assume a new Cold War exacerbated by modern technology like AI or 5G. However, the nature of war has altered, as the digital sphere must be regarded differently than the physical world, and thus the options each country has within (Ciolan, 2014). Therefore, this is not a new Cold War but a "world that is at war – hot war, cold war, technological warm trade war, social war, and internecine political war" (Ciuriak, 2023, p. 2), due to ongoing multiple intersecting crises (polycrisis) exacerbated by digital transformation. Given the realization, that war has become multifaceted – beyond mere physical capacities - it is surprising, that small, targeted states like Estonia, Latvia, and Lithuania have not been studied as the digital world enables them to power beyond the limiting physical world (Kunkunrat, 2022). As the focus in the geopolitics of digital transformation nearly exclusively lies on the USA and China, with some also studying Russia or the Indo-Pacific region, the digital possibilities of small states to employ emerging technologies to safeguard identity and engage in digital warfare are under-highlighted, ignoring their increased potential. Disproportionately targeted, however, they are also drafting policies around the current black-box-like technology with *über*-human potential, having patiently observed how AI "[…] became a major redistributor of power among states and a significant force shaping international relations." (Franke & Torreblanca, 2021, p. 3). Being at the forefront of techno-nationalism in all but also foreign policies, the question arises of how the digital transformation and subsequent geopolitical changes are shaping their national identities and how small states are using this momentum to leverage political control over a digitalized world.

1.3. Research Question

> The "[…] Russo-Ukrainian war is the first large-scale conventional war of the 21st century, and military observers around the world are watching closely and trying to understand what lessons the conflict will provide for future wars." (Shu, 2023, p. 3).

As the Baltic states, also a placeholder for other smaller states, have gone largely unnoticed in the geopolitics of emerging technologies, their approaches to deal with this paradigmatic shift have been ignored as well as their use of strategic partnerships to politically control and influence the geopolitics of emerging technologies as a response to the digital identity warfare (Chiappetta, 2022). Reevaluating their identity and thus strategic allegiances, and a keen interest in employing recent technologies, Estonia, Latvia, and Lithuania are starting to introduce emerging technologies into their foreign policies, mirroring their overall eagerness and advancement in technology (Ringhof & Torreblanca, 2022). They already invest heavily into their digital infrastructure and R&D, always positioned at the EU median or higher in spending per capita, despite being comparably small and new member states acknowledging their critical position of being under Moscow's cyber-attacks (Górka, 2023). With NATO, EU, and other international alliances revising their foreign strategy from a state of slumber to one of alert, the Baltic states are offered a crucial position within the digital shift in national and international foreign policies (Urbelis, 2020).

It is not only small-countries-approaches but also the visibility of new emerging technologies in foreign policies that are under-studied in the Baltic states, additionally often limited to their post-Soviet identity (Kļaviņš, 2021). Restricting Estonia, Latvia, and Lithuania to their USSR background, neglects the fast and autonomous transformation that enables them to be part of shaping the geopolitical landscape. Although usually diligently working together, grouping the Baltic states is a convenience for the West (since the 1960s), limiting the view on the variety and distinctiveness of the three countries and their respective approaches to digital transformation and a common threat (Paulauskas, 2006). Thus, analyzing their foreign policies helps to understand their differences and the overall approach to how small states navigate not only their (new) identity, but how the digital transformation is actively shaping this quest. Assuming digital identity-building is directly linked to the geopolitics of digital transformation, even and mutually supporting each other, leads to the following research question:

RQ: How can the variety of geopolitics of digital transformation in Baltic foreign policy be explained?

To answer this question an inductive approach is used to find the yet assumed interlinking of national identity-building and the geopolitics of digital transformation. As Ciolan (2014) states identity warfare is digital warfare and knowing that the Baltic states are already amidst the new hybrid conflict between the West and Moscow, finding evidence is most likely within foreign policies, addressed at national security and international actors. Examining how and to what extent the diversity of geopolitics of digital transformation is visible in Baltic foreign relations the first sub-question proposed is the following:

SQ1: How and to what extent is geopolitics of digital transformation visible in Baltic foreign policy?

To analyze this visibility further, highlighting similarities and differences helps to understand how the Baltics' distinct approaches to form their identities within the geopolitics of digital transformation. If they do so, their approaches are bound to be multi-level, as governance has become decoupled from mere state action (Ciolan, 2014). Thus, highlighting different actors, autonomous or collaborative approaches, and innovative ideas could possibly provide valuable insights into their standing in the geopolitical arena. Thus, the second sub-question proposed is the following:

SQ2: What are the differences and similarities in the geopolitics of digital transformation in Estonian, Latvian, and Lithuanian foreign policy?

Lastly, derived from the prevalent idea of the Baltic states as a bloc, dissecting the differences and analyzing their approaches to politically control the geopolitics of digital transformation is needed. Although they share significant parts of their history the Baltic states are to be seen as distinct identities, also assuming different approaches to the digital transformation in foreign policy. Supposing the Baltic countries use technology in their national identity-building and in digital defense, would allow them to link it to their role in geopolitics of digital transformation, possibly seen in their foreign policies. The last sub-question proposed is hence the following:

SQ:3 How can the differences in the geopolitics of AI be explained in terms of the political control of emerging technologies?

2. Theoretical Framework

2.1. Introduction

In the evolving tapestry of global geopolitics, especially after the fall of the ideology-driven 20th century, history did not end but rather took unexpected and unknown turns when new technologies emerged and significantly altered the character of international relations (Oswald, 2000). The new identity war has quickly altered its face with the emergence of digital transformation, showing its inherent janiform character (Kunkunrat, 2022). The theoretical framework provides insight into a web in which identity-building is understood through a digital lens – being a question and an answer to a world in digital transformation. It outlines how small states create their own archetypes of (digital) identity in international relations and how they can defend themselves against these new threats that are targeting this very identity by using emerging technologies. Enabled by a digital world that transcends physical power, a constructivist approach to the reformed power of small states using new forms of political control in security communities is provided, resulting in a framework that encompasses the intricacies of technology in geopolitics.

2.2. The Geopolitics of Identity

The dissolution of the Soviet Union, and thus the end of the Cold War, posed significant questions for scholars of International Relations (IR), as traditional theories such as realism or institutionalism failed to explain anarchy and identity during these times of change (Mengshu, 2020). The collapse has transformed a once bipolar world into a multipolar one overnight, adding 15 countries to the global community, struggling to define their post-Soviet identity for the future. Traditionally, the Soviet Union was a complex construct, being the epitome of identity politics as "the Soviets created nations at least as much as they destroyed them." (Weitz, 2002, p. 9). Since the rise of constructivism in the early 1990s, scholars have much better achieved explaining the collapse of the USSR and the 're-awakening' of various new identities with differing collective memories. In contrast to the nineteenth-century romanticization of nation-building stemming from ethnic and racial purity, constructivism opened identity as a nation's major variable for self-perceptions and subsequent actions leading to the rise of the geopolitics of identity (Vogel & Kunze, 2011).

To understand how post-Soviet states built their current identity it has to be acknowledged that this is a currently persistent struggle e.g., in the Baltic states, not least of all due to ongoing foreign designation by Western actors, denying their differing experiences with Soviet oppression (Kļaviņš, 2021). Although the Baltic states can be analyzed separately from other post-Soviet states due to occupation instead of accession to the USSR, they still can be seen in relation to each other, forming a unique geopolitical, historic, and social bond. Hence, for the lack of a better description, the terms *post-Soviet* and *Baltic states* do offer a point of view to understand *some* aspects of their identities-building process, norms-creation, and self-perceptions, important to understand current events and their role within.

Identifying identity as a driver for a nation's geopolitical actions does not deny the "existence of objective facts" (Mengshu, 2020, p. 3), but merely put these as secondary. Thus, it is no surprise that Wendt lends aspects from neorealists by acknowledging objective interests such as survival, autonomy, independence, and economic well-being, but still denying that a state's survival is its sole purpose (Waltz, 1979). Therefore, acknowledging identity as a geopolitical factor resonates with material facts, as identity can be seen as a tool used to push and legitimize security and sovereignty issues in the evolving global arena. The strive to construct a new national identity follows Wendt's argument that "identities and interests of purposive actors are constructed by these shared ideas rather than given by nature" (Wendt, 1999). Building and deciding upon such a national identity stems from consciousness and (shared) memory, acknowledging the material body of a state but putting non-material factors at the forefront (Mengshu, 2020). Wendt describes four types: *personal*, *type*, *role*, and *collectivity, explained in Table 1* (Wendt, 1999),.

Table 1

Types of identity-building according to Wendt (1999)

Personal (or corporate) identity	Refers to internal characteristics and self-perception of the state as a distinct entity, stemming from culture, history, and political system that shape its unique character

Type identity	Refers to broader categories and classifications of a state based on shared characteristics shared with others like being a democracy, a developed nation, or a member of strategic alliances and international organizations
Role identity	Refers to the role a state assumes in the global arena, shaped by self-perception and others perceiving them e.g., being a leader, mediator, or challenger in the international system
Collective identity	Refers to identity forms by shared norms, values, and understandings stemming from social interaction and self-conception of a group of states, e.g., in the European Union or NATO

All four identity-building characteristics are not mutually exclusive, but rather interconnected most importantly they are dynamic, adapting to social change such as digital transformation (Wendt, 1999). Self-conception, consciousness, and memory build an identity juxtaposed to the ‘Other’. This ‘Other’ is contrasting the standardized homo sovieticus, ultimately manifesting the idea of the geopolitics of identity as a driver in IR, as it formed by agreeing on shared ideas, and knowledge (Mengshu, 2020).

2.3. The Rise of Geopolitics of Digital Transformation

In times when identity is becoming multi-faceted and scattered, digital transformation plays into it by allowing for technology to penetrate various fields, inter alia, geopolitics, significantly altering the face of governance and resulting in e.g., techno-nationalism (Möllers, 2021). Digitalization is a janiform process, that provides faster administration and more efficient supply chains but also offers a broader and more vulnerable platform to attack critical infrastructures (Kunkunrat, 2022). Thus, all aspects of governance are affected ranging from national economies, international diplomacy, or multi-level policymaking. The latter is especially important as it needs to constantly adjust to new threats arising along modernization, making the sphere of security pivotal in the rise of geopolitics of digital transformation (Collins, 1981; Kunkunrat, 2022).

Digitalization, as cyberspace is inherently borderless, bears new challenges to sovereignty and security, making national borders complicated to define and protect. Thus, it comes as no surprise that conflicts have migrated into cyberspace, visible in new threats like cyber terrorism, and cyber war, offering a wide array of new features, ranging from Lethal Autonomous Weapons Systems (LAWS) on the battlefield to cyber propaganda targeting civil society (Ciolan, 2014). Power can also be exerted by various (non-) state actors, single actors working for governments (Kunkunrat, 2022). This new borderless and multi-actor security landscape is described as a 'gray-zone operation' (GZOs), a range of politico-military tools circumventing traditional warfare, exemplified by the infamous 'Gerasimov Doctrine.' Although Galeotti, who coined the name 'doctrine' pedaled back on the importance and purpose of the article 'The Value of Science in Prediction' by General Staff General Valeriy Gerasimov, it can be marked as an important turning point of the importance of technology in geopolitics. Being published in 2013, and subsequently used in academia to explain the Kremlin's behavior, it highlights the tendency of blurring the lines between peace and war in the 21st century, as the latter no longer must be declared to begin (Galeotti, 2018, p. 10). Nevertheless, Russia was not the first and certainly not the last country being inclined to use gray zone operations that are becoming "a more typical pattern in world politics, [as] it will be used in ambitious and active ways by a broad range of actors" (Mazar, 2015).

Most major powers, such as the USA, China, or Russia already make use of gray zone operations such as propaganda, proxy and covert wars, or information operations. The difference between their intentions is, however, their self-perception and, thus, identity in the global community. Revisionist states like Russia are more inclined to use GZOs as their motivations and intentions lie in changing the existent global system "[as they] view existing global rules, institutions, norms, and power balances as insufficient to meet their goals, or unjust, or biased against them, or some combination of all of these." (Mazar, 2015, p. 30). In GZOs, revisionist states see the option to transform the global status quo as they are frustrated with their current positions, influence, and ability to shape international norms and institutions (Mazar, 2015). From a constructivist standpoint, their norm agents are insufficiently equipped to influence institutions, resulting in dissatisfaction with a state’s self-perception and a supposed disrespect towards their identities as nations. Lead by their identification these states are willing to change the international distribution of goods and territories to maximize their security patterns and global standing (Mazar, 2015). Randall Schweller summarizes that “staying in place is not the primary goal of revisionist states. They want to increase, not just preserve, their core values and to improve their position in the system.” (Schweller, 1994, p. 4). Thus, they are willing to undertake military adventurism and violate core norms of the international community by employing strategic gradualism, aiming at approaching key thresholds without crossing them (Mazar, 2015).

Acknowledging that revisionist states are in it for the long game, they launch a “set of interconnected actions calculated to make the gradual progress” (Mazar, 2015, p. 31). Using GZOs offers to undertake actions that are either not important enough for greater escalation or to achieve goals while using fewer resources- monetary as well as personnel. These newly coined gradual approaches can already be found within different existing concepts like ‘salami slicing’ and ‘fait accompli,’ illustrating that GZOs are not new, but rather changing through technology and the increased importance of identity geopolitics (Mazar, 2015). In geopolitics, salami slicing refers to a strategy of implementing small actions that individually might not seem significant but collectively achieve a larger goal that would be unacceptable or provoke a strong response if undertaken all at once. It can additionally lead to “[exploiting] political and economic instability, blur truth [keyword: post-truth era] and dilute international support for a victim” (Colby & Solomon, 2015, p. 12). While this tactic is used in various contexts, it can also be applied to GZOs, as incremental advancement takes away the impact and evades greater consequences. In contrast, a fait accompli is a rather swift and irreversible action, creating a new status quo, and forcing parties to accept the change rather than confront it (Colby & Solomon, 2015). In gray zone operations, this can mean e.g., the occupation or militarization of disputed territories without formal declarations of war. Both concepts are thus “the slow accumulation of small changes, none of which in isolation amounts to a casus belli, but which add up over time to a substantial change in the strategic picture” (Haddick, 2014, p. 1)

Using known concepts in explaining gray zone operation can familiarize and expand the understanding of how revisionist states use them for their benefit. As these concepts are also used in traditional warfare, they can be most seen in connection with recent technologies in geopolitics. Mazar argues that the gradual approach is especially interesting for measured revisionists as they want to "overturn elements of the system without causing general instability […] being patient enough to take a piecemeal approach if it will help balance their mixed goals of transformation and stability" (Mazar, 2015, p. 31). Avoiding the red line of confrontation, GZOs can be nuclear saber-rattling, economic sanctions, or cyber propaganda. The tools make it harder to detect conflicts, as gradualist approaches are measured to establish complicated balances unfolding over time; not taken seriously until a full-on escalation or a fait accompli. Elaborate innovative technology exacerbates the slow unfolding, as unconventional tools and multipurpose use can be used to stay below the threshold of traditional conflict (Mazar, 2015).

Lastly, gray zone operations inherently include the use of so-called 'unconventional tools'- leading to the assumption that the rise in GZOs also comes with a rise of technology in geopolitics. Mazar points out three concepts- hybrid warfare, unconventional warfare, and political warfare- made possible through gray zone operations (Mazar, 2015). Frank Hoffmann defines hybrid warfare as "any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior at the same time and battlespace to obtain their political objectives. States or groups [..] select from the whole menu of tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography, and aims." (Hoffmann, 2009, p. 2). Although it lacks scope when it comes to describing non-violent attacks, hybrid warfare includes a wide array of technological tools, combining them with otherwise conventional tactics. Unconventional warfare is better suited to include non-violent actions from revisionist states, e.g., underground guerilla groups, auxiliaries, or other groups to avoid confrontation. However, unconventional warfare is not able to include a wide range of technological use, usually concentrating on on-site proxy forces, working for a goal that is of secondary interest to the perpetrating actors. Here, political warfare can better explain the use of technology as it aims for fragmentation and instability, using cyber campaigns to convey political messages. Usually political "activities are integrated tightly into political realities and dynamics, and it can only work if it succeeds in molding political realities and perceptions in the intended way." (Mazar, 2015, p. 34). Gray zone operations can thus be best described as a mix of all the tools above, as they all have different aims and can be used to web an intricate tapestry of non-traditional warfare.

To counteract GZO's Finnemore & Sikkink (1998) suggest the formation of *security communities* that can come in various forms on a spectrum from uniformity to sovereignty, to develop a sense of security, resulting in practices and institutions that have a prominent level of transaction. Constructivists, although reluctant on the traditional note of power, acknowledge international organizations' impact on international security norms emphasizing that "shared a common history, common norms, the alliances to which the two actors have been part over time" (Savu, 2021, p. 2). Therefore, security choices are not necessarily based on physical capabilities, but also on normative agreements made with other actors in mind, observed in small states like the Baltics (with limited physical capabilities) joining numerous (Savu, 2021). Pluralist security communities, based on sovereignty, (e.g., the EU) are created by endogenous and exogenous factors such as external threats and technological development, seeking security through coordination. The community then forms social interaction and lastly, an environment charged with positive interaction, mutual trust, and a collective identity (Savu, 2021). Forming a collective identity against (mutual) threat thus motivates nations to act and construct new norms that help to understand emerging politics and policies. Understanding the Baltic unity and diversity within the security communities of the EU and NATO, presupposes the understanding of their essential features and subsequent moral judgment, resulting in rational and logical decision-making of joining as a result of an emotional and historical appeal of past occupation (Finnemore & Sikkink, 1998). Organizations such as the EU and NATO are based on such agreements, making member states adopt shared frameworks and norms easier and quicker and thus offering security frameworks (Finnemore & Sikkink, 1998).

These communities are especially formed via shaping discourse, and thus common speech acts like language and symbols to frame events is of utmost importance to solidify identity within security communities (Savu, 2021). Via post-truth objective facts have become less influential in shaping public opinion than appeals to emotion, personal belief, and identity building – fruitful grounds for characteristically subjective identity war (Ciolan, 2014). Common languages and shared speech acts influence security understandings within security communities as "language comes and assigns a certain meaning, depending on the context […] and in the absence of discourse and language, international reality does not exist and cannot be communicated […] emphasizing that speech acts are means of constructing intersubjective meanings.” (Savu, 2021, p. 3). Intersubjective meanings are, thus, assigned within social groups that can transcend borders and establish stable order and lasting peace. By framing the 2007 Estonian cyberattack as a precedent to the attack on Western democracies, the cyber war is solidified as a coherent story, socializing participating actors, and security communities (Ciolan, 2014). Materializing this threat through speech acts like “viruses”, “firewalls” or “bugs” helps to grasp the impact of the changed warfare, shaping the paradigmatic shift within the security communities, and exerting power over the happenings of the events (Savu, 2021).

This shared language and symbolism, lacking in 20th-century constructivism, is exacerbated by a new phenomenon, pivotal in the new digital warfare - the post-truth era. This shift has significant implications for geopolitics, as post-truth dynamics can lead to the formation of divergent or often conflicting interpretations of international events, challenging the idea of collective national memories (van Dyk, 2022). These conflicting and contradicting interpretations lead to information warfare in geopolitics, where misinformation and disinformation become tools in the state’s geopolitical strategies, as controlling narratives become a source of power. The normative power of language and symbols is exacerbated by the post-truth era and digital technologies, dispersing connotations and influencing actors to perceive and respond to events in a specific manner as security communities form a collective identity, inter alia, through shared language and symbols to grasp the shift of changed warfare. (Ciolan, 2014; Finnemore & Sikkink, 1998). Thus addressing e.g., compatriots in post-Soviet countries is a form to actively shape the internal identity formation of other states, by playing with the identity struggles of these communities (Ciolan, 2014). The rise of the Internet, and subsequent interconnectedness via social media and communication technology, has amplified this trend where increased niches of identity have developed, directly influencing state behavior. Identity politics and post-truth, through the lens of constructivism, are heavily influencing geopolitics’ comeback and the rise of geopolitics of identity (Chacón, 2018; Mazar, 2015).

Observing the workings of gray zone operations shows how complex and multifaceted its use and inherent link to technology is. Traditional warfare has declined, but security dilemmas peace and war" (Schadlow, 2014) show the trend for future world politics. Thus, gray zone operations can ultimately be defined as (1) political objectives pursued through cohesive, integrated campaigns, (2) aim to stay below the escalation threshold and not cross the line, and (3) the gradual move toward the main objective or target (Mazar, 2015). The definition, however, distinctively misses the definition of war and conflict, as legally GZOs cannot be defined as war. As traditionally the absence of war does not constitute peace, scholars are met with the new obstacle of defining this relatively new geopolitical phenomenon, that does not follow traditional rules and expectations of warfare e.g., missing a declaration of war, clear-cut goals, or a victory (Mazar, 2015). The establishment of so-called security communities is one response to the fast-paced environment of gray zone operations, allowing actors especially small states to establish security frameworks based on their values, even going as far as shaping these institutions themselves.

2.4. The Geopolitics of Emerging Technologies

As conflicts have now (partly) migrated into cyberspace, challenging traditional understandings of peace and war, states have become more aware and are trying to protect their digital borders through cybersecurity strategies and other forms of digital regulations. But just as the adaption to human action in cyberspace and conflict has been somewhat adequately understood, emerging technologies are now challenging this awareness once again by introducing an *über*-human notion never known before (Popescu, 2021). Technologies like 5G/6G, independent cloud infrastructure, satellite systems, deep fakes, and the metaverse – but especially Artificial Intelligence - now operate detached from close human surveillance, providing it with an autonomy only known to humans (Popescu, 2021). Thus, they have the potential to be disruptive in geopolitics, as conventional aspects of international influence like economy or military (read: physical abilities), are now challenged by emerging technologies and their strategic advances (Kunkunrat, 2022). Given the possibilities emerging technologies offer, GZOs can be brought to the next level, skewing the current international security framework by automating the aforementioned attacks on e.g., critical infrastructures or dispersion of fake news to compatriots (Silini & Molina, 2024). Although the USA has long dominated this field, while China and Russia are catching up, the shift away from mere physical capabilities defining power and influence, opens possibilities for smaller states such as the Baltics to assert dominance in this field.

The geopolitics of emerging technologies are intrinsically linked to security aspects, as the "technological sprint" (Popescu, 2021, p. 1) encompasses politics, strategy, economy, and society, involving states, international organizations, and private companies alike. As emerging technologies offer to influence beyond physical capabilities but are dependent on multi-level governance and cooperation, aspects of global leadership, sovereignty, and dependency are changing as well, being especially interesting for formerly disadvantaged small countries (Kunkunrat, 2022). Kunkunrat argues that the international arena changed from an agreement-based security framework to a multi-level cooperation, leading to multi-level governance that creates "new forums for information exchange and multilateral diplomacy" (Kunkunrat, 2022), resulting in the aforementioned security communities. These communities are aiming to navigate emerging technologies in need to adapt to constant shifts in the current geopolitical landscape that are based on evolutions, innovations, and navigating new risks (Silini & Molina, 2024). Under constructivism this means that international collaboration can lead to standard and norm settings, resulting in joint (ethical) research, and managing shared challenges like security threats. The EU is an example of such a security community, setting legal frameworks and fostering innovation and ethical use of e.g., AI, hoping to influence the global standard and skewing power balances in their favor as others are dependent on these norms, rules, and standards to interact with the EU (Clüver Ashbrook, 2023). Tilovska-Kechdji even argues, that the major AI powers "balanced out their antagonism and joined forces" (Tilovska-Kachedji, 2023), to stay afloat in the fast-paced environment of new inventions. Additionally, such alliances can also help to rely on indigenous technological infrastructure, lowering the chances of being dependent on other, possibly antagonist, actors. Thus, in addition to forming partnerships countries find anathematic strategies of "strategic outpacing and attempted hermetic closure" (Clüver Ashbrook, 2023, p. 35) in which autocracies and democracies try to find accommodation in areas of technology, supporting Tilovska-Kachedji's assumption of a current geopolitical balance of power in the sphere of the geopolitics of digital transformation.

In security and surveillance matters, new technologies also pose changes within the global arena, as matters of diplomatic or military matters become vulnerable to e.g., AI systems or faster 5G internet. Diplo acknowledges that “Foreign policy and international security are considered to be current hotspots when discussing the use and risk of AI in international politics. Technological developments have raised contemporary issues for discussion on the international scene, posed challenges to geostrategic relations, provided a useful instrument for diplomats and negotiators, and given rise to concerns regarding human rights” (Diplo, 2023, p. 3). In digital times, new technologies can be used as key tools e.g., cybersecurity, threat detection, or even combat systems like autonomous weapons or intelligence analyses. LAWS are as much part of the current repertoire as descriptive analyses in diplomacy and negotiation, or visa application fraud detection (Silini & Molina, 2024). The possibility of using, inter alia, AI in foreign relations, “intensifies anxieties about technological advances fostering global instability and creating unilateral advantages for early technology developers” (Silini & Molina, 2024, p. 3). Therefore, using new *über*-human technologies in gray zone operations offers the possibility to automatize strategic operations within the cybersphere, e.g., using bots in fake news dissemination to target society [post truth], DDoS attacks to attack the critical infrastructure of economy and administration, and intelligence surveillance software to gain advantage for military and diplomatic purposes.

2.5. Varieties of Baltic Political Control of Emerging Technologies

Observing the disruptive character of emerging technologies that allow for the never-known automation of conflicts poses the question of how states act if they can control emerging technologies that trespass traditional forms of power. With the rise of pluralist security communities like the EU or NATO, small countries can finally be part of norm-creation and standard-setting, exacerbated by new digital possibilities. This allows us to question how and to what extent Baltic foreign policies are now controlling the changed geopolitical landscape as unlike materialist approaches, constructivism yet again emphasizes the importance of ideas, beliefs, norms, and identities in shaping actors’, and thus communities’, behavior. As historically occupied and disadvantaged actors with limited physical capabilities, digital transformation, and emerging technologies offer them new opportunities, open to be leveraged as a modern response to unique historical, cultural, and geopolitical contexts (Ciolan, 2014).

The constructivist core is the premise that international relations are a branch of human relations, “considering that the processes of identities and interest formations happen at the same time with the process of interaction” (Ciolan, 2014, p. 10). The emergence of new technologies has accelerated this aspect, as *au contraire* to threats coming from air, sea, or land, cyberspace is entirely human-made and much more complex to handle, needing a variety of actors to respond accordingly (Ciolan, 2014). Acknowledging security as a social and not materialistic threat allows us to understand the concept of social threat exacerbated by technology, as deploying it in times of conflict upholds the idea of the constructivist notion of the ‘looking-glass self’, suggesting that one actor’s action reflects another one's reaction guiding the current security complex (Ciolan, 2014). Supposing that the Baltics already react and mirror Moscow’s actions through the theoretical assumption of the looking-glass self as well as the need to diversify their approach to digital transformation results in political control via tools of norm-setting, discourse shaping, or institutionalization, all within security communities (Ciolan, 2014; Kunkunrat, 2022).

As new emerging technologies are potentially disruptive due to their automation of warfare, Baltic security awareness has translated from a mere perception to a real-life threat, forcing them to take on new measures (Eriksson & Giacomello, 2007). Constructivism emphasizes that paradigmatic events like the emergence of cyber-threats (e.g., the 2007 attack on Estonia) are necessary to form new norms, as they are not merely reactive but actively shaped by actors’ identities, interests, and beliefs (Mengshu, 2020). By identifying their security needs states transfer these into proposals for new norms and standards via norm agents in international organizations, making their security a matter of the community. Thus, to safeguard their identity, states must be actively involved in setting international norms and agreements, which is possible for all actors alike in pluralist security communities – no matter their size. This implies that as traditional forms of influence on intelligence and warfare lost their island position, small states can achieve power in the norm-setting by gathering a critical mass through negotiation and consensus (Kunkunrat, 2022). By being involved in multi-level governance and finding this mass in multiple actors comprised of private, local, global, and individual, small states can now exert power in the international arena no matter their physical capabilities (Ciolan, 2014).

Although traditional warfare has diminished, institutions further play a crucial role in setting the agenda, being longstanding and thus having the ‘memory’ to derive policies from historical experiences, cultural contexts, and political ideologies (Ciolan, 2014). This correlates with the constructivist approach that institutions are not external structures but are directly influenced and internalized by their actors, and thus their behavior and decision-making are derived from this memor (Mengshu, 2020)y. Organizations are therefore socialized into institutionalizing actors’ specific norms and practices through mutual interaction and the establishment of multilateral networks and governance practices. This not only empowers the states institutionalizing but simultaneously legitimizes the institution and establishes mutual collaboration and trust, that the institutions are working in the actors’ interests (Ciolan, 2014).

Thus, under constructivism political control is manifested in various forms ranging from norm-setting in institutionalization to shaping discussions and event perceptions, resulting in a web that allows small countries to leverage never-known control over their and their security communities' identities. The rise of techno-nationalism and multi-stakeholder governance is a direct result of the paradigm shift in security, juxtaposing the “cyber-sovereignty” group of states like Russia and China and relying on international collaboration (Pawlak, 2013).

2.6. Conclusion

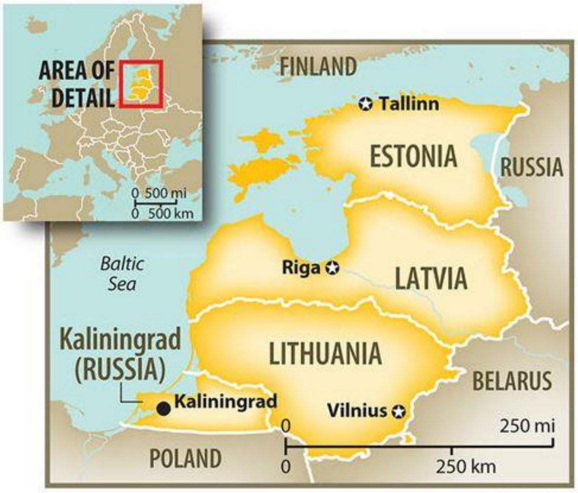
The theoretical framework provides an intricate web to understand how small states react and adapt to the rise of the geopolitics of digital transformation, by interlinking (digital) state identity-building and emerging technologies in modern warfare. While the former supposes a multi-level and international approach, the latter is intensified by current changes in the perception of truth and identity. As the outer characteristics of statehood and conflict have changed, the Baltics are exposed to new threats but also to new opportunities, both being the question and answer to the janiform face of the geopolitics of digital transformation. Small states can profit most, as they have been and still are over proportionately targeted but are now able to leverage power via the digital transformation and pluralist security communities.

3. Methodology

3.1. Introduction

To adequately answer the research question of how the variety of geopolitics of digital transformation in Baltic foreign policy can be explained regarding small countries' new abilities in the geopolitical arena, a two-tiered approach was employed aiming at understanding the Baltic identity and the use of (new) technologies and their inherent interlinking. To understand how small countries globally politically control both, digital identity and digital security, a thematic textual analysis of Estonia's, Latvia's, and Lithuania's foreign policies were chosen, focusing on their self-description, international collaboration, and the use of emerging technologies in security, economy, and diplomacy. This offered insights that are inward as well as outward, encompassing the different types of identity-building and addressing new hybrid threats in foreign policies. Before outlining the methods of data collection and analysis, a case description is provided to understand the Baltic states' distinctiveness and suitability to understand the geopolitics of digital transformation.

3.2. Case Description



RICH CLABAUGH/STAFF

Figure 1: Political map of the Baltic region (PDGA, 2014)

Choosing the Baltic states to understand the geopolitics of digital transformation and its link to the global shift towards identity politics stems from its unique history and distinct geopolitical position. They offer a rich analytical standpoint as they have recently undergone the particular development of identity formation after being grouped and occupied for the better part of the last century, as well as a distinct approach to the trend of digitalization, known as highly technologized countries. Being additionally located on the EU and NATO external borders facing Russia and Belarus adds a security component that few other states can offer for analysis (Figure 1). Their unique interplay of recent history, strategic positioning, and the imperative of establishing sovereignty and exerting power as small states amidst external pressure makes them an invaluable research object (Berg, 2007).

Regarding their historical and social background, and the subsequent need for identity development, Estonia, Latvia, and Lithuania offer the special positioning of being post-Soviet states, that considered themselves occupied rather than part of the USSR, making their collective memory of the 20th century distinctively different from that of other SSR's (Kasekamp, 2019). Although they were striving for the reinstatement of their independence, the Baltics nevertheless faced similar problems in forming a national identity, as they also suffered from the Soviet archetype being imposed, eradicating culture, ethnic homogeneity, and historical memories (Saburova, 1955). These obstacles are visible to this day, as e.g., former Russification policies left Estonia with 24%, Latvia with 37%, and Lithuania with 6% ethnic Russians[7], leading to societal and political tensions since the 1991 independence (Kasekamp, 2019). Although often describing themselves as the "Three Baltic Sisters" (Foreign Policy Research Institute, 2020) and acting accordingly, Estonia, Latvia, and Lithuania are more heterogenic than expected by the West, leading to a unique interplay of collective Baltic and distinct national identity. Table 2 visualizes some of the key differences in Baltic societies, highlighting their unique identities.

Table 2

Key differences between the Baltic states

	Estonia	**Latvia**	**Lithuania**
Language	Finno-Ugric[8]	Baltic[9]	Baltic[10]
Population	1,3M ~300.000 ethnic Russians[11]	1,8M ~445.000 ethnic Russians[12]	2.8M ~145.000 ethnic Russians[13]

[7] We remember the word 'compatriots'
[8] Britannica (n.d.b)
[9] Britannica (n.d.a)
[10] Britannica (n.d.a)
[11] Statista Estonia (2021)
[12] Oficiālās statistikas portāls (2021)
[13] Oficialiosios statistikos portalas (2021)

Imperial influences	Germany, Sweden, Russian Empire, Soviet Union	Germany, Sweden, Russian Empire, Soviet Union	Grand Duchy of Lithuania, Polish-Lithuanian Commonwealth, Soviet Union
Religions	No religion (58.4%) Eastern orthodoxy (16.3%) Lutheranism (7.7%)[14]	Lutheranism (36.51%) Catholicism (19%) Eastern orthodoxy (13.49%)[15]	Catholicism (74.19%) Eastern orthodoxy (4.4%) Lutheranism (0.56%)[16]
Neighbors	Finland, Russia, Latvia	Estonia, Russia, Belarus, Lithuania	Latvia, Belarus, Poland, Russia (Kaliningrad)

Regarding their technological affiliation, the Baltics have already established themselves in the sphere of emerging technologies and digital transformation, guided by their desire to integrate more closely with Western Europe, de-aligning from their past ties to the Soviet Union and Russia (Berg, 2007). This alignment is not just economic or political but also deeply technological, with Estonia known for its e-governance system, Latvia’s start-up-infrastructure infrastructure, and Lithuania’s focus on fintech and blockchain technologies are not only about enhancing efficiencies but also aligning with Western technological standards and practices (The Baltic Times, 2023a). This integration helps build a digital identity that resonates with Western values of democracy, transparency, and innovation, further distancing themselves from Russian influence (Berg, 2007).

Each Baltic state has been leveraging technologies to position itself on the global stage since the early 2000s, making them prime examples to be studied in the realm of digital transformation. Estonia is already known as a global pioneer for its e-businesses and handles its health through online public services (Česnauskė, 2019). In addition to the EU AI Act, the Estonian government launched its “Kratt AI” national AI Strategy as early as

[14] Statistics Estonia (2021)
[15] Tieslietu ministrija (2019)
[16] Statistics Lithuania (2022)

2019, aiming to enhance its already strong public services and boost business competitiveness on the global stage. Following an open approach, emphasizing the transparency of public data, Estonia wishes to extensively fuel innovation and AI development (Djeffal & et.al., 2022). Latvia and Lithuania, while following Estonia's footsteps, are carving out niches in areas like startups and fintech, with Latvia fostering a favorable environment for young firms and Lithuania investing in their R&D intersection (Djeffal & et.al., 2022). Latvia, although being the 'weakest' of the three, also introduced its "Digital Latvia 2020" program in the mid-2010s, focusing on improving digital infrastructure and increasing digital skills among citizens for following e-government services. Following up the strategy, Riga introduced its AI outline in 2021 aiming at integrating AI in public administration, healthcare, and administration (Goldberga, Kreislere, Sauka, Stürmane, & Virbule, 2014). In 2020, Vilnius also initiated its AI strategy to foster development and deployment in various sectors such as healthcare, public services, and finance. Lithuania is a pioneer as it offers a favorable regulatory environment for tech companies, especially in fintech and blockchain technologies, fueling its strategic economic growth and international branding to further intertwine its geopolitical identity with its technological policies (Djeffal & et.al., 2022). Technology and digital governance have emerged as key areas in which these nations can assert sovereignty, modernity, and foremost power. By establishing advanced digital infrastructures and governance systems, they not only strengthen the internal administrations but also project their identities as forward-looking, technologically advanced states on the global stage (Česnauskė, 2019).

What makes the mix of geopolitics of identity and geopolitics of digital transformation distinct in the Baltic states compared to others is the combination of their vulnerable geopolitical positions, post-Soviet identity-building, and aggressive moves towards modernity. These elements have fostered a unique blend where technological advancement is not just a matter of economic strategy but a foundational component of national security and identity, exemplary for small-state approaches to the geopolitics of digital transformation.

3.3. Method of Data Collection

To understand how the Baltic states manage the geopolitics of digital transformation, a focus on their demeanor in the geopolitical arena offers the needed insights. Thus, the data collected focuses on national interests on the international stage, centering the attention on Baltic government documents, policy papers, strategic plans, and international reports from relevant bodies like the EU, OECD, or NATO, that discuss technology and digital governance in the Baltics.

3.3.1. Data Gathering

In this thesis, data was collected from a variety of primary and secondary sources to ensure a comprehensive understanding of the Baltic foreign policies and the visibility of digital transformation within. Primary data is classified as official government-released policies, ensuring first-hand information about how small states communicate their approach to the geopolitics of digital transformation. It data was gathered from official government websites, which provided access to Cybersecurity Strategies, AI Strategies, Defense Strategies, Foreign Policies, and National Threat Assessments, all being national interests translated for the global community. These sources were selected for their direct relevance and authoritative insights into the governmental agendas of Estonia, Latvia, and Lithuania when it comes to their international action and defense objectives. To limit the scope and focus on recent developments, the primary sources used were dated between 2019 and 2024, highlighting the paradigm shift experienced with the COVID-19 pandemic and subsequent digitalization, the escalated Russo-Ukrainian war, as well as the ringed-in era of digital transformation by the "no-limits"-pact by Putin and Xi in 2022 (Ciuriak, 2023). Secondary sources include published academic research and contributions of international bodies like the EU, UN, NATO, and OECD offering evaluative perspectives on the region's compared success in digital transformation. Allowing international bodies, of which the Baltic countries are members, to contextualize Baltic policies from the objective perspective of a bystander, offers to get a counter-checked insight. This is especially important as policies' successes are not always transparently discussed by respective governments.

Ethical considerations were strictly adhered to by ensuring that all data collected from public domains was accurately cited and used solely for academic purposes. Limitations of the data collection process were the exclusion of classified or unreleased governmental data which might have provided additional insights. Additionally, linguistic challenges that arose, were circumvented by either referring to the official translation to English or

Russian[17] as well as translating certain not-yet translated documents into English via DeepL. Despite these limitations, the data collection methods employed were robust and aligned with the thesis's objective, ensuring a solid foundation for analyzing the intersection of identity, technology, and geopolitics in the Baltic states.

3.3.2. Data Organization

Once collected, the data was meticulously organized to streamline the analysis process and reinforce the objective of a thematic discourse analysis. A digital repository was created using the document management software Atlas.ti which allowed for effective sorting and easy retrieval. Documents were cataloged and categorized in two steps. First, by geographical positioning, meaning: (i) Estonia, (ii) Latvia, (iii) Lithuania, acknowledging the sovereign approach of each country within the Baltics. Second by source type meaning primary and secondary sources. The first includes national policy papers, legal documents, and strategic reports, whereas the latter includes international reports, documents, and reports as well as academic articles, establishing a hierarchy based on their importance and authoritativeness. Thus, for Estonia 17, Latvia 15, and Lithuania 16 primary sources were chosen and used for the context of this thesis. The divide between national and international helped to prioritize Baltic foreign policy approaches and merely complemented the data set by using information provided by international bodies. This systematic organization not only facilitated efficient access during the analysis phase but also aided in maintaining a clear overview of the data landscape, ensuring all relevant materials were readily available and manageable throughout the research process. This level of organization was crucial for supporting the subsequent phases of coding and thematic analysis argued in the next chapter.

3.4. Method of Data Analysis

For a case study approach such as in this thesis, a thematic content analysis offered a suitable method to find, compare, and interpret the Baltic way of interlinking the geopolitics of identity with the geopolitics of digital transformation. Thematic analysis allows for an open and inductive approach, leaving room for unexpected findings, which was anticipated due to the under-researched small-state approaches. Originally coined by Virginia Braun and Victoria Clarke, the thematic analysis allowed drawing out and

[17] both languages widely used in the administrative field of the Baltic countries

interpreting data patterns found in foreign and digital policies in the Baltic states, offering insights into how these policies are intertwined with national identity and geopolitical ambitions (Braun & Clarke, 2012). This method provided a solid foundation to build a compelling analytical narrative and allowed it to be deployed flexibly to adequately answer the intricate research questions, that simultaneously aim at identity and technology deployment. The original authors used six steps for their method of thematic analysis, however, due to the scope of this thesis, the last four stages were merged into two, resulting in a more compact and inductive approach that allowed for staying open and vigilant to the nuanced topic of identity and digital transformation. Simultaneously the structured approach ensured rigorous examination of the data, supporting the reliability and validity of research findings to identify important themes for analytical interpretations.

3.4.1. Data Familiarization

In the first step toward a thematic analysis, the data chosen was read and re-read to gain a comprehensive understanding of the content and context. This involved in-depth reading and re-reading of the collected documents, which include policy papers, strategic plans, and international reports relevant to digital governance and AI strategies in the Baltic states. During this stage, meticulous notes were taken to capture key concepts, recurrent themes, and initial insights that emerged from the data, attention was paid to both the explicit content and subtler nuances of the text such as the tone and the implied assumptions, which could have influenced later coding and thematic development. This deep engagement with the data ensured a more informed and grounded approach to generating initial codes and eventually themes. A robust platform for the analytical rigor required in the later stages was built by systematically documenting observations and reflections during this phase.

3.4.2. Coding Scheme

The second step was the coding scheme being a fundamental component within this thesis and the thematic analysis process, serving as a mechanism through which raw data was organized into manageable and meaningful segments. In this thesis, coding will be initiated post the familiarization phase, primarily inductive and allowing themes to emerge organically from the data rather than imposing preconceived categories. This ensured that the analysis remained closely aligned with the actual data; facilitated by the qualitative analysis software Atlas.ti, which supported the organization and retrieval of data efficiently. Each text segment relevant to the research questions was coded with a short, descriptive label that captures its essence. This included both manifest content (explicitly stated information) and latent content (underlying ideas). The coding process was reflexive, and codes were constantly reevaluated, removed, and added according to the data work. This structured yet flexible coding strategy was designed to ensure that all pertinent data is captured, and categorized in a way that genuinely reflects the complexities and nuances of the topic. Table 3 displays the final codes used during the analysis, having emerged during the aforementioned two steps of the thematic analysis framework. The number of codes is more extensive than usual and expected, however, the open coding process allowed for and revealed the abundance of Baltic geopolitics of digital transformation. Other codes that have emerged but have not resulted in relevant findings have been discarded.

Table 3

Relevant codes and descriptions

Code	Explanation
Cyber diplomacy	The use of technology for diplomatic use in fields of economy, humanitarian aid, and foreign relations
Digital identity	Strong ties of cyberspace to national and societal identity
Digital leadership	Self-awareness to holding a leadership position in the field of technology in the world
Digital security/ security threat	Acknowledgment of cyberspace being a threat to national/international security
Cyber attacks	Detection and description of different forms of digital attacks on national infrastructures
Identity threat	The external threat to national identity via technological tools
International cooperation	Strong incline to use bi-and multilateral cooperation in the sphere of technology

Baltic cooperation	Emphasis on the Baltic unity and their shared interest in technology in international relations cooperation
AI for security	The use of AI-enabled systems for national/international security
Cyber Defense	National/International defense provision in the cyberspace
Regional cooperation	Cooperation in the field of technology with actors seen as regional partners, foremost former Soviet Union members
Regional security	Technological threats that are directly related to regional security
Societal issues	The mentioning of societal issues in relation to the digital sphere
Security threat	The perceived security threat from other parties also exceeds the technological sector
Western identity	Highlighting of identity markers that are directly related to the Western identity and values
AI for the economy	The use of AI in the private sector
AI for the public sector	The use of AI in the public sector, especially administration
Asymmetric/hybrid threat	Mentioning hybrid warfare and the asymmetric threat emerging from new technologies
Digital economy	The description of technology within the private sector
Digital R&D	Research and development funds and resource allocation for technological advancement

3.4.3. Generating & Reviewing Themes

The third step, composed of two steps, was generating and reviewing themes. Once the initial coding was complete, the next critical step was the thematic analysis process, involving grouping related codes into themes. This stage was pivotal for synthesizing and interpreting data in a meaningful way. During this phase, all collected codes that share common underlying concepts or ideas were grouped into potential themes. This involved an iterative process of mapping out the codes, examining their interrelationships, and organizing them into thematic clusters. Each cluster represents a potential theme that encapsulates a specific aspect of digital governance and AI strategies in the Baltic states. To ensure coherence and validity, these provisional themes were continuously reviewed and refined. These themes were evaluated not only in terms of their ability to represent the coded data accurately but also for their significance to the research objectives and theoretical framework. This systematic grouping was crucial for developing a nuanced understanding of how technology and geopolitics of identity intertwine within the geopolitical concerns of Estonia, Latvia, and Lithuania. Ultimately, the goal was to distill these themes into distinct and insightful narratives that can effectively address the research question posed. Grouping the codes into themes was a useful way to analyze the research questions and objectives as the data told the main approaches and ideas of policies.

After the initial theme grouping, the themes identified were sorted to ensure their alignment with the data extracts. This stage involved iterative refinement, where themes are either merged, subdivided, or refined to better capture the underlying patterns in the data. Each theme was rigorously revised to conform to consistency and relevance across the dataset, ensuring that interpretations are robust and reflective of the data's nuances. This rigorous examination and restructuring of themes were fundamental in achieving a comprehensive understanding of the data, allowing for a deeper exploration of the research question. Table 4 displays the code groups and why they have been grouped to later be translated into themes.

Table 4

Code groupings and themes

Codes	Themes
1. International cooperation 2. Regional cooperation 3. Baltic cooperation	International/regional cooperation
1. AI for the public sector 2. AI for administration 3. AI diplomacy	Digital public sector

4. Digital Diplomacy	
1. AI for the economy 2. Digital Economy	Digital economy
1. Asymmetric threats 2. Security threats 3. Cyber Defense 4. Cyberattacks	Cybersecurity against external threat
1. Digital identity 2. Western identity,	Global digital leadership in e-government
1. Western identity 2. Societal issues	Regional digital leadership in anti-disinformation
1. Western identity 2. Digital R&D	Global digital leadership in cybersecurity

3.4.4. Defining and Naming Themes & Writing Up

The fourth step, a combination of two steps, was defining and naming themes as well as writing them up. The stage of defining and naming themes served as a phase to transform abstract ideas into tangible insights. This involved an in-depth examination of each theme to accurately describe its essence and implications within the broader context of the topic of geopolitics of digital transformation and geopolitics of identity. Effective naming was critical as it provided a succinct and precise label that encapsulated the core concept of each theme. This not only facilitated a clearer understanding and communication of the findings but also ensured that the themes were distinct and meaningful. The process was again iterative often requiring data to validate and refine the themes' definitions, ensuring they accurately reflected the collected evidence and supported the research narrative.

The final write-up phase involved the articulate presentation of the themes, ensuring each is thoroughly described, evidenced by quotes from the data, and contextualized with the existing literature. Careful attention was paid to maintaining logical flow, integrating analytical insights, and providing a critical evaluation of the themes in relation to the theoretical framework and research objectives. As a thematic analysis was straightforward and intuitive, close attention to possible bias was given, to avoid wrongful interpretation of the dataset. Table 5 displays the final themes for each country, used during the analysis.

For a better understanding of commonalities and differences that emerged during the analysis, shared themes have been marked in green color.

Table 5

Main influences on Baltic identity

Country	Themes			
Estonia	International cooperation in technology	Digital public sector	Cybersecurity against external threat	Global digital leadership in e-government
Latvia	International cooperation in technology	-	Cybersecurity against external threat	Regional digital leadership in anti-disinformation
Lithuania	International cooperation in technology	Digital economy	Cybersecurity against external threat	Global digital leadership in cybersecurity

3.5. Conclusion

In summary, the methods chapter of this thesis detailed the comprehensive approach used for data collection, organization, and analysis concerning the interplay between the geopolitics of identity and the geopolitics of digital transformation in the Baltic states. The case of the Baltics offered a unique insight into how small countries shape and evolve their digital identities, trying to politically control the geopolitics of digital transformation. Thus, to highlight these approaches the methodology followed an open-coding iterative coding scheme to unravel prevalent themes for each Baltic country providing room for unexpected findings. These themes are tools to understand the distinct foci of Estonia, Latvia, and Lithuania as well as their similarities stemming from their historic cooperation. In light of the rise of GZOs, highlighting the themes for each country offered to not only understand the Baltic approach in foreign policies but also how the Baltics control the digital transformation via different channels.

4. Analysis

4.1. Geopolitics of Digital Transformation in Baltic Foreign Policies

4.1.1. Introduction

To understand how small states adapt to the geopolitics of digital transformation by using emerging technologies, analyzing their digital self-perception and international standing helps to identify their distinct identity-building. Using the four identity types by Wendt, personal, type, role, and collective, reveal how the Baltic states use emerging technologies in foreign policies to form their (new) identities, resulting in an Estonian digital identity, a Latvian digital defense, and Lithuanian digital security.

4.1.2. Estonia's Digital Identity

Estonia's personal identity is guided by its strong national identity shaped through history and culture, resulting in an interplay between "Estonia and the other Baltic states" (Estonian Ministry of Foreign Affairs, 2020, p. 30), assuming that Estonia's identity must be (partly) understood through Baltic unity (Republic of Estonia, 2023). What makes Estonian digital identity distinct is the divide of its personal identity, into an Estonian Finno-Ugric cultural and Baltic historical approach to building the "self-organizing homeostatic structure" (Mengshu, 2020). While AI is used to safeguard the Estonian language to counteract former Russification policies and revive Estonian culture, the Baltic historical aspect is guiding Estonian economic and security aspects (Ministry of Economic Affairs and Communications, 2021). Especially the latter is visible in its digital foreign policy, strongly focusing on developing shared Baltic infrastructure to bolster electronic services and data exchange and the depiction of the Baltic states as one entity vulnerable to Russian cyber warfare, juxtaposing the Baltic bloc against the 'Other' (Estonian Foreign Intelligence Service, 2023). However, Russian and to an extent Chinese espionage and propaganda are mentioned, due to its considerable ethnic Russian community, potentially being harmful to Estonia's national identity (Estonian Foreign Intelligence Service, 2023).

The 'Other', Russia, is also highlighted in Estonia's type identity, which is firmly rooted in liberal democracy, adhering to the rule of law, a market-based economy, and corresponding values (Republic of Estonia - Ministry of Foreign Affairs, 2020). These principles paired are mirrored in its approach to integrating emerging technologies in its foreign policies, resulting in an Estonian digital identity that focuses on e-governance, characterized by a holistic approach to digitalizing all aspects of society, economy, and public services (Republic of Estonia, 2023). This is symbolically linked by integrating historic elements into its modern approach through the national AI-driven public system called 'bürokratt'. The wordplay and symbol in Figure 2 can be traced back to the Estonian "Kratt", a folkloric servant in traditional households playing on the concept of a Weberian subservient bureaucrat in Western administration (E-Estonia, 2023). Thus, emerging technologies are seen as a tool to uphold, and even extend its type but also personal identity as a (new) Western actor.

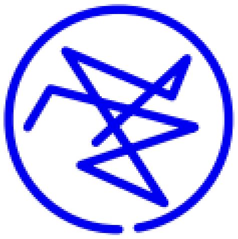


Figure 2: "In Estonian mythology, a Kratt is a magical creature. Essentially, Kratt was a servant built from hay or old household items. Therefore, the Estonian government uses this character as a metaphor for AI and its complexities". (E-Estonia, 2023, p. 1)

To further solidify this new position, Estonia's role identity is emphasized by its aspirations for global digital leadership, particularly in the realm of cybersecurity and AI. After securing strategic investment to nationally pioneer e-governance, comprising a comprehensive digital infrastructure for all government services, the digital identity is now translated into foreign policies (O'Dwyer, 2024). Its technology like bürokratt is strategically used in diplomacy, ensuring that new strategic cooperations are globally dispersed via digital diplomats, relying on Estonian expertise (Estonian Ministry of Foreign Affairs, 2020). Using a multi-level approach allows to establishment of comprehensive digital leadership, channeling Estonia's efforts to culminate in global e-governing across stakeholders, adhering to Kunkunrat's assumption of diversified international cooperation forced by digitalization.

This multi-level approach is especially visible in Estonia's collective identity, manifested through its extensive international engagement, with over 303 memberships in international organizations assuming a strong focus on security communities (Estonian Ministry of Foreign Affairs, 2020). With its significant investment in its Foreign Ministry, Tallinn aims to take leadership positions in as many organizations as possible, blending its role identity with collective identity to establish itself within the frameworks of EU, NATO, and Nordic-Baltic Cooperation (NB8) (Estonian Ministry of Foreign Affairs, 2020; Republic of Estonia, 2023). Estonia focuses on sharing its digital expertise within the communities underlining that Estonia seeks to not only be protected but also actively influence these security communities (Republic of Estonia - Information System Authority, 2022).

To sum it up, Estonia’s new e-identity is marked by an intricate Estonian-Baltic personal identity and a strong Western alignment, symbolizing a continuum from its past to its present, reinforcing its belonging to the Western community. Estonia aspires to be a leader in the geopolitics of emerging technologies by attracting international actors and implementing its e-governance expertise globally. This ambition is supported by its involvement in security communities which form the backbone of its leadership endeavors.

4.1.3. Latvia’s Digital Defense

Latvia’s personal identity is linked to its national but more so to its Baltic and also Nordic belonging, commonly highlighted in aspects of digital security (Ministry of Defense - Republic of Latvia, 2023a). Latvian foreign and defense policies frequently start with a Latvian position culminating in pan-Baltic issues, always making national standpoints a Baltic argument (Latvian Institute for International Affairs, 2023). This focus on historic Baltic (and Nordic) identity seems to divert from Latvia’s challenged cultural identity, as the societal divide between ethnic Latvians and ethnic Russians is a prevalent theme highlighted as it “advocates the cohesion of society, the belonging of the population to the country’s present and future through unified historical memory” (The National Concept on Strategic Communication and Security of the Information Space 2023–2027, 2023, p. 52). Thus, its personal identity appears less consolidated and vulnerable to altercations as this social cohesion is after more than 30 years not yet achieved.

Latvia’s quest to strengthen its personal identity is also visible in its type identity of Western democracy, emphasizing the importance of technologies in achieving and adhering to norms of human rights, environmental protection, and international rule-based order (Ministry of Defense - Republic of Latvia, 2023a). Digital transformation is seen as a means to enhance these standards via a plethora of policies, promoting not only techno-nationalism to build a digital society that is to solve its social divide but also a robust ICT-based infrastructure for its comparably lagging economy (The National Concept on Strategic Communication and Security of the Information Space 2023–2027, 2023).

However, the need for emerging technologies to safeguard its type identity reveals the country's weak ministerial cooperation, which struggles to translate these ambitious policies into effective action, thereby further eroding public trust (OECD library, n.d.). This is exemplified by Latvia's relatively underdeveloped AI strategy, which despite its focus on various issues like the dangers of deep fakes and AI misuse, lacks comprehensive execution guidelines and is not yet accessible in English (Ministry of Defense - Republic of Latvia, 2023a; Informative report " On the development of artificial intelligence solutions ", 2020).

Latvia's role identity is shaped by these administrative shortcomings and the political warfare waged by the Kremlin among its ethnic Russian population (The National Concept on Strategic Communication and Security of the Information Space 2023–2027, 2023; OECD library, n.d.). However, instead of capitulating Latvia leverages this victim status to establish itself as an expert in anti-disinformation and propaganda campaigns, by aiming at educating national and regional society, enhancing efficiency within public and private sectors to gain trust and operationalize its objectives through emerging technologies (Ministry of Defense - Republic of Latvia, 2019).

Due to its perceived vulnerabilities, Latvia's collective identity is strongly emphasized by its memberships in NATO, EU, and NB8, serving as the cornerstone of its national security (Latvian Foreign and Security Policy, 2021). As collective identity is always an intricate interplay between type and role identity, it is not surprising that, unlike Estonia, Latvia does not seek multiple leadership positions but focuses on introducing digital communication and protecting civil society from digital political warfare as core policy areas (The National Concept on Strategic Communication and Security of the Information Space 2023–2027, 2023). Its commitment to cybersecurity strongly aligns with NATO and EU, visible in the unquestioned adherence to its security communities guidelines like the NIS2 Directive, reflecting its dependence on its communities to establish effective frameworks (Ministry of Defense - Republic of Latvia, 2023a).

To sum it up, Latvia's digital identity encapsulates its national dilemma: viewing modern technology as both a threat and a defensive tool to a small country. Despite its victim status, Latvia proactively uses its weaknesses to build a more resilient digital society, capable of withstanding the hybrid threats to its national identity. Nonetheless, Latvia's shortcomings necessitate strong affiliations with international organizations to transform its challenges into strengths effectively.

4.1.4. Lithuania's Digital Security

Lithuania's personal identity can be traced back to its circle network depiction in its AI strategy, ranking the importance from Lithuania to global Lithuania over to the Baltic Region, the Nordic-Baltic region, and culminating in the EU and other global institutions (Ministry of Economy- Lithuania, 2019). While Lithuania strongly focuses on its regional hubs, highlighting its rich cultural infrastructure for developing a digital identity, it ranks its diaspora second, relying on the national identity of ex-pats to contribute to Lithuania's success in the geopolitics of emerging technologies (Ministry of Economy- Lithuania, 2019). Its historic connection to the Baltic region is said to be a basis for global interaction and value dispersion, resulting in a personal identity that with its intricate mix of national-cultural and historic-Baltic, can be compared to Estonia.

This mix is visible in Lithuania's emphasis on integrating itself into the Western community, emphasizing its democratic values but foremost a market-based approach, as it is the fastest-growing economy in the Baltics (World Bank, n.d.). As articulated by the Ministry of Foreign Affairs of Lithuania (2022), the country, although comparably small, sees itself playing a similar role to other nations when it comes to defending democracy, highlighted by its commitment to a strong advocacy role it metaphorically describes as "not a sprint but a marathon [for] persistence and resilience" (Minister of Foreign Affairs of Lithuania, 2022, p. 23), resulting in an assumed leadership position striving for its former imperial influence in the European community.

This interlinking of emerging technologies and national identity highlights Lithuania's role identity as a leader in AI and cybersecurity, reflected in its comprehensive AI strategy that encompasses all aspects of national infrastructure (Ministry of Economy- Lithuania, 2019). Unlike Estonia, Lithuania places a greater emphasis on the private sector, recognizing its dynamic start-up culture and robust IT infrastructure as catalysts for economic growth and innovation to keep up with its northern partner (Ministry of Economy- Lithuania, 2019). Lithuania's political and economic stance, particularly its recognition of Taiwan and the subsequent tensions with China has directed its IT export markets towards other Southeast Asian countries, thereby increasing revenue and expanding its global influence (Defense Intelligence and Security Service under the Ministry of National Defence, 2022). Thus, Lithuania uses its emerging technologies leadership to grow economically, even daring to challenge big players like China and Russia.

Its daring nature, despite its size, is also visible in its collective identity, reinforced by its active participation in various international organizations, establishing strong security communities. Geopolitically situated between Russia (Kaliningrad) and Belarus, Lithuania plays a critical role in Baltic defense, however, in contrast to its Baltic neighbors, Lithuania frequently emphasizes the importance of Euro-Atlantic security over trans-Atlantic ties, indicating a stronger security focus on Europe than NATO (National Security Strategy, 2021). Lithuania's commitment to strengthening its European security community is evident in its effort to enhance the cybersecurity of critical infrastructure particularly in the energy sector, being a result of its strategic location for Russo-European energy transactions (National Threat Assessment, 2021). This strategic focus highlights the interconnectedness of cybersecurity, economic prosperity, and resilience, underscoring Lithuania's holistic approach to European security (National Security Strategy, 2021).

To sum it up, Lithuania's identity is guided by its strong self-perception as a democratic leader in the European community, asserting dominance in the economic sector and even challenging big international players. Its emphasis on interlinking emerging technologies with its quest for European security underlines its role in its security communities where it sees itself as an important actor.

4.1.5. Conclusion

To summarize, Estonia, Latvia, and Lithuania each interpret their personal, type, role, and collective identity differently, manifesting the assumption that they are self-aware actors who are keen on forming their new archetypes, juxtaposing Russia and its post-Soviet past. Especially emerging technologies play a crucial part, leading to the assumption that the Baltics have each formed a digital identity now being part of their distinct archetypes. Their individual approaches are, however, also based on a personal identity that includes pan-Baltic unity, making them unique, as Wendt argued for personal identities to be self-reflective and not mutual. As the collective identity is an interplay of type and role identity, each state finds its own niche within the security communities, inspiring leadership positions through a unified, yet diverse, approach.

4.2. Security Communities: The Answer to the Geopolitics of Emerging Technologies

4.2.1. Introduction

To effectively address gray zone operations coming mainly from Russia, Estonia, Latvia, and Lithuania opt to integrate themselves into numerous security communities, offering them a new collective identity, mutual trust, and positive interactions. Although all of them offer these benefits, each community is exemplary highlighted in relation to one community being either the EU, NATO, or the Nordic-Baltic 8, to highlight their strongest attributes found within Baltic foreign policy. By actively aligning their security and defense with their international partners, the Baltics do not shy away from using symbolism and speech acts, that indicate their involvement in digital warfare, despite their limited physical capabilities.

4.2.2. Security Communities

4.2.2.1. The NB8 - Positive Interaction

Going from the smallest to the biggest security community, NB8 manifests the Baltic geographical realignment away from the archaic notion of a pan-Slavic community and reinforcing a distinctly Baltic self-perception closely tied to Nordic culture. For the Baltic countries, this realignment with their Nordic partners signifies not only a symbolic return to their historical roots - such as when Estonia and Latvia were part of the Swedish Empire - but also a departure from being associated with the Eastern bloc (Estonian Ministry of Foreign Affairs, 2020). Established in the 1990s when the Nordic Council of Ministers initiated the Baltic project to support the transition back to market-based democracies, NB8 provided positive interaction through initiative and trust as it swiftly tried to incorporate its neighbors into their security community (Nordic Co-operation, 2018b).

Since then, the NB8 has been pivotal in fostering political dialogue in the region and facilitating discussion in regional security, defense cooperation, and foreign policy alignments (Ministry of Foreign Affairs Republic of Latvia, 2024). NB8 embodies regional cooperation primarily focusing on economic aspects but also regional digitalization and utilizing emerging technologies for economic purposes. Especially for Latvia, which highlights its Nordic personal identity, received this quick integration into the Nordic region well, making NB8 a crucial partner in its foreign policy aspect of societal cohesion (Minister of Foreign Affairs of Lithuania, 2024; Ministry of Foreign Affairs Republic of Latvia, 2024).

As most Nordic countries share the Baltic fate of Eastern aggression and gray zone operations against their countries, the NB8's response has been in line with the evolving geopolitics of digital transformation, resulting in the introduction of an AI Declaration in 2018 (Nordic Co-operation, 2018a). As the release date was significantly earlier than the EU or NATO reacting to the changed digital sphere, the positive interaction NB8 provides stems from a shared threat, that is geographically and geopolitically closer to this security community compared to the EU or NATO. Their cooperation ultimately culminated in various ethical guidelines, and data-sharing agreements across borders most important to Estonia, and its voiced need to feed its e-governance system to grow (Ministry of Economic Affairs and Communications, 2021). Lithuania is highlighting the benefits of minimizing unnecessary regulations on the market, able to quickly introduce its AI approach such as 'AI badges' for national companies that pioneer abroad (Ministry of Economy- Lithuania, n.d.). The smaller NB8 allows for more leverage than communities like the EU or NATO and is additionally filled with more prosperous and societally liberal Nordic countries, making ideal partners for sharing the benefits of new technologies, as their higher data availability and lower reluctance to adopt tools like AI create transformative market opportunities (Nordic Co-operation, 2018a).

4.2.2.2.The EU – Mutual Trust

The second-biggest security community is the EU, which with its normative framework provides the Baltic states with a new Western collective identity, derived from endogenous factors of identity-building under a pluralist security community safeguarding their sovereignty (Finnemore & Sikkink, 1998). As the Baltics are located at the EU's external borders in proximity to antagonistic states, they regularly highlight their strategic yet vulnerable position (State Border Guard- republic of Latvia, 2019). By constantly reminding its community of the increased hybrid threats such as migrant smuggling at the Russian and Belarusian borders, they make their issues that of the community, ergo making their border issues a societal problem for the entire European community (Republic of Estonia, 2023). As they are constantly advocating for their fate, the Baltics received what can be called a symbol of mutual trust - a FRONTEX Liaison Officer to the

Baltic States appointed in 2017. As the community acknowledged the Baltic's security issues as a collective threat, it ordered the Liaison officer to take preventative measures, including competencies in the use of emerging technologies in border security (EU Cyber Direct, 2019). The Latvian State Border Guard has emphasized the increased use of AI-powered drones and unmanned aerial vehicles (UAVs) at its Eastern borders since the Officer's role was established, correlating with Latvia's AI strategy and participation in the PESCO Integrated Unmanned Ground Systems (UGS), translating the project into active defense in digital hybrid warfare (State Border Guard- republic of Latvia, 2019).

Additionally, this mutual trust is met by answering Baltic calls to adopt policies such as the Cybersecurity Act (2019) or the NIS2 Directive (2024), for which Estonia especially advocated as it saw the need to safeguard digital infrastructure after the 2007 attack. (Estonian Ministry of Foreign Affairs, 2020). Lithuania's focus on European security is translated in the EU's security community as it sees these policies as a response to strengthening "the EU common security and defense policy as well as European security and defense policy" (Seimas of the Republic of Lithuania, 2016, p.1). Despite the EU's limited competencies when it comes to the CSDP, digital security bypasses physical borders, circumventing these limitations by adopting digital security measures and thus still safeguarding Baltic sovereignty and interest.

4.2.2.3.NATO – Collective Identity

NATO's security community is one that is formed out of the exogenous factor of threat, once being a defense union established against the Warsaw Pact (NATO, 2023). Today, as the threat has increased, but the external community has changed and mostly reduced to Russia and Belarus, the defense pact becomes once again important, especially for the Baltic states that once belonged to the other side.

The collective identity results from Article 5 of NATO, that if "a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take action that it deems necessary to assist the Ally attacked (NATO, 2008). In its Cybersecurity Strategy 2023-36, Latvia argues that digital warfare falls under this provision, assuming that the current digital warfare invokes the article and triggers its allies' action (Ministry of Defense - Republic of Latvia, 2023a). Lithuania exemplified how the three existing core tasks of collective defense, crisis management, and cooperative security are updated to four via building resilience to comprehensive threats i.e. gray zone operations, being a response to Article 5 already (Latvian Foreign and Security Policy, 2021; Ministry of National Defence - Republic of Lithuania, 2022a). As the collectivity is highlighted, and the communities' security and defense policy is described as the backbone of their own foreign and defense policies, the Baltics actively align their goals with those of NATO (National Threat Assessment, 2021).

Given their strategic yet vulnerable position, the Baltics see themselves as a crucial link to international and regional peace and security, which they underline with unwavering commitment by always adhering to the community guideline of allocating 2% of GDP to military spending (Ministry of Defense - Republic of Latvia, 2023b; NATO, 2024). Although other, wealthier states like Germany failed to even do so after the start of the Russo-Ukrainian war, the Baltic states saw their allies strengthening the political stance on cyberattacks and their consequences, exemplified in heightened visibility and new command elements to react accordingly (Ministry of Defense - Republic of Latvia, 2023a, 2023b; Ministry of National Defence - Republic of Lithuania, 2019; NATO, 2024).

4.2.2.4.Conclusion

The Baltics' use of security communities to establish their comprehensive security framework against gray zone operations including digital warfare, allows them to be fitted with the benefits of mutual trust, positive interaction, and a new collective identity. These differ significantly from their former Union, involuntarily being caught up in conflict it did not support. These new communities offer these small states the security and defense provisions they need, as their own physical capabilities are limited. While NB8 offers a more normative and economic basis for digital cooperation, the EU provides a new security framework and NATO collective defense in times of war.

4.2.3. Symbolism as Common Speech Acts

As the security communities of NB8, EU, and NATO provide Estonia, Latvia, and Lithuania with a comprehensive security framework, they underline their newly gained confidence with symbolism, allowing them to not only voice their opinions but also do so in the security of their communities. As Savu (2021) outlines the importance of shared language and symbols for socializing within communities and materializing threats, the Baltic states, are participating as well by attacking national symbols and establishing a common perception of international events exacerbated by an emotionalized post-truth environment.

Estonia particularly stands out as it uses objectively “aggressive” language against the Kremlin, regularly leading the diplomatic jargon astray. Exemplary seen in Figure 6, it is mocking Russia’s intelligence services for being inadequately equipped to “see the invisible, and hear the inaudible” (Estonian Foreign Intelligence Service, 2022, p. 27). In Figure 8, Russian cyberattacks are depicted using traditional Russian matryoshkas, metaphorically dissecting the nice-looking doll into a materialized death, attacking and destroying national symbols (Ciolan, 2014; Estonian Foreign Intelligence Service, 2022, p. 38). As foreign policies are directed to the global audience, Estonia’s use of language and imagery can be seen as a political attack against Moscow, also engaging in the political warfare it so desperately tries to defend itself from.

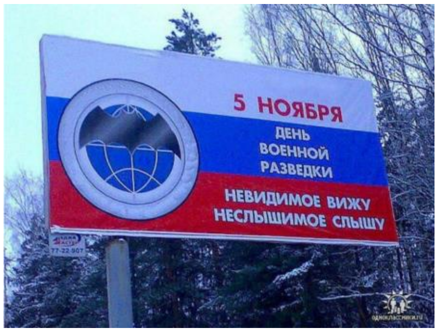


Figure 3: A Russian poster celebrating the 5th of November as National Military Intelligence Service Day. The exclamation in red says: "I see the invisible, I hear the inaudible." (International Security and Estonia, 2022)

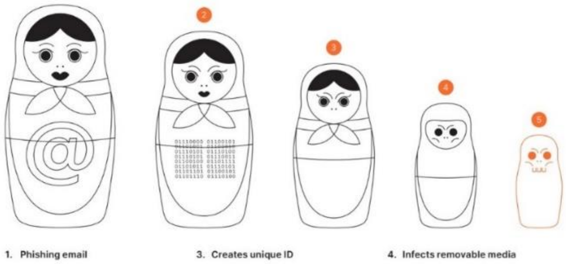


Figure 4: Russian cyber threat depicted by Estonia (International Security and Estonia, 2022)

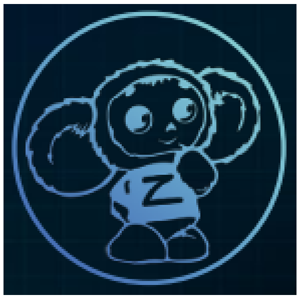


Figure 5: The mystic figure of "Cheburashka" from a popular Soviet children's movie. Here depicted with the “Z” (Republic of Latvia - Constitution Protection Bureau, 2023, p. 31).

Latvia’s approach is more subtle focusing on its digital communication in support of Ukraine or by shaping the ‘other’ in relation to its Soviet past. As Ukraine was and is targeted by cyber warfare, Latvia is constantly highlighting how it warned its allies of Russia while also already being a victim of similar aggressions like DDoS attacks (Latvian Institute for International Affairs, 2023). This beginning is depicted by the Soviet-era character Cheburashka, depicted with the war sign “Z” in its chest (Figure 8), illustrating the subtle infiltration of Russian propaganda, especially into Latvian homes, making it a modern version of a wolf in sheep’s clothing (Republic of Latvia - Constitution Protection Bureau, 2023). By additionally using hot war symbolism of fire (Figure 7), it materializes this

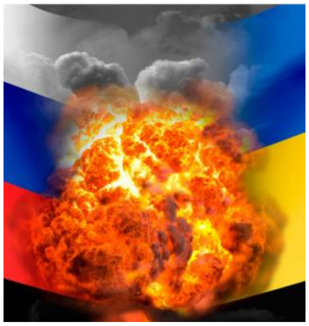


Figure 6: Picture of the 2022 full-scale invasion in the (Republic of Latvia - Constitution Protection Bureau, 2022, p. 15)

cyber threat, as the Russo-Ukrainian physical war stated long after digital political warfare, dispersing the idea it could be next and thus forcing its allies to act. Latvia's unwavering support for Ukraine throughout its foreign policies and national threat assessments, painting all colors in blue and yellow, symbolically intertwines their post-Soviet fate in solidarity. Thus, Latvia tries to assert dominance in a field it is most vulnerable in, marketing itself as an expert and thus in a position to be at least a regional leader.

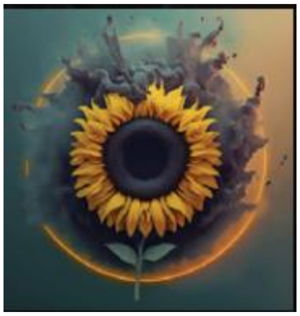


Figure 7: AI-generated cover featuring an image that portrays a joint interpretation of Lithuanian intelligence and Ukraines national symbol (State Security Department of The Republic of Lithuania, 2023)

Lastly, Lithuania's quest to become a leader in AI, while simultaneously juxtaposing Russia in the war is visible in interlinking with Ukrainian fate by providing specialized digital training for defense against Moscow's hybrid warfare, to bring the country closer to the democratic community (Ministry of National Defence - Republic of Lithuania, 2022b). This interlinking is interestingly done via AI-generated imagery on the 2022 National Threat Assessment cover sheet (Figure 9), featuring symbols of Lithuanian AI intelligence with the Ukrainian national symbol of the sunflower (State Security Department of The Republic of Lithuania, 2023). In contrast to Estonia and Latvia, it is neither aggressive nor frantic in its imagery but paints a picture of a calm and knowledgeable actor that although guided by emotions and historical appeal wants to be perceived as a rational to secure its communities' trust.

In summary, the Baltics use symbolism in their foreign policies out of the security of its communities providing them but also to underline their perception of shared events seen differently by their Eastern counterparts. However, as they sometimes even aggressively target national symbols, it can be argued that the Baltic states are participating in digital political warfare, using similar methods of information dispersion and tools of post-truth such as emotionality to persuade their allies.

3.3.5. Conclusion

To sum it up, the Baltic states approach their security in times of digital warfare by integrating themselves within security communities, establishing leadership and expertise in and through the geopolitics of emerging technologies, not only relying on their security communities but actively shaping them through collaboration. Although the communities offer positive interaction, collective identity, and mutual trust, these are achieved as Estonia, Latvia, and Lithuania work together, being a source of power and leverage needed to assert dominance in the shifting realm of security. As small states were traditionally disadvantaged, lacking physical capabilities, gray zone operations have challenged but also allowed the Baltics to actively shape their own security seen in how they use symbolism and speech to juxtapose themselves to Russia and use the backbone of their communities to engage in digital political warfare themselves.

4.3. The new Baltic Way: Political Control of the Geopolitics of Emerging Technologies

4.3.1. Introduction

The first chapter revealed how Estonia, Latvia, and Lithuania each have distinct digital identities, which however they partly link to their Baltic unity, while the second highlighted the Baltic security framework to counteract digital warfare. However, as the symbolism and thus participation in digital political warfare presupposes, the Baltic states are more active than passive actors, not correlating with the idea of vulnerable small states. To understand how they do so, their forms of politically controlling their security communities in the digital sphere become interesting. Thus, this chapter assumes a new power emerging from the Baltic states, which is an intricate interplay of mastering the geopolitics of emerging technologies collectively as small states by translating them into leverage over their security communities to establish a “new Baltic Way”, named after their collective protest against the USSR in 1998, that subsequently lead to its dissolution.

4.3.2. Institutional Norm Setting

Traditional warfare partly shifted to the digital sphere, and new emerging technologies have translated Baltic fears of their neighbors into a real-life threat, forcing them to take on new measures. As power becomes ideational, soft power and norm-setting to shape institutions become more important, leading to possibilities for small states to leverage power (Eriksson & Giacomello, 2007). As the identity analysis revealed how each Baltic state carved its niche in which it operates as an international or regional leader, but overarchingly works together, their institutionalization process is focused on its security communities, resulting in strong leverage in the sphere of the geopolitics of digital transformation.

4.3.2.1.Estonia

Estonia’s approach is guided by its international e-governance focus, highlighting that it specifically encourages “target countries to apply information and communication technologies and e-government solutions more extensively in various fields*”* (Estonian Ministry of Foreign Affairs, 2020, p. 12). Its approach to becoming a global norm creator in cybersecurity is underlined as it institutionalizes its standards through various channels, inter alia, hosting the 2008 established Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, immediately following the 2007 supposedly Russia-funded cyberattack that rang the new digital warfare. Estonia’s swift response to this change of warfare is thanks to its pioneer position in e-governance, allowing it to make digital warfare a staple in the common defense policies of its 32 allies (CCDCEO, 2017).

Its global approach also encompasses other states not belonging to its security communities, e.g., in Africa, Southeast Asia, and the Caucasus, where it introduces an e-governance system to streamline processes in areas like development aid (Republic of Estonia - Ministry of Foreign Affairs, 2020). It thus sets standards according to its Western values to ensure global digital dominance in norm creation, directly juxtaposing other actors who seek to influence emerging developing countries. By focusing on its allies' efficiency and policy coherence in using emerging technologies, Estonia ensures that they not only advance these systems but also adhere to Estonian ideals of digital ethical guidelines that are codified into law as fourth-generation human rights including, inter alia, Internet connection for every inhabitant (Freedom House, 2023).

4.3.2.2.Latvia

Latvia’s leadership ambitions are more limited, partly due to its governance shortcomings and weak economic performance (OECD library, n.d.). Its leadership focus is tailored to its specific needs to establish a common Latvian resilient society, which it sees as one of the main defense objects to protect against Russian digital political warfare (Ministry of Defense - Republic of Latvia, 2023b). Thus, stemming from its victim position, Riga hosts the Strategic Communications Center of Excellence (StratCom COE), which focuses on countering disinformation and propaganda, established in response to the Russo-Ukrainian conflict in 2014. Leveraging this victim position, Latvia has become indispensable for NATO as it provides crucial research and analysis on emerging communication technologies, such as AI-enabled DDoS attacks, and digital propaganda education (NATO Strategic Communications Center of Excellence, 2024). One aspect is to constantly highlight its internal problems, framing internal issues related to disinformation strategic communication on its Russian population as a pan-European threat that could influence political processes via, hostile actors (Ministry of Defense - Republic of Latvia, 2023b).

In the NB8, although the Nordics aimed at moving the Baltics closer to the Nordics, influencing them in crucial norms and values, it was mostly Latvia that changed the face of the NB8, swiftly integrating emerging technologies into the community, marking its influence, and digitalizing the region. During its first chair position in 2010, Latvia immediately drafted the Wise Men Report soon becoming a cornerstone of NB8 collaboration, inter alia, introducing cyber security into the communities' civil security framework (NB8, 2010). By aligning NB8 with its regional and civil ambitions, Latvia influences international policymaking by setting new standards based on its threat perception, particularly concerning Moscow's digital political warfare on societies stemming from its own aforementioned malheur. Subsequently, Estonia and Lithuania have since each reinforced Latvia's initiatives during their coordinator tenures by e.g., emphasizing the importance of cybersecurity and the impact of emerging technologies on regional security, thus, underlining the pan-Baltic mutual support in security communities (Republic of Estonia - Ministry of Foreign Affairs, 2024).

4.3.2.3.Lithuania

Lithuania's approach is once again guided by its economic ambitions, which emerging technologies like AI and cybersecurity are to safeguard. Thus, Vilnius hosts the Energy Centre of Excellence (ENSEC COE), reflecting Lithuania's strategic position in Europe's critical energy infrastructure and its long-standing effort to diversify from Russia's energy sector (Ministry of National Defence - Republic of Lithuania, 2023). It frequently underlines the importance of hosting events on the future resilience of transitioning in the energy sector highlighting the importance of mitigating the risks associated with asymmetric warfare as Europe's critical infrastructure is strongly tied to its economic identity and survival (NATO, n.d.). Its norm dispersion relies on its perceived exceptionality for cybersecurity especially in the energy sector, highlighted by being "ranked 4th globally and 2nd in the EU, scoring highest ratings in legal, technical, organizational and cooperation domains" (Ministry of Economy- Lithuania, n.d.) resulting in generated trust and ability coming from its allies (Ministry of Economy- Lithuania, n.d. p.1).

This trust through exceptionality is also manifested through common European security and defense measures. Although traditional security and defense are limited within the EU, the paradigmatic shift to digital warfare offers new possibilities, including voluntary projects in the Common Security and Defense Policy notably under the PESCO framework. Given the aforementioned eagerness to establish digital leadership, it is not surprising that the Baltic states actively participate in cyber-related projects within this framework, although Lithuania, in particular, stands out for its coordination of the Cyber Rapid Response Team and Mutual Assistance in Cyber Security (CRRT). As it hosts, inter alia, the largest cybersecurity exercise, Cyber Shield it takes on this leading role in the security community inserting not only its own priorities of European digital defense but also training its allies to shape a collective identity based on a common threat (EU Cyber Direct, 2019). Hence, Vilnius actively influences the EU's perception of the 'other' within the EU's security community for its own benefits, also manifesting in its pride as it states the CRRT to be "among the most successfully developed and most advanced PESCO projects" (Ministry of National Defence - Republic of Lithuania, 2023, p. 63), correlating with Lithuania's focus on European collective identity,

In conclusion, Estonia, Latvia, and Lithuania each use forms of political control that are mainly guided by their role identity, establishing leadership through e.g., NATO Centers of Excellence that align with their expertise and foreign policy aims. Within their security communities, the Baltics are not only protected, but they are also actively shaping their institutions to their needs and objectives, underlining the options the digital transformation offers small states.

4.3.3. Norm Agents: Digital Diplomats

The constructivist core is the premise that international relations are a branch of human relations, "considering that the processes of identities and interest formations happen at the same time with the process of interaction" (Ciolan, 2014, p. 3). To uphold their leadership positions within their security communities, new agents must leverage power, underlining the constructivist assumption that the decline of physical warfare has increased the importance of soft power, shaping new norms and standards to effectively address cyber warfare as a social threat. For small states gaining leverage and influencing the institutional norm-setting can be more difficult, as despite their leadership positions, material facts like size and limited number of human resources due to demographic change and emigration do matter. Thus, to circumvent their shortage of human resources, the Baltics are using digital transformation to establish forms of digital diplomacy, consolidating their approach to politically control emerging technologies via norm agents abroad.

Estonia's approach is set out in its Foreign Policy Strategy through 2030, in which it establishes a system of citizens, diplomats, and foreigners to extend Estonia's digital proficiency in the global arena. Its diplomats are actively trained to use bürokratt and other ICT to participate in international fora to "shape the global regulatory environment" (Estonian Ministry of Foreign Affairs, 2020). Additionally, its citizens can become e.g., economic diplomats or digital diplomats used in over 30 main export markets also already swiftly penetrating new markets as they emerge (Estonian Ministry of Foreign Affairs, 2020). Most interestingly it also uses ex-pats and non-Estonians, for its e-residency encompassing a wide range of people approaching e-identity as a global endeavor, consolidated in the first e-Embassy in the world "ensuring [its] presence in every location across the globe" (Estonian Ministry of Foreign Affairs, 2020, p. 17). Thus, its digital identity becomes a trademark that can be acquired and dispersed.

Latvia is also using digital diplomats for the first time since 2021, actively promoting them as an opportunity to mitigate challenges (Latvian Foreign and Security Policy, 2021). In contrast to Estonia's comprehensive approach, however, Latvia is once again guided by its victim status, underlining the constructivist notion of the 'looking-glass self', as its e-diplomacy can be seen as a response to Russian soft power and propaganda influence (Latvian Foreign and Security Policy, 2021). As it does not outline the specifics of how and where these diplomats are used and who besides citizens could become one, the e-diplomacy approach is more limited.

Lithuania’s approach, especially in emerging technologies is guided by its stellar economic rise during the last years, also stemming from a younger and bigger population than its neighbors (World Bank, n.d.). As it always lags some years behind, its e-diplomacy approach is more focused on economic prosperity with ‘Global Lithuania’ being the second innermost network to its foreign and AI strategy. (Ministry of Economy- Lithuania, 2019). More than Estonia, it highlights the relatively unique diaspora that it considers to be special due to Lithuania’s size, history, and activism using it to create a registry of AI and digital experts that will represent Lithuania in dispersing their norms through social media success stories or as advocates in AI-related committees and offices abroad (Ministry of Economy- Lithuania, 2019). By trusting in its own community worldwide used as norm agents, Lithuania understands its norm dispersion as a ‘Lithuanian matter’, serving its role in the European critical infrastructure and economic success.

To conclude, the Baltic states each use digital diplomacy as a means of circumventing their limited size and resources that could possibly hinder them by not having enough norm agents to set new norms and standards globally. While Estonia has the most comprehensive approach, building upon its advanced e-residency system and inviting foreigners to be part of their e-identity, Lithuania is more reluctant, focusing on its own diaspora and economic benefits, as it still suffers least from demographic change. Latvia, caught in its victimhood, is withdrawing from too much e-diplomatic intervention, merely using digital diplomats as a response to Russia, but focusing on its internal problem, manifesting its role identity as a regional player.

4.3.4. Conclusion

To conclude, the Baltic states use the new Baltic Way as a form of political control in the emerging geopolitics of digital transformation but focus on taking on various leadership, by always having each other’s support. It is through their collaboration in security communities that the new Baltic Way can flourish as it is marked by not needing to liberate themselves but gaining never-known leverage shaping these communities and managing the fast-evolving threats of gray zone operations coming from roles correlating with their role identities. With every state carving its own niche, they are able to insert its norms and standards of e-governance, cybersecurity, and societal cohesion into these communities, using new digital diplomacy, as a digital answer to their problem of lacking human resources as small states. By using digital diplomacy that encompasses various norm agents from government officials to foreigners, the digital transformation allows these small countries to leverage their standards and translate them into global action.

5. Conclusion

5.1. The Variety of Geopolitics of Digital Transformation Explained

This thesis sought to explore the variety in the geopolitics of emerging technologies within Baltic foreign policy and find answers as to why this variety exists in the first place. The question was aimed to explore how small, in this case, also young, states use the traction of a changing digital world to not only build their new digital identities but also how these are translated into power and leverage, never known to small states before. Through a detailed analysis, it became evident that the geopolitical strategies of Estonia, Latvia, and Lithuania are deeply influenced by their unique national identities, historical experiences, and current security concerns.

First, digital transformation is highly visible in the foreign policies of the Baltic states, each showcasing distinct national strategies. As their personal, type, role, and collective identity are inherently and increasingly digital, their overall approach is one that relies on shared identity formation visible in a personal identity guided by national beliefs and Baltic historic unity. Instead of renouncing this regional cooperation after their independence from the USSR, their distinct identities are always framed and guided by their pan-Baltic collaboration.

Second, the differences and similarities in their approaches are rooted in their historical contexts and strategic priorities. While all three states leverage their integration into Western security communities such as NB8, NATO, and the EU, they each find their niches within this framework to secure their sovereignty within digital warfare. As each community offers them mutual trust, collective identity, and positive interaction Estonia, Latvia, and Lithuania as small states are protected. This secure feeling, however, leads them to also actively engage in digital political warfare, using symbolism as speech acts to attack Russia, show solidarity with Ukraine, or highlight their abilities to be helpful actors. Thus, their common speech acts frame international events on emotional appeal, feeding into the post-truth era.

Third, the political control of emerging technologies in the Baltic states is explained through a constructivist lens, where identity and geopolitical context play crucial roles. Estonia uses its digital identity and e-diplomacy to shape global norms and standards. Latvia’s political control is evident in strategic communication efforts and management of information threats within the security communities, Lithuania’s approach is made by embedding security norms within both domestic and international frameworks, fostering a collaborative ecosystem that ensures technological advancement contributing to national security and subsequent economic prosperity.

The new Baltic Way is thus a multifaceted and collaborative yet individualized strategy in navigating the geopolitics of digital transformation – answering how the variety of approaches can be explained. The new Baltic Way underscores the Baltic's ability to leverage digital transformation to reinforce their national identities and security, offering viable insights into the interplay between technology, identity, and international relations. They are thus indeed acting as the ‘Three Sisters’ they are described as, going their own ways but always having each other’s back. The importance of these insights lies in their broader implications for understanding the role of emerging technologies in geopolitics. They suggest that small states can leverage the digital transformation not only to enhance their security but also to assert their identity and sovereignty in the international arena. This is particularly relevant in the contexts of increasing cyber threats and geopolitical instability, where technology becomes both a tool for empowerment and potential vulnerability.

5.2. Situating the Findings

The various findings integrate themselves into the state of the art, filling the gap of small-state approaches to the geopolitics of digital transformation yet lacking in the academic discourse. As this discourse is still limited to big players like the USA, Russia, and China it is ignoring the potential of digitalization to mitigate risks and circumvent traditional shortcomings of small state security frameworks. Patil and Mishra highlight how the “geopolitics of the next few decades is likely to be shaped by technological competition between two axes of power – China on the one hand and a US-led coalition on the other” (Patil & Mishra, 2022). This thesis, however, shows that this statement is probably not the case, at least not in its dramaturgy of axes. As small states can circumvent traditional forms of power, although still limited by economic factors, they can leverage their normative power by indeed using the digital technologies they might not yet have. It might be that the big players will accelerate the pace, but at least in pluralist communities in which the US is allied with the Baltic states, small states have significant power in navigating these waters by streamlining procedures and influencing standards.

Popescu (2021) showcased how Romania, also a (comparably small) post-communist country even with influences on the African continent has lost its level of technological power and reduced its foreign policy, leaving “the capital of influence” (Popescu, 2021) behind. She underlines how the lack of a digital strategy and the subsequent establishment of a digital identity harmed her country, not only leaving its former innovation bonus but also failing at solving societal issues by using emerging technologies. Thus, she indirectly underlines this thesis’ argument that investing and creating influence in a techno-nationalism enables small states to establish leverage and power but also to defend themselves against cyberwarfare, to which Romania is highly vulnerable as it did not yet recalibrate its R&D to the challenges of e.g., Artificial intelligence (Popescu, 2021).

Lagging in R&D also has a significant impact on being able to defend oneself, which Khan coined the causality between global geopolitical risk (GPR) and technology (TEC), using a rolling window approach (2022). As he highlights that GPR increases with TEC, due to increased competition between countries, he showcases how important the acknowledgment of new technologies in security repertoire really is. However, he fails to include strategic partnerships, in which such competition is less important and could even be circumvented by aid through mutual trust and knowledge exchange. This provision is, given by Patil and Mishra (2022) acknowledging how although this intersection increases the fragmentation of the world order via digital transformation, it is counteracted with international cooperation via e.g. democratic states working together (Patil & Mishra, 2022). The fragmentation of the world order is also less dramatic as Patil and Mishra depict, as Tilovksa-Kachedjis’s (2023) ‘strategic outpacing’ between actors results in a geopolitical.

Additionally, providing security communities provides allies with enough leverage to also decrease their risk by becoming ‘untouchable’ in at least the physical sense. Mazar’s (2015) grey zone operation includes such hybrid warfare and how the untouchables are being touched but ignores how the change of digital transformation also affects small-state behavior, seen as the Baltic states, especially Estonia, become more inclined to participate in digital political warfare.

What this situating of the finings highlights most, is how the academic community ignored to apply the highlighted benefits of the digital revolution to actors, that could benefit most from them. While the geopolitical framework changes with emerging technologies, so do the states within, asking for more research on less prominent countries and how these interact with the fourth revolution. As this thesis highlighted an individualized approach to digital transformation, this translates into a need to look further into other small states across the globe, analyzing what their individual approach is and how it benefits defense and security.

5.3. Practical Insights

From a practical perspective, this thesis offers key insights to policymakers and scholars interested in the intersection of technology, identity, and foreign policy. First, it emphasized the need for tailored strategies that align with national identity and security concerns. Policymakers in the Baltic states and similar regions, e.g., Nordics or Southeast Asia, should prioritize the development of digital infrastructures and cybersecurity measures that reflect their unique geopolitical challenges and historic experiences. The importance of integrating digital strategies with broader national identity narratives, aids at not only protecting the states' digital sovereignty but also using technology to reinforce their cultural and historical identities on the global stage. Shared identities and adversaries can be seen as breeding grounds for technological advancement, national security, and increased power on the international stage.

Second, to achieve this digital identity, this thesis emphasized the importance of investing in digital literacy and public education, crucial for fostering technologically savvy citizens capable of navigating the complexities of the digital age. In a world where “glocal” is a response to an increasingly fractured globalization, collaborative initiatives within frameworks like the EU or NATO, but also ASEAN, MERCOSUR, or ECOWAS, can provide essential support for small states facing asymmetric threats. Thus, this thesis highlights the importance of regional cooperation in building resilient digital ecosystems. Collectivity is a keyword, as its multi-level use disperses from citizenry to regional cooperation over to international security frameworks, important to enhance collective security against cyber threats. This approach will enable small states to assert their sovereignty, enhance their security, and play a more influential role in international relations.

Lastly, this thesis suggests that ongoing digital transformation should be viewed not only as a technological challenge but also as an opportunity for small states to redefine their roles in the global arena, leveraging technology to enhance their diplomatic and strategic influence. Traditionally disadvantaged by lacking substantial physical capabilities, emerging technologies offer to circumvent their physical need for security, enhancing existing digital capabilities for comprehensive security frameworks. As this thesis provides a comprehensive framework for understanding the geopolitics of digital transformation, it offers both theoretical and practical guidance to embrace the transformation strategically and identity-consciously to face the challenges of the 21st century.

6. References

Antoniuk, D. (2022, October 28). Latvia’s cyberspace faces new challenges amid war in Ukraine. The Record: The Record. Retrieved from https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine

The Baltic Times (2023a, May 1). Are Baltic Countries a Tech Hotspot? *The Baltic Times*. Retrieved from https://www.baltictimes.com/are_baltic_countries_a_tech_hotspot_/

The Baltic Times (2023b, May 1). Are Baltic Countries a Tech Hotspot? *The Baltic Times*. Retrieved from https://www.baltictimes.com/are_baltic_countries_a_tech_hotspot_/

Berg, E. (2007). Where East Meets the West? Baltic States in Search of New Identity. Retrieved from https://src-h.slav.hokudai.ac.jp/coe21/publish/no15_ses/03_berg.pdf

Boyle, M. J. (2020). *The Drone Age: How Drone Technology Will Change War and Peace.*

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57–71). Retrieved from https://doi.org/10.1037/13620-004

Britannica (n.d.a). Baltic languages. Retrieved from https://www.britannica.com/topic/Baltic-languages

Britannica (n.d.b). Finno-Ugric languages. Retrieved from https://www.britannica.com/topic/Finno-Ugric-languages

The National Concept on Strategic Communication and Security of the Information Space 2023–2027 (2023).

CCDCEO (2017). The Tallinn Manual. Retrieved from https://ccdcoe.org/research/tallinn-manual/

Česnauskė, J. (2019). DIGITAL ECONOMY AND SOCIETY: BALTIC STATES IN THE EU CONTEXT. *ECONOMICS and CULTURE*, *16*(1). Retrieved from DOI: 10.2478/jec-2019-0009

Chacón, R. (2018). Diagnosing the Fault Lines of Globalization in a Post-Truth Era. *The Flechtcher Forum of World Affairs*, *42*(2).

Chahal, H., Fedasiuk, R., & Flynn, C. (July 2020). Messier than Oil: Messier than Oil: Assessing Data Advantage in Military AI. Retrieved from https://cset.georgetown.edu/wp-content/uploads/Messier-than-Oil-Brief-1.pdf

Chiappetta (2022). Digital Geopolitics. In R. Baikady, S. Sajid, V. Nadesan, J. Przeperski, M. R. Islam, & J. Gao (Eds.), *The Palgrave Handbook of Global Social Change* (pp. 1–18). Retrieved from https://doi.org/10.1007/978-3-030-87624-1_245-1

Ciolan, I. M. (2014). DEFINING CYBERSECURITY AS THE SECURITY ISSUE OF THE TWENTY FIRST CENTURY. A CONSTRUCTIVIST APPROACH. *Revista De Administratie Publica Si Politici Sociala*, *12*(1). Retrieved from https://www.proquest.com/openview/95f174fdd3a40176ae1ff5f7ba24a597/1?pq-origsite=gscholar&cbl=816332

Ciuriak, D. (2023). The Digital Revolution Has Transformed Geopolitics. Retrieved from https://www.cigionline.org/articles/the-digital-revolution-has-transformed-geopolitics/

Clüver Ashbrook, C. (2023). GEOPOLITICS, GOVERNANCE AND DIPLOMACY OF TECHNOLOGY: RECENT TRENDS. In *Democracy- Affirming Technologies: Aligning Technology With Public Interest And Social Good* (pp. 34–52). Retrieved from https://globernance.org/wp-content/uploads/2023/07/2023.07.02-Report-Tech4Democracy-and-Social-Good.pdf#page=34

Colby, E., & Solomon, J. (2015). Facing Russia: Conventional Defence and Deterrence in Europe. *Global Politics and Strategy*, *57*(6), 21–50. Retrieved from https://doi.org/10.1080/00396338.2015.1116146

Collins, R. (1981). Does modern technology change the rules of geopolitics? *Journal of Political & Military Sociology*, *9*(2), 163–177. Retrieved from https://www.jstor.org/stable/45293569

Crosby, C. (2020). Operationalizing Operationalizing Artificial Intelligence for Algorithmic Warfare. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-20/Crosby-Operationalizing-AI-1.pdf

National Threat Assessment (2021).

Defense Intelligence and Security Service under the Ministry of National Defence (2022). National Threat Assessment. Retrieved from https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf

Diplo (2023). AI Diplomacy: geo-politics, topics and tools in 2023. Retrieved from https://www.diplomacy.edu/topics/ai-and-diplomacy/

Djeffal, C., & et.al. (2022). Role of the state and responsibility in governing artifical intelligence: a comparative analysis of AI strategies. *Journal of European Public Policy*, *29*(11), 1799–1821. Retrieved from https://doi.org/10.1080/13501763.2022.2094987

Dov Bachmann, S.-D., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, *14*(5), 858–869. Retrieved from DOI: 10.1111/1758-5899.13257

E-Estonia (2023). Factsheet: AI- "kratt" strategy. Retrieved from https://e-estonia.com/wp-content/uploads/factsheet-ai-strategy-feb2023.pdf

Epp, A. (2012). The Problem of Soviet Colonialism in the Baltics. *Journal of Baltic Studies, 43*(1), 21–45. Retrieved from doi:10.1080/01629778.2011.628551

Eriksson, J., & Giacomello, G. (2007). *International Relations Theory and Security in the Digital Age*.

Estonian Foreign Intelligence Service (2022). International Security and Estonia. Retrieved from https://www.valisluureamet.ee/doc/raport/2022-en.pdf

Estonian Foreign Intelligence Service (2023). International Security and Estonia. Retrieved from https://raport.valisluureamet.ee/2023/en/

Estonian Ministry of Foreign Affairs (2020). Estonian Foreign Policy Strategy 2030. Retrieved from https://vm.ee/sites/default/files/documents/2022-08/estonian_foreign_policy_strategy_2030_final.pdf

EU Cyber Direct (2019). Cyber-related PESCO projects. Retrieved from https://eucyberdirect.eu/atlas/sources/cyber-related-pesco-projects

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4), 887–917. Retrieved from https://www.jstor.org/stable/2601361

Flockhart, T., & Korosteleva, E. A. (2022). War in Ukraine: Putin and the multi-order world. *Contemporary Security Policy*, *43*(3), 466–481. Retrieved from https://doi.org/10.1080/13523260.2022.2091591

Foreign Policy Research Institute (2020). A Chain of Friendship: Reflections on the Baltic Way and Inspirations for Belarus. Retrieved from https://www.fpri.org/article/2020/08/a-chain-of-friendship-reflections-on-the-baltic-way-and-inspiration-for-belarus/

Franke, U., & Torreblanca, J. I. (July 2021). GEO-TECH POLITICS: WHY TECHNOLOGY SHAPES EUROPEAN POWER. Retrieved from https://ecfr.eu/wp-content/uploads/Geo-tech-politics-Why-technology-shapes-European-power.pdf

Freedom House (2023). Estonia: Freedom of the Net. Retrieved from https://freedomhouse.org/country/estonia/freedom-net/2023

Fukuyama, F. (1989). The End of History? *The National Interest*, *16*, 3–18. Retrieved from https://www.jstor.org/stable/24027184

Galeotti, M. (2018). The mythical 'Gerasimov Doctrine' and the language of threat. *Critical Studies on Security*. Retrieved from https://doi.org/10.1080/21624887.2018.1441623

Galeotti, M. (04.2019). The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy. George C. Marshall European Center for Security Studies: George C. Marshall European Center for Security Studies. Retrieved from https://www.marshallcenter.org/en/publications/security-insights/baltic-states-targets-and-levers-role-region-russian-strategy-0

Goldberga, A., Kreislere, M., Sauka, J., Stürmane, A., & Virbule, I. (2014). RDA: From Strategy to Experiments and Implementation in Latvia (Including an Overview of the Situation in the Baltic States). *Journal of Library Metadata*, *14*(3.4), 205–221. Retrieved from https://doi.org/10.1080/19386389.2014.992710

Górka, M. (2023). Baltic States Cyber Security Policy: Development of digital capabilities in 2017-2022. *Stosunki Międzynarodowe – International Relations*, *3*(15). Retrieved from https://doi.org/10.12688/stomiedintrelat.17684.1

Haddick, R. (2014, February 6). America Has No Answer to China's Salami-Slicing. Retrieved from https://warontherocks.com/2014/02/america-has-no-answer-to-chinas-salami-slicing/

Herdt, C. S., & Zublic, M. (2022, November 14). Baltic Conflict: Russia’s Goal to Distract NATO? Center for Strategic & International Studies: Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/baltic-conflict-russias-goal-distract-nato

Higgins, A. (2022, June 27). Lithuania blames Russia for cyberattacks, citing threats over cargo restrictions.: Hackers have struck dozens of Lithuanian government and private organizations, according to a Lithuanian official. The New York Times: The New York Times. Retrieved from https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html

Hodunova, K. (2024, January 17). ISW: Putin attempts to destabilize Baltic countries. The Kyiv Independent: The Kyiv Independent. Retrieved from https://kyivindependent.com/isw-putin-attempts-to-destabilize-baltic-countries/

Hoffmann, F. (2009). Hybrid Warfare and Challenges. *JFQ*. (52). Retrieved from https://www.academia.edu/22884324/Hybrid_Warfare_and_Challenges

Kasekamp, A. (2019). Survival against the Odds: The Baltic States at 100. *Slavic Review*, *78*(3), 640–647. Retrieved from https://www.jstor.org/stable/26844316

Kļaviņš, D. (2021). The transformation of the Ministries of Foreign Affairs in the Baltic countries. *Journal of Baltic Studies*, *52*(2), 245–267. Retrieved from https://doi.org/10.1080/01629778.2021.1912790

Kunkunrat, K. (2022). TECHNOLOGY AND GEOPOLITICS: A CHALLENGE IN THE DIGITAL AGE. *Journal Ekonomi*, *11*(3). Retrieved from http://ejournal.seaninstitute.or.id/index.php/Ekonomi

Latvian Foreign and Security Policy (2021).

Latvian Institute for International Affairs (2023). Latvian Foreign and Security Policy Yearbook 2023: FSP2023. Retrieved from https://www.liia.lv/en/publications/latvian-foreign-and-security-policy-yearbook-2023-1047?get_file=2

Loh, M. (2024, January 18). Putin is starting to talk tough about the Baltics, laying the groundwork for 'future escalations' with NATO: ISW. *Business Insider*. Retrieved from https://www.businessinsider.com/vladimir-putin-baltic-states-future-escalations-nato-ukraine-war-2024-1

Martin, A., Sharma, G., Souza, S. P. de, Taylor, L., Boudeqijn, Eerd, McDonald, Sean Martin, Cheesman, Margie, Scheel, Stephan, & Dijstelbloem, H. (2023). Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics*, *28*(3), 1362–1397. Retrieved from https://doi.org/10.1080/14650045.2022.2047468

Mazar, M. J. (2015). Mastering the Gray Zone: Understanding a Changing Era of Conflict. *Monographs, Books, and Publications*, *428*. Retrieved from https://press.armywarcollege.edu/monographs/428

Mengshu, Z. (2020). A Brief Overview of Alexander Wendt's Constructivism. *E-International Relations*. Retrieved from https://www.e-ir.info/2020/05/19/a-brief-overview-of-alexander-wendts-constructivism/#google_vignette

Minister of Foreign Affairs of Lithuania (2022). Geopolitical Future and Lithuania's Foreign Policy. Retrieved from https://jp.mfa.lt/uploads/default/documents/Speech%20by%20Gabrielius%20Landsbergis%20at%20the%20annual%20meeting%20of%20Lithuanian%20Ambassadors.pdf

Minister of Foreign Affairs of Lithuania (2024). In Vilnius, the Nordic-Baltic Eight (NB8) State Secretaries discussed security challenges, strengthening regional cooperation. Retrieved from https://www.urm.lt/en/news/928/in-vilnius-the-nordic-baltic-eight-nb8-state-secretaries-discussed-security-challenges-strengthening-regional-cooperation:34947

Ministry of Defense - Republic of Latvia (2019). The National Security Concept. Retrieved from https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf

Ministry of Defense - Republic of Latvia (2023a). The Cybersecurity Strategy of Latvia 2023-2026. Retrieved from https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf

Ministry of Defense - Republic of Latvia (2023b). The State Defense Concept. Retrieved from https://www.mod.gov.lv/sites/mod/files/document/The%20State%20Defence%20Concept%202023-2027.pdf

Ministry of Economic Affairs and Communications (2021). Estonia's National Artificial Intelligence Strategy or Kratt Strategy for 2022-2023. Retrieved from https://www.kratid.ee/en/_files/ugd/980182_4434a890f1e64c66b1190b0bd2665dc2.pdf

Ministry of Economy- Lithuania (n.d.). Let's talk Lithuania: safe and professional: Proposal to host the European Cybersecurity Industrial, Technology and Research Competence Centre. Retrieved from https://www.consilium.europa.eu/media/46681/3-lithuania-eccc-brochure_en.pdf

Ministry of Economy- Lithuania (2019). Lithuanian Artificial Intelligence Strategy. Retrieved from https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_ENG(1).pdf

Informative report " On the development of artificial intelligence solutions " (2020).

Ministry of Foreign Affairs (n.d.). Cyber diplomacy. Retrieved from https://www.vm.ee/en/activity/digital-and-cyber-diplomacy/overview-cyber-diplomacy

Ministry of Foreign Affairs Republic of Latvia (2024). Foreign Ministers of the Baltic States: Russia, by planning to hold its presidential elections in the temporarily occupied territories of Ukraine, gravely violates Ukraine's sovereignty and international law. Retrieved from https://www.mfa.gov.lv/en/article/foreign-ministers-baltic-states-russia-planning-hold-its-presidential-elections-temporarily-occupied-territories-ukraine-gravely-violates-ukraines-sovereignty-and-international-law?utm_source=https%3A%2F%2Fwww.google.com%2F

Ministry of National Defence - Republic of Lithuania (2019). National Cyber Security Strategy. Retrieved from https://kam.lt/wp-content/uploads/2022/11/2019-EN-KibernetineSaugumoStrategija-el.pdf

Ministry of National Defence - Republic of Lithuania (2022a). Key Trends and Statistics of the National Cyber Security Status of Lithuania. Retrieved from https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cybersecurity.pdf?__cf_chl_tk=j22IxQabjvhMU04muSflUUZvHIHvmX2Rjd7p5JPkD_U-1715859565-0.0.1.1-1429

Ministry of National Defence - Republic of Lithuania (2022b). Lithuania's membership in NATO. Retrieved from https://kam.lt/en/lithuanias-membership-in-nato/

Ministry of National Defence - Republic of Lithuania (2023). Lithuanian-coordinated EU Cyber Rapid Response Teams – incident response with the EU and in support of EU partners and military missions. Retrieved from https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/

Möllers, N. (2021). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, *46*(1), 112–138. Retrieved from https://doi.org/10.1177/0162243920904436

NATO (n.d.). NATO Energy Securtiy Centre of Excellence. Retrieved from https://www.enseccoe.org/

NATO (2008). What Is Article 5? Retrieved from www.nato.int/terrorism/five

NATO (2023). NATO’s military presence in the east of the Alliance. Retrieved from https://www.nato.int/cps/en/natohq/topics_136388.htm

NATO (2024). Defence Expenditure of NATO Countries (2014-2024). Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf

NATO Strategic Communications Center of Excellence (2024). Defence Strategic Communications. Retrieved from https://stratcomcoe.org/

NB8 (2010). The Wise Men Report. Retrieved from https://www.stjornarradid.is/media/utanrikisraduneyti-media/media/skyrslur/nb8-wise-men-report.pdf

Neumann, I. B. (1998). Russia as Europe's other. *Journal of Area Studies*, *6*(12), 26–73. Retrieved from https://doi.org/10.1080/02613539808455822

Nordic Co-operation (2018a). AI in the Nordic-Baltic region. Retrieved from https://www.norden.org/en/declaration/ai-nordic-baltic-region

Nordic Co-operation (2018b, May 15). Artificial intelligence (AI) can help solve major societal challenges and provide significant benefits in a variety of areas. Retrieved from https://www.norden.org/en/declaration/ai-nordic-baltic-region

O'Dwyer, G. (2024). Estonia: Rebuilding The Economy. Retrieved from https://gfmag.com/emerging-frontier-markets/estonia-rebuilding-the-economy/#:~:text=Estonia%20has%2C%20since%20its%20independence,investment%20and%20grow%20indigenous%20wealth.

OECD library (n.d.). Going Digital in Latvia. Retrieved from https://www.oecd-ilibrary.org/sites/8eec1828-en/index.html?itemId=/content/publication/8eec1828-en#:~:text=linklink%20copied!-,Increasing%20adoption%20and%20use%20of%20digital%20technologies,behind%20those%20in%20OECD%20countries.

Oficiālās statistikas portāls (2021). Iedzīvotāji pēc valstiskās piederības un dzimšanas valsts gada sākumā 2011 - 2023. Retrieved from https://data.stat.gov.lv/pxweb/lv/OSP_PUB/START__POP__IR__IRV/IRV040/

Oficialiosios statistikos portalas (2021). Rodiklių duomenų bazė. Retrieved from https://osp.stat.gov.lt/en/statistiniu-rodikliu-analize?hash=0078cd86-acd6-46a8-9843-623bdf998aba#/

Oswald, I. (2000). *Die Nachfahren des "homo sovieticus"*. Waxmann Verlag.

Patil, S., & Mishra, V. (2022). Democracy, Technology, Geopoltics. Retrieved from https://www.researchgate.net/profile/Samir-Saran/publication/360861301_Raisina_Files_2022/links/628f45b18d19206823dc4a28/Raisina-Files-2022.pdf#page=28

Paulauskas, K. (February 2006). *The Baltics: from nation states to member states*. Retrieved from European Union Institute for Security Studies website: https://www.iss.europa.eu/sites/default/files/EUISSFiles/occ62.pdf

Pawlak, P. (2013). Cyber world: sit eunder construction. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/d1e5b7c0-34a5-4a07-a500-acd3190c28b1/language-en

PDGA (2014). Baltic countries map. Retrieved from https://www.pdga.com/2014-prodiscus-baltic-sea-tour

Popescu, A.-I. C. (2021). THE GEOPOLITICAL IMPACT OF THE EMERGING TECHNOLOGIES. *Bulletin of "Carol I" National Defence University*, *4*, 7–21. Retrieved from https://www.ceeol.com/search/article-detail?id=1007754

Priyono, U. (2022). CYBER WARFARE AS PART OF RUSSIA AND UKRAINE CONFLICT. *Jurnal Diplomasi Pertahanan*, *8*(2). Retrieved from DOI: https://doi.org/10.33172/jdp.v8i2.1005

Republic of Estonia (2023). Cybersecurity Strategy. Retrieved from https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf

Republic of Estonia - Government, & Republic of Estonia - Ministry of Economic Affairs and Communications (2019). Report of Estonia's AI Taskforce. Retrieved from https://www.kratid.ee/_files/ugd/980182_681757534b4a444caf6b7bd8796cfc4c.pdf

Republic of Estonia - Information System Authority (2022). Cyber attacks against Ukraine and possible impact in Estonia: Threat and Risk Assessment. Retrieved from https://ria.ee/en/news/threat-assessment-cyber-attacks-against-ukraine-and-possible-impact-estonia

Republic of Estonia - Ministry of Foreign Affairs (2020). Foreign Policy Development Plan 2030 of the Government of the Republic of Estonia. Retrieved from https://vm.ee/sites/default/files/documents/2022-08/estonian_foreign_policy_strategy_2030_final.pdf

Republic of Estonia - Ministry of Foreign Affairs (2024). Nordic-Baltic Cooperation (NB8): In 2024, the Nordic-Baltic cooperation format (NB8) is chaired by Sweden which was taken over from Latvia. Estonia chaired the Nordic-Baltic cooperation in 2020. Retrieved from https://vm.ee/en/international-relations/regional-cooperation/nordic-baltic-cooperation-nb8

Republic of Latvia - Constitution Protection Bureau (2023). Annual Report. Retrieved from https://sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_ENG.pdf

Ringhof, J., & Torreblanca, J. I. (May 2022). THE GEOPOLITICS OF TECHNOLOGY: HOW THE EU CAN BECOME A GLOBAL PLAYER. Retrieved from https://ecfr.eu/wp-content/uploads/2022/05/The-geopolitics-of-technology-How-the-EU-can-become-a-global-player.pdf

Roussi, A. (2022, August 18). Estonia fends off 'extensive' cyberattack following Soviet monument removal: Baltic states facing attacks from pro-Kremlin hackers as they pressure Russia. Politico: Politico. Retrieved from https://www.politico.eu/article/estonia-extensive-cyber-attack-following-soviet-war-monument-removal/

Saburova, I. (1955). The Soviet Occupation of the Baltic States. *The Russian Review*, *14*(1), 36–49. Retrieved from https://www.jstor.org/stable/126075

Savu, L.-M. (2021). REALISM, LIBERALISM AND CONSTRUCTIVISM IN THE PURSUIT OF SECURITY. Retrieved from DOI: 10.53477/2668-2001-21-02

Schadlow, N. (August 2014). Peace and War: The Space Between. Retrieved from https://warontherocks.com/2014/08/peace-and-war-the-space-between/

Schweller, R. (1994). Bandwagoning for Profit: Bringing the Revisionist State Back In. *International Security*, *19*(1), 72–107. Retrieved from https://www.jstor.org/stable/2539149

Seimas of the Republic of Lithuania (2016). Programme of the Government of the Republic of Lithuania (Foreign Policy part). Retrieved from https://www.urm.lt/en/key-foreign-policy-documents/programme-of-the-government-of-the-republic-of-lithuania-foreign-policy-part/1335

National Security Strategy (2021).

Shu, H.-H. (2023). Anniversary of Russia-Ukraine War: Battlefield Experience and Lessons about the Main Battle Equipment. Retrieved from https://indsr.org.tw/uploads/enindsr/files/202305/eabf0d64-9c04-43e9-8d4c-d55b19a1b094.pdf

Silini, G., & Molina, L. (2024). The geopoltiical effects of Artificial Intelligence: The implications on International Relations. Retrieved from https://mondointernazionale.org/focus-allegati/the-geopolitical-effects-of-artificial-intelligence-the-implications-on-international-relations

Song, L., & Changshan, M. (2022). Identifying the fourth generation of human rights in digital era. *International Journal of Legal Dscourse*, *7*(1), 83–111. Retrieved from https://doi.org/10.1515/ijld-2022-2065

State Border Guard- republic of Latvia (2019). Introduction of the FRONTEX Liaison Officer at a kick-off meeting. Retrieved from https://www.rs.gov.lv/en/article/introduction-frontex-liaison-officer-kick-meeting?utm_source=https%3A%2F%2Fwww.google.com%2F

State Security Department of The Republic of Lithuania (2023). National Threat Assessment. Retrieved from https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf

Statista Estonia (2021). RL21429: POPULATION BY ETHNIC NATIONALITY, SEX, AGE GROUP AND PLACE OF RESIDENCE (ADMINISTRATIVE UNIT). Retrieved from https://andmed.stat.ee/en/stat/rahvaloendus__rel2021__rahvastiku-demograafilised-ja-etno-kultuurilised-naitajad__rahvus-emakeel/RL21429

Statistics Estonia (2021). RL21451: AT LEAST 15-YEAR-OLD PERSONS BY RELIGION, SEX AND PLACE OF RESIDENCE (SETTLEMENT REGION). Retrieved from https://andmed.stat.ee/en/stat/rahvaloendus__rel2021__rahvastiku-demograafilised-ja-etno-kultuurilised-naitajad__usk/RL21451

Statistics Lithuania (2022). Population by religious community indicated, municipalities (2021). Retrieved from https://osp.stat.gov.lt/lt/statistiniu-rodikliu-analize?hash=dadee47b-9204-48d2-a55e-e125d581f1b6#/

Sytas, A. (2023, February 8). Russian threat to Baltic security rising- Estonian intelligence report. Reuters: Reuters. Retrieved from https://www.reuters.com/world/europe/baltic-security-risk-rising-estonian-intelligence-service-says-2023-02-08/

Taagepera, R. (1990). The Baltic States. *Electoral Studies, 9*(4), 303–311. Retrieved from https://escholarship.org/content/qt6s22w6sr/qt6s22w6sr.pdf

Thom, F. (2023, February 26). War in Ukraine ‘stems from the Orange Revolution, a humiliating ordeal for Putin’: One year into the war that Russia launched against Ukraine, FRANCE 24 takes a closer look at the anti-Western rhetoric President Vladimir Putin used to justify the conflict, which is rooted in events in the early 2000s, according to historian Françoise Thom, an expert on post-Communist Russia. France 24: France 24. Retrieved from https://www.france24.com/en/europe/20230226-war-in-ukraine-stems-from-the-orange-revolution-a-humiliating-ordeal-for-putin

Tieslietu ministrija (2019). Ziņojums par Tieslietu ministrijā iesniegtajiem reliģisko organizāciju pārskatiem par darbību 2019.gadā. Retrieved from https://www.tm.gov.lv/lv/media/3934/download

Tilovska-Kachedji, E. (2023). NAVIGATING THE GEOPOLITICAL LANDSCAPE OF ARTIFICIAL INTELLIGENCE: REFLECTIONS AND CHALLENGES. *Journal of Liberty and International Affairs*, *9*(3). Retrieved from https://doi.org/10.47305/JLIA2393599tk

Trenin, D. (2011). *Post-imperium: A Eurasian story.*

Tsereteli, M. (2014). Georgia and Moldova: staying the course. In Starr, Frederick, S. & S. E. Cronell (Eds.), *Putin's Grand Strategy: The Eurasian Union and Its Discontents* (pp. 133–144). Washington DC, Stockholm. Retrieved from https://www.silkroadstudies.org/resources/pdf/publications/11-1409GrandStrategy-Georgia.pdf

Urbelis, V. (2020). THE NEW UNITED STATES DEFENCE STRATEGY: CONSEQUENCES FOR THE BALTIC STATES. In G. Cesnakas & N. Statkus (Eds.), *Lithuania in the global context: National security and defence policy dilemmas* (pp. 64–83). Vilnius. Retrieved from https://biblioteka.lka.lt/data/PDF-leidiniai/2016-2020/2020-Matonyte-Lithuania%20in%20the%20global%20context.pdf#page=65

Urbina, Fabio, et. al. (2022). Dual use of artificial-intelligence-powered drug discovery. *Nature Machine Intelligence*, *4*(3), 189–191. Retrieved from https://doi.org/10.1038/s42256-022-00465-9

Van Dyk, S. (2022). Post-Truth, the Future of Democracy and the Public Sphere. *Theory, Culture & Society*, *39*(4), 37–50. Retrieved from https://doi.org/10.1177/02632764221103514

Vogel, T., & Kunze, T. (2011). Von der Sowjetunion in die Unabhängigkeit. Retrieved from https://www.bpb.de/shop/zeitschriften/apuz/59638/von-der-sowjetunion-in-die-unabhaengigkeit/

Waltz, K. (1979). *Theory of International Politics* (First Edition). Boston: Addison-Wesley.

Weitz, E. D. (2002). Racial Politics without the Concept of Race: Reevaluating Soviet Ethnic and National Purges. *Slavic Review*, *61*(1), 1–29. Retrieved from https://www.jstor.org/stable/2696978

Wendt, A. (1999). *Social Theorey of International Politics*. Virtual Publishing: Cambridge University Press. Retrieved from https://www.guillaumenicaise.com/wp-content/uploads/2013/10/Wendt-Social-Theory-of-International-Politics.pdf (Original work published 1999

Whyte, A. (2024, January 19). Think tank: Putin tough talk on Estonia groundwork for 'future escalation'. ERR.ee: ERR.ee. Retrieved from https://news.err.ee/1609226874/think-tank-putin-tough-talk-on-estonia-groundwork-for-future-escalation

World Bank (n.d.). GDP per capita (current US$). Retrieved from https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?end=2023&skipRedirection=true&start=1991&view=chart

Wright, H., & Tambur, S. (2021, August 23). The Baltic Way - the longest unbroken human chain in history. *Estonian World*. Retrieved from https://estonianworld.com/life/estonia-commemorates-30-years-since-the-baltic-way-the-longest-unbroken-human-chain-in-history/