TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance

Hauke Claus Schulz

Georgia's, Moldova's, and Ukraine's cybersecurity engagements with the EU and NATO

Master's thesis
Technology Governance and Sustainability

Supervisor: Radu Antonio Serrano Iova, MSc

Tallinn 2023

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.

The document length is 15929 words from the introduction to the end of the conclusion.

Hauke Claus Schulz, 19.12.2023

TABLE OF CONTENTS

ABSTRACT

The author of this thesis has scrutinised how Georgia, Moldova, and Ukraine cooperate with the EU and NATO in the cybersecurity domain below the threshold of full organisational membership and how that engagement provides them shelter as small states. By drawing from small state literature and utilising framework analysis as the main research methodology, this qualitative comparative case study used both primary as well as secondary sources. The findings indicate that cybersecurity cooperation is accomplished through numerous ways including, exercises, trainings, other educational activities, information sharing, capacity building initiatives and more. Cybersecurity engagements between the two international organisations and the three countries appear to have been significantly strengthened since February 2022, i.e. since the full-scale war against Ukraine started. The study further suggests that as a result of their engagements, the three countries are sheltered in the political, economic as well societal sphere.

Keywords: Georgia, Moldova, Ukraine, small states, cybersecurity, international cooperation, shelter theory, EU, NATO, framework analysis

List of Abbreviations

Acronym	Explanation
ANP	Annual National Programme
APT	Advanced Persistent Threat
BI	Building Interoperability Programme
CCB	Cyber(security) capacity building
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CoE	Council of Europe
COVID	Coronavirus disease
CSDP	Common Security and Defence Policy
DCB	Defence and Related Security Capacity Building Initiative
DCFTA	Deep and Comprehensive Free Trade Area
DEEP	Defence Education Enhancement Programme
EAEC	European Atomic Energy Community
EaP	Eastern Partnership
EDA	European Defence Agency
eGA	e-Governance Academy
ENISA	European Union Agency for Cybersecurity
EPF	European Peace Facility
EU	European Union
EUR	Euro
FIIAPP	International and Ibero-American Foundation for Administration and Public Policies
GDF	Georgian Defence Forces
GDP	Gross domestic product
GRENA CERT-GE	Georgian Research and Educational Networking Association Computer Emergency Response Team
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
ICT	Information and Communication Technologies
IDC	Information and Documentation Centre
IP	Interoperability Platform
IPAP	Individual Partnership Action Plan
IR	International Relations
IT	Information Technology
JTEC	NATO-Georgia Joint Training and Evaluation Center
MAFCIRC	Moldova Armed Forces Cyber Incident Response Capability
MAP	Membership Action Plan
MISP	Malware Information Sharing Platform
MoD	Ministry of Defence

NATO	North Atlantic Treaty Organization
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NATO StratCom COE	NATO Strategic Communications Centre of Excellence
NCSS	National Cyber Security Strategy
NIDC	NATO Information and Documentation Centre
NIS	Network and Information Security (Directive)
OSCE	Organization for Security and Co-operation in Europe
PARP	Partnership for Peace Planning and Review Process
PESCO	Permanent Structured Cooperation
PfP	Partnership for Peace
SAFE	Safety Actions for Europe
SNGP	Substantial NATO-Georgia Package
SPS	NATO Science for Peace and Security
SSSCIP	State Service for Special Communications and Information Protection of Ukraine
TAIEX	Technical Assistance and Information Exchange
UA	Ukraine
UNOPS	UN Office for Project Services
US	United States of America
USD	United States dollar

1. Introduction

In 1988, a graduate student in Computer Science from the United States named Robert Morris released a piece of software, which was later dubbed the "Morris Worm", and became known as the first documented cyber-attack in history. The software led to disruptions on the Internet which was still in its infancy at that time. (Gordon & Rosenbach, 2022, p. 12) Since then, 35 years have passed, and the wide-spread adoption of Information and Communication Technologies (ICT) has dramatically altered the way governments, businesses and people interact with one another. In fact, the proliferation of ICTs and networking technologies is a cross-dimensional concern which besides technical aspects, has implications on humans, politics, cultures, legal systems, and societies (Neuneck, 2013, p. 92). Naturally, the "*Cyber Revolution*" (Kello, 2013) also had a profound impact on the overall cyber threat landscape. Societies are increasingly reliant on digital infrastructures which in turn give malicious actors ample opportunities for online abuse, criminal activities as well as cyber warfare. While classifications of cyber threat actors can differ, they usually encompass actors such as cybercriminals, hacktivists, cyberterrorists/ terrorist groups, thrill seekers, insider threats, state-sponsored actors, and nation states (these last ones also referred to as advanced persistent threat, APT). (Årnes, 2022, pp. 2-4) Observing the more recent past, the COVID-19 pandemic has caused both governments and private companies to transition to online modes of working arrangements and services which significantly increased the number of people relying on online security. Following this, the issuance of vaccines and health certificates drew attention to issues concerning digital health and data security. (Maigre, 2023, p. 55) Since February 2022 24th , i.e. since Russia's full-scale invasion against Ukraine, it has become evident that cyber-attacks are not a separate arena but are rather an integral part of the conflict (Maigre, 2023, p. 55) targeting Ukrainian governmental authorities, critical infrastructure (CI) operators, local governments, military and security sectors (Information System Authority, 2023, pp. 14-17; State Service of Special Communications and Information Protection of Ukraine, 2022). In fact, several reports and domain experts indicate that cyber-attacks aimed at both the private and public sector are on the rise (Poireault, 2023; SonicWall, 2023; Microsoft, 2022a). Cyber threats are also considered, by representatives from both sectors, to belong to the top organisational and global risks (World Economic Forum, 2023a; World Economic Forum, p. 2023b; ENISA, 2023a). Cyber-

attacks aimed at states can have severely detrimental consequences on social trust, the pillars of democracy and also disrupt the functioning of the global economy (Gordon & Rosenbach, 2022, p. 10). It should be emphasised that cyber-attacks are not exclusively a challenge for bigger states, but also smaller ones are frequently exposed to such attacks. In fact, evidence suggests that particularly small states are confronted with a greater risk of cyber-attacks stemming from the world's major powers in this domain. These "cyber powers" are allocating substantial financial resources into their offensive cyber capabilities and demonstrating willingness to use them against smaller and weaker states in conflicts. (Burton, 2013, p. 224) In contradistinction to larger states, small states are more vulnerable to the ramifications of cyber conflict. Larger states might employ offensive cyber means to affect the national policy outcomes of smaller target states. (Tan, 2019, p. 159) More recent examples of cyber-attacks targeting small states include the Western Balkan states of Albania, Montenegro and North Macedonia which became targets to varying degrees of severity in 2022 (Microsoft, 2023; Microsoft., 2022b; Reuters, 2022; Marusic, 2022). Burton (2013) argues that the cyber vulnerabilities of small states can be associated with the past geopolitical struggles involving countries in their immediate vicinity (p. 224). In a similar vein Crandall (2014) notes that small former Soviet states with bigger neighbours might have to deal with soft security threats, i.e., potential security issues short of military conflict, including cybersecurity threats (p. 31). Georgia, Moldova, and Ukraine are a case in point in that context. These three post-Soviet states are confronted with an increasingly encroaching and assertive Russia. It would go beyond the scope of this introduction to elaborate on all the crucial challenges and nuances these countries are facing vis-à-vis Russia, but all three are grappling with separatist regions, territorial disputes and hybrid warfare activities including cyber-attacks. (see Neljas, 2020; Mirel, 2021; Całus, 2023) While at the time of writing, the unprovoked full-scale war against Ukraine is in full swing, Georgia and Moldova have had similar experiences with the Russian Federation since their independence.

One way for states to address the challenges stemming from cyberspace in a systematic way is to develop their own National Cyber Security Strategy (NCSS). Both numerous smaller and bigger states have developed NCSSs in the past which are periodically (mostly every 3-5 years) renewed (see National Cyber Security Index, n.d.; International Telecommunication Union, n.d.). Among other crucial focus areas, cooperation at the regional and international levels is identified to be of importance (NCS Guide, 2021, pp. 5, 50-53; Osula & Kaska, 2013, pp. 15, 17, 24). This is because of the transnational character of cyber threats which requires *"(...) international cooperation and coordination of activities, including cooperation in international and regional organisations with*

a cyber security agenda, organisations whose agenda affects national, regional or international cyber security (...)" (Osula & Kaska, 2013, p. 17). It is particularly relevant for small states, as their security relies on stability, predictability, and collaborative approaches to international challenges (Brady & Thorhallsson, 2021, p. 2). In this setting, international cooperation is also deemed necessary to thwart the potential of future cyber conflict (Neuneck, 2013, p. 92). Additionally, since small states tend to have less resources at their disposal compared to their bigger counterparts, they seek protection and assistance from international organisations where they may also have the opportunity to influence these organisations for their advantage (Crandall, 2014, p. 32). In other words, small states can significantly benefit from international cooperation and also through institutional memberships (Bailes et al., 2016, pp. 1, 5). In the European and Euro-Atlantic context, international cybersecurity cooperation can be achieved at international institutions such as the EU and military alliances as the North Atlantic Treaty Organization (NATO). In the past, NATO and EU enlargement has given small states the institutional and legal framework to engage with more powerful nations on an equal footing (Crandall, 2014, p. 31). Notably, while neither Georgia, Moldova nor Ukraine are members of the EU or NATO, they nevertheless have close and institutionalised ties to both organisations via, among other initiatives, the Eastern Partnership (EaP) and Partnership for Peace (PfP) respectively.

1.1. Research Problem & Research Aim

The author of this thesis seeks to scrutinise the approaches of small states, to be more precise, of Georgia, Moldova, and Ukraine, in regard to international cooperation in the cybersecurity domain with regional international organisations and how these countries are sheltered through that cooperation. The need for such a study is threefold covering arguments about the role of small states in International Relations (IR); cybersecurity and IR more generally; both small states and cybersecurity in IR and the pronounced lack of comparative studies in these sub-domains. First, Veenendaal & Corbett (2014) argue that comparative scholars need to put more emphasis on small states as these are strikingly missing from traditional comparative political research (pp. 527-528). The small state concept is particularly relevant to studies focusing on security matters as small states face unique challenges in regard to their size such as political and physical survival (Knudsen, 1996, p. 5). Small states have specific needs, pursue distinct foreign policies, and face more difficulties in realising beneficial policy objectives (Thorhallsson & Steinsson, 2017, p. 1). Second, while emerging scholarly output on cybersecurity issues in the IR sub-field of security

studies can be observed (Kello, 2013, p. 8; Burton 2013, p. 216), and the importance of it has been recognised (Valeriano & Maness, 2018, p. 259), comparative case studies remain scarce and focus has been rather put on outlier occurrences such as the Stuxnet attack in 2010, the Sony Hack of 2014 or the Estonian cyber-attacks of 2007 (Valeriano & Maness, 2018, p. 260; Crandall & Allan, 2015). In a comparable manner, Domingo (2022) notes that existing studies have mostly scrutinised powerful states (e.g. China, the United States of America, Russia) and their hostilities and rivalries in the cyber domain (pp. 6, 37). Valeriano & Maness (2018) concede that examining such atypical events might enhance the overall understanding of the topic, but they bring attention to the circumstance that *"(...) explaining the everyday and typical in cyber interactions is often overlooked"* (p.260). Third, notwithstanding that academic literature on cybersecurity in IR is an emerging field, considerably less attention has been paid on how cybersecurity issues are affecting small states (Burton, 2013, p. 216). Existing small state studies in this sub-subdomain have mostly focused on the responses to cyber-attacks and less on the implications of technology on cyber strategy and foreign policy (Domingo, 2022, p. 5). Taking this into account, it can be stated that the approaches of Georgia, Moldova, and Ukraine regarding international cooperation with the EU and NATO in the cybersecurity field are understudied. This is particularly true from a comparative case study perspective employing small state literature. The fact that none of the three countries in question are members of either NATO or the EU makes this study particularly relevant as it can give further insights on how small states are sheltered below the threshold of full organisational membership. While Ukraine might not appear to be a small state at first appearance, Baldacchino & Wivel's (2020) synthetised definition of the small state concept, which puts emphasis on power asymmetries, suggest that also Ukraine can be construed as a small state. Against this backdrop, the author seeks to contribute to the growing literature on small states and cybersecurity.

1.2. Research Questions

This thesis is trying to answer the following research questions:

- How do Georgia, Moldova, and Ukraine cooperate with the EU and NATO in the cybersecurity field?
- How does this cooperation provide them political, economic, and societal shelter as small states?

1.3. Research Design & Structure of the Thesis

To find answers to the research questions, the author has conducted a qualitative small-n comparative case study by drawing from small state literature, such as Thorhallsson's Shelter Theory and Burton's (2013) conceptual model of small state security which is predicated on alliances, institutions, and norms. The research methodology is rooted in framework analysis. Primary sources such cybersecurity related strategies and policies as well as secondary sources including official reports and press releases served as the basis of the data collection process.

Following this introduction, the next chapter (2. Theory) will present a comprehensive literature review in which the reasons for utilising small state literature, the small state concept, shelter theory and the conceptual framework are discussed. Subsequently, the ensuing chapter (3. Research Methods) outlines the peculiarities of the research design in more detail, addresses conceptualisation issues, data collection and data analysis aspects, case selection as well as limitations and challenges. The fourth chapter (4. Empirical part) provides the necessary context for the analytical section. The focal point of the thesis is the analytical section (5. Analysis). Methodologically, this section is structured by first discussing the key elements that have been identified as per the framework analysis method (e.g. strategic and regulatory alignment) followed by an analysis through the prism of shelter theory. The sixth chapter (6. Conclusion) concludes this thesis by summarising key findings and suggesting potential areas of future research.

2. Theory

This chapter will first elaborate on the reasons why it is adequate for the study at hand to opt for small state literature and not some other major IR theory. This will be followed by a comprehensive exploration of the small state concept and the reasons why Baldacchino & Wivel's (2020) synthetised definition has been chosen. Subsequently, the main tenants of shelter theory will be presented. Ultimately, Burton's (2013) conceptual model of small state security, which is based on alliances, institutions, and norms, will be summarised in a synthesised fashion by also drawing insights from other scholars and sources.

2.1. Why small state literature?

As this thesis aims to scrutinise the international cooperation approaches of small states with international organisations, it would have been conceivable to draw from some of the traditional theories in IR, namely realism, liberalism, or constructivism. These theories present accessible frameworks for analysing the very intricate environments in which states, international organisations and other actors operate (Thorhallsson, 2018, p. 23; McGlinchey, 2022). In fact, Bailes et al. (2016) observe the tacit assumptions of IR scholars that theoretical frameworks or models which give insights about great power behaviour can be readily applied to small states or even that small states lack relevance as independent objects of study because of their limited impact on global politics (pp. 1-2). For instance, according to the realist school of thought, the role of small states in IR is limited and smaller states are deemed to function as pawns in great power competition (Thorhallsson, 2018, p. 23). Also, proponents of small state literature point out that constructivism is rather a framework about social facts than a universal theory about international affairs, which means that it is not possible to draw coherent lessons from it, as long as attention is not given to the development of distinct theories about small states grounded in constructivist theory (Brady & Thorhallsson, 2021, p. 5).

Traditional IR theories might be valuable for understanding the actions of great powers, however, they are inadequate to shed light on the behaviours of small states. The latter encounter situations,

obstacles, influences, and opportunities that former do not experience (Bailes et al., 2016, p. 2). In addition, due to their unique vulnerabilities, small states face different types of threats than their bigger counterparts. Besides conventional military threats, also newer phenomena such as national security threats centred around financial security, energy security, national identity security and cybersecurity are more pronounced. (Crandall & Allan, 2015, p. 346; see also Thorhallsson, 2018, p. 21; Crandall, 2014, p. 31) Small states are unique actors in international affairs and for researchers to be able to adequately interpret their behaviours, it is imperative to apply nuanced theoretical frameworks (Bailes et al., 2016, p. 1). Thus, it is appropriate to utilise small state literature for the thesis at hand and not rely on traditional IR theories such as realism, liberalism, or constructivism.

2.2. Defining Smallness

Within the IR subfield of small state studies, the question what constitutes a small state and what does not is a common and contested subject and there is no scholarly consensus on that matter (Burton, 2013; Crandall, 2014, p. 3; Baldacchino & Wivel, 2020, p. 3; Bladaitė & Šešelgytė, 2020, p. 1012, Randma-Liiv & Sarapuu, 2019, p. 163, Thorhallsson, 2006, p. 9; Veenendaal & Corbett, 2014, p. 529). This also applies to the question how smallness affects the security of small states (Bladaitė & Šešelgytė, 2020, p. 1012). Distinctions between different (sub-)categories such as microstate, small state and middle power are often vague and unsystematic (Mouritzen and Wivel, 2005; Raadschelders, 1992 cited in Baldacchino & Wivel, 2020, p. 3).

One of the more parsimonious approaches is to define a small state as a state which is not a great power (Baldacchino & Wivel, 2020, p. 4). As Baldacchino & Wivel (2020) point out such an understanding has deep historical origins: *"During the European Concert (1815–1914), all states except Austria, Prussia, Russia, the United Kingdom and France were small states."* (p. 4). However, distinctions between "great" and "small" nowadays are not self-evident. (Baldacchino & Wivel, 2020, p. 4) In a similar vein, Thorhallsson & Steinsson (2017) note that definitions of small size become more variable and contingent, i.e., open for interpretation, the more one goes back in history *"(...) as political units were far more diverse and fragmented, with different sources of state power and with far lower absolute population numbers"* (p. 3). In short, defining smallness based on such anachronistic premises would relegate small states to marginalised and overlooked entities in international relations (Baldacchino & Wivel, 2020, p. 4).

Most small state concepts focus on material factors such as population size and economic factors with cut-offs/ limits ranging from 1-15 million people and economies making up less than 1 % of world total output respectively (Burton, 2013, p. 217; see also Thorhallsson, 2018, p. 18; Pevcin, 2020 pp. 7-8; Veenendaal & Corbett, 2014, p. 528; Streeten, 1993, p. 197). Territory is also a factor often being considered (Thorhallsson, 2018, p. 18). When measuring absolute or relative material capabilities, strong emphasis is often put on military power as *"[m]ilitary capability permits a projection of state power beyond its territory; it creates the potential for military actions with or against other states; and builds domestic defensive capability or deterrent in case of invasion or attack"* (Baldacchino & Wivel, 2020, p. 5) These traditional variables (i.e. population size, territory, GDP, military capabilities) are the most common ones used when attempting to define small states (Thorhallsson, 2006, p. 8). It should be noted that there are also studies examining the administrative / bureaucratic capacities of small states and the consequences of smallness and limited human resources (see Farrugia, 1993; Thorhallsson, 2015, Jugl, 2018, Randma-Liiv & Sarapuu, 2019). The benefit of approaches centred around material factors are clearly and easily applicable working definitions. The shortcomings relate to cut-off points and absolute / relative selection criteria (e.g. population size, GDP, defence expenditure, etc.). First, scholars and international institutions employ different measurements when demarcating population sizes or GDPs of small states. Second, the question which selection criteria should be used and would be appropriate for defining smallness remain uncertain, especially when considering that the diminishing return of armed conquest has changed the capability preferences for all states. (Baldacchino & Wivel, 2020, p. 5) In fact, Thorhallsson (2006), by referring to the experiences of recent European history, argues that traditional variables might have been useful to outline the size of states in the old global system where military power was of utmost important to ensure the survival of states, the economies played a crucial role in developing countries militias and states were concerned with territorial acquisitions; however, nowadays European countries are predominantly concerned with economic and political collaboration (p. 13). Furthermore, territory or economy may not be valuable determinants on their own. It is conceivable that a state with a small territory might otherwise be powerful (i.e. it has a large population, big economy, and advanced military capacities) or that a state with a vast territory has limited power (Thorhallsson, 2018, p. 18).

Perceptions of smallness are also put forth by some scholars. These researchers argue that when countries perceive themselves to be small and/ or are perceived by other countries to be small, then

these countries will behave accordingly and can be seen as small (Thorhallsson, 2018, p. 20; Thorhallsson & Steinsson, 2021, p. 8) According to Thorhallsson (2006), there are six features which are of importance when it comes to perceptual size and the way it influences small state behaviour in international affairs: the opinion of the national elite on the size of the country and its external / internal capacity; the perspective of voters; the stances of other national stakeholders (companies, pressure groups); the perspectives of other countries and their political elites on the country in question; the standpoints of international organisations and other foreign international groups (e.g. external pressure groups and companies) (p. 24). The perception-based approach enables researchers to separate the small state concept from materialist and national security considerations, however, it also risks overemphasising the autonomy of action and opportunities of small states by neglecting inequalities between smaller and bigger nations (Baldacchino & Wivel, 2020, p. 6).

This thesis follows Baldacchino & Wivel's (2020) synthetised definition of small states, which aims to be both functional and pragmatic. To begin with, the scholars base their definition on international customary law and the 1933 Montevideo Convention on the Rights and Duties of States (Baldacchino & Wivel, 2020, pp. 3-4, 6). Accordingly, (small) states are understood as states with the following characterises: *"a permanent population"*; *"defined territory"*; *"government"* and the *"capacity to enter into relations with the other states"* (Montevideo Convention on the Rights and Duties of States, 1933, Article 1). While small states are (de jure) sovereign legal entities, (de facto) their autonomies differ. Furthermore, instead of trying to come up with a universally applicable definition of small states throughout time and space, the highly context-dependent nature of the small state concept is acknowledged. (Baldacchino & Wivel, 2020, pp. 6-7) In other words, traditional power-related and non-traditional variables (i.e. perception/ image) are combined and focus is put on the power that a state exercises as opposed to the power the country actually has. As per this relational understanding, highlighting power disparities, a (small) state can be relatively powerful in one relation with another state while comparatively weak with another one. (Thorhallsson, 2018, pp. 18-19; Knudsen 1996, p. 5) The pragmatic small state definition is centred around two insights. First, small states have limited capacities which is mirrored in their political, economic, and administrative systems but at the same time they also benefit from small state characteristics such as informality, strong personalisation, and a more egalitarian society. Second, relations with other states are marked by power disparities which small states cannot change on their own. (Baldacchino & Wivel, 2020, p. 7) This synthesised and pragmatic definition that puts emphasis on asymmetric relationships allows researchers to

subsume states under the category of small states which otherwise prima facie might not be deemed "small", as for example Ukraine (Pedi, 2020, p. 168; Thorhallsson & Steinsson, 2021, p. 9). In this setting Knudsen (1996) aptly states: *"The small-state experience is familiar to anyone who has had to deal with the potential threat of being swallowed up or integrated into an adjacent and significantly more powerful neighbour"* (p. 5). Following Baldacchino & Wivel's (2020) synthesised approach of the small state concept is appropriate for the study at hand, as it allows the author to incorporate Ukraine into the analysis and test shelter theory through the prism of Burton's conceptual framework.

2.3. Shelter Theory

To address the various security related challenges small states can either buffer from within, i.e., enhance their own domestic capacities / buffers (e.g. cyber capacities; robust state entities; improvement of the rule of law; achieve societal resilience etc.), or seek external shelter (Bladaitė & Šešelgytė, 2020, pp. 1011, 1014, 1025-1026; Thorhallsson, 2011; similarly see Knudsen, 1996, p. 8). Shelter theory is deducted from the shortcomings and necessities which small states face in the political, economic, and societal domains. Small states seek shelter to overcome their inherent vulnerabilities through different types of shelter provided by larger states and / or international organisations. (Thorhallsson & Steinsson, 2018) These shelters are crucial as they can mitigate risks before a crisis unfolds, minimise the ramifications when risks eventually materialise, and assist in post-crisis restoration efforts (Thorhallsson, 2011, pp. 326-327; Thorhallsson & Steinsson, 2021, p. 11). Shelter theory can also be helpful to facilitate the evaluation of costs and benefits of multilateral engagement (Brady & Thorhallsson, 2021, p. 8).

Political shelter is ensured through bigger states and / or international- / regional organisations for both military and diplomatic purposes (Thorhallsson & Steinsson, 2018) as smaller states are dependent on safety guarantees and diplomatic support (Brady & Thorhallsson, 2021, p. 6). International and regional organisations are vehicles in which small states can overcome power asymmetries. International organisations penalise deceivers and encourage cooperation and organisational norm adherence. The norms and rules of the international system are an additional avenue of how small states can be sheltered. (Thorhallsson & Steinsson, 2018; Thorhallsson & Steinsson, 2017, p. 11) Small states are facing a number of challenges in the economic sphere. Because of their smaller domestic markets, they are more reliant on open trade than their bigger

counterparts; are more exposed to economic crises; have less sectoral diversity; and have weaker fiscal institutions (Thorhallsson & Steinsson, 2018; Streeten, 1993). Moreover, small states tend to focus on goods in which they hold a comparative advantage (Streeten, 1993, p. 198). Economic shelter for small states might be provided by international organisations or other states in the shape of direct economic aid and investment, a currency union, favourable loans, market access, a common market (Thorhallsson & Steinsson, 2018; Thorhallsson, 2011, p. 327) or even access to goods of strategic value such as healthcare equipment as could be observed during the COVID-19 pandemic (Brady & Thorhallsson, 2021, p. 6). Within the social domain, small states might be in less favourable positions vis-à-vis larger states as they are usually composed of homogenous populations and potentially have less diverse, unconventional, and impactful people to retrieve from. Far more than their bigger counterparts, small states are reliant on exchanges with other cultures, world views and ideas, and may take proactive measures to prevent isolation by bringing in new ideas and approaches from other places (Brady & Thorhallsson, 2021, p. 7). Consequently, small states may also need that its citizens undertake university studies in foreign countries as they do not possess the scalability effects of larger states to educate their nationals appropriately (Thorhallsson & Steinsson, 2021, p. 17). To prevent societal inertia and to compensate for their lack of internal knowledge, small states look for societal shelter through international organisations / larger states that would allow for the spread of ideas and people (Thorhallsson & Steinsson, 2018).

2.4. Conceptual Framework – Alliances, Institutions, Norms

2.4.1. Alliances

Compared to larger states, small states have limited military capabilities due to the confines of small populations which reflects itself in the circumstance that they only have the capacity to deploy a limited number of armed forces, are able to allocate fewer financial resources to research and development for military technology and are less capable to be involved in longer military engagements (Thorhallsson & Steinsson, 2017, p. 4). As small states are less powerful in the military domain, they tend to seek to counterbalance this vulnerability by entering into alliances with more powerful states (Burton, 2013, p. 218). This usually takes the form of either bandwagoning – where small states algin themselves with more powerful or threatening ones – or balancing behaviour – in which weaker/ smaller states work together against a more powerful or threatening state (Thorhallsson & Steinsson, 2017, p. 7). The organisational aspects and goals of

alliances can differ. For example, they may be of an ad-hoc nature focusing on specific tasks or are long-term and established security partnerships as NATO (Burton, 2013, p. 218). Even small states that are lacking formal security guarantees and that are not part of NATO can benefit from a security environment where the application of forceful measures is discouraged. Potential adversaries of small states must calculate that alliances might nevertheless assist its (non-member) partner countries in the event of an attack. Finland and Sweden are examples that have benefited from such perceptions in the past. (Thorhallsson & Steinsson, 2021, pp. 12-13)

Previously, alliances were a collective security endeavour of like-minded nations for the protection of the physical domain, however, today they are also offering mechanisms for the protection of the cyber domain. Small states can profit in this field through cooperation, capacity building and information / technology sharing (Burton, 2013, p. 237). It should be stressed that cyberspace differs in a fundamental respect from traditional military domains as it has its own unique technologies that are used to transfer, process, and save digital information. However, leaving technological aspects aside, cyberspace and the other domains of warfare (i.e. land, sea, air, space) have in common that they are spaces of human practice marked by an extensive array of activity, encompassing both state and non-state actors, and by a range of weapons with different effects. (Denning, 2015, pp. 8, 15) As noted earlier, small states tend to be more vulnerable to the ramifications of cyber conflict and are confronted with the potential threat that bigger states may use offensive cyber capabilities to influence national policy outcomes (Tan, 2019, p. 159). In fact, the majority of known and recorded malicious cyber activities / operations have been attributed to bigger states (see Cyber Operations Tracker, n.d.; Significant Cyber Incidents, n.d.) and the most capable and advanced "cyber powers" tend to be bigger states, as for example reflected in the National Cyber Power Index 2022 (Voo et al., 2022, p. 9). It is not expected that small states will be capable to match the offensive and defensive cyber capabilities of their bigger counterparts (Burton, 2013, p. 224). Because of such resource constraints, small states also have less options at their disposal for punitive counteractions against hostile bigger states in the event of cyberattacks. Potential restrictive measures such as sanctions may remain ineffective due to the possibility of bigger states to seek alternative markets. (Tan, 2019, p. 162) Moreover, disproportionate foreign policy reactions to cyberattacks by small states can lead to escalation dynamics which can have severely negative consequences for them considering their inherent vulnerabilities in terms of economy, infrastructure, and physical size (ibid, p. 163).

By referring to the Estonian cyber-attacks in 2007 and Article 5 of the North Atlantic Treaty (i.e. the so-called collective defence clause), Burton (2013) states that: *"Alliances are commonly based on collective defence, whereby members will provide mutual aid in the event of an attack. There is little evidence to suggest that this is happening in the cyber security arena"* (p. 221). However, it should be noted that in 2014 at the NATO Summit in Wales, NATO allies agreed upon a new cyber defence policy. Cyber defence has been recognised to be among the responsibilities of NATO's core tasks of collective defence. This means that under certain circumstances a cyberattack can in indeed trigger Article 5 of the North Atlantic Treaty. At the same Summit, NATO allies also recognised the applicability of international law in cyberspace. (NATO, n.d.-a; see also Crandall & Allan, 2015) That is not to say that the challenges with collective cyber defence that Burton (2013) has highlighted may still persist in the case of a cyber-attack, such as attribution problems and the circumstance that malicious cyber activities are often carried out by non-state actors (p. 237). It should be highlighted that several scholars argue that there might be (sovereignty) costs for smaller states associated with alliance support. Bigger allies may require smaller states to make autonomy concessions which translates into influence of bigger states over their smaller allies. (Burton, 2013, p. 218; also, Bailes et al., 2016, p. 1; Thorhallsson, 2018, p. 23, Thorhallsson & Steinsson, 2018, Knudsen, 1996, p. 10) Moreover, smaller states might also have to fear that bigger allies withdraw their support when their interests are not being served anymore. This is why the foreign policy approaches of smaller states are often aligned with those of great powers (Burton, 2013, p. 218).

2.4.2. Institutions

The institutional approach implicitly assumes that understandings of power have evolved and that, besides military aspects, other factors also play a role in determining a country's security (Burton, 2013, p. 219; similarly, also Baldacchino & Wivel, 2020, p. 2). Small states tend to show a strong commitment to international law, prefer multilateral approaches to security problems and generally abstain from military interventionist approaches to settle conflicts (Burton, 2013, p. 220). While some scholars state that small states are confronted with structural weaknesses in international institutions, they put forth the argument that small states can nevertheless leverage multiple tactics to exert influence (Thorhallsson, 2018, p. 21) via persuasion-based strategies such as argument and framing (Panke, 2012, pp. 390, 395). Thorhallsson (2015) indicates that small states can exert significant influence within EU structures when they prioritise certain policy areas (pp. 2, 4; Thorhallsson & Steinsson, 2017, pp. 2, 9-10). Luxembourg has been successful in negotiating

beneficial terms in relation to its financial sector; the Baltic states have focused on energy security, the frictionless implementation / launch of the euro, CSDP matters; Cyprus has been lobbying against advantageous EU policies in regard to Türkiye and North Cyprus (Thorhallsson, 2015, p 2). The implementation of EU membership requirements during the pre-accession process can also have positive spill-over effects on domestic politics and organisational arrangements of would-be Member States and encourage the creation of enhanced domestic governance structures as also exhibited in the case of the Baltic states (Thorhallsson, 2016 cited in Bladaitė & Šešelgytė, 2020, p. 1018). Moreover, via international organisations small states can lower their transaction costs. Other member states, specialists, and different interested parties in these organisations can be utilised for information sharing, coordination, intake of best practices, the development of non-military alliances, and for agreements with states that otherwise would not be possible. (Thorhallsson & Steinsson, 2017, p. 11)

2.4.3. Norms

There seems to be scholarly consensus on the definition of a "norm" as it is generally understood *"(...) as a standard of appropriate behavior for actors with a given identity (...)"* (Katzenstein 1996b, 5; Finnemore 1996a, 22; and Klotz 1995b cited in Finnemore & Sikkink, 1998, p. 891). Norms can reach domestic, regional, or even global endorsement and their overall strength depends on a critical mass that shares and subsequently adopts and promotes them. Domestic norms may turn into regional / international ones over time with the help of norm entrepreneurs. (Finnemore & Sikkink, 1998, pp. 892-893) Finnemore & Sikkink (1998) argue that norms have a what they refer to as a "life cycle" which includes a three-stage process, namely an emergence, an acceptance / cascade and internalisation phase. The emergence phase takes place when a norm entrepreneur tries to persuade a substantial number of states (norm leaders) to support the new norms (Finnemore & Sikkink, 1998, pp. 888, 895). Adamson & Homburger (2019) argue that small states can also be actors in the emergence phase and may transform into entrepreneurs over time (p. 219). During the second stage a substantial number of states try to convince other states also to follow and adopt the new norms (Finnemore & Sikkink, 1998, p. 895). Within the final stage, norms become unquestioned and reach a *"taken-for-granted quality"* (ibid). It should be noted that a full completion of the life cycle is not guaranteed, and norm promotion efforts might fail already at the initial stages (Finnemore & Sikkink, 1998, p 895). In order to be successful at norm promoting, an organisational platform for promotion may be required (Crandall & Allan, 2015, p. 356). Crandall & Allan (2015) have shown in their case study on Estonia that NATO has served as

such a platform and conclude that ambitious small states can indeed utilise norm promotion to significantly enhance national interests at an international level. Furthermore, the authors demonstrate that key national individuals can utilise various mechanisms to advocate for norms. For example, by giving *"(...) speeches at universities, speeches at international conferences, addresses at or towards international organizations, discussions with other state leaders (...)"* (ibid, p. 354). Estonia's role in the establishment of the CCDCOE have inspired Latvia and Lithuania to set up similar Centres of Excellences (ibid, p. 362). In the past, small states also have been engaged in norm entrepreneurship at the United Nations level, for example through the UN Group of Governmental Experts and other international / regional organisations and / or started their own initiatives / platforms for norm promotion (see Adamson & Homburger, 2019). Norms can also be seen as an initial step towards the formation of international law (ibid, 2019, p. 226).

3. Research Methods

3.1. Conceptualisation and Definition of Key Terms

This subsection will address how key terms and concepts of this thesis are understood. First, it is crucial to highlight that the thesis is written in the field of social sciences. To be more precise, in the IR subdisciplines of security and small state studies. Second, the primary focus is on international strategic level cooperation with NATO and the EU. This thesis understands "cybersecurity" in line with Valeriano & Maness (2018) approach: *""Cyber security" refers to the threat opportunities from digital and computational technologies"* (Valeriano & Maness, 2018, p. 261). However, "cybercrime", while closely related, is not the focus of this study. Thus, cross-border law enforcement cooperation is excluded. Also, other hybrid threats such as mis-/ disinformation and election interference, election cybersecurity are outside of the main objectives of this research. Third, by drawing from the insights of Baldacchino & Wivel's (2020) synthetised definition of small states, the author conceptualises Georgia, Moldova, and Ukraine as small states. Fourth, Computer Emergency Response Team (CERT), also often referred to as Computer Security Incident Response Team (CSIRT), is a *"capability set up for the purpose of assisting in responding to computer security-related incidents (...)"* (NIST, n.d.). Fifth, cyber(security) capacity building (CCB) is understood as any EU- / NATO activity that *"(...) can strengthen a country's legal, technical, and policy capability, and protect against malicious cyber activity"* (Naylor, Painter, & Hakmeh, 2022). Sixth, the analysis section is divided into three parts, namely alliance, institution, and norms as per Burton's (2013) conceptual framework. For the purposes of this thesis, "alliance" refers to NATO and "institution" to the EU. When referring to both entities, the terms "organisations" or "international organisations" will be utilised. Importantly, other international organisations with a cybersecurity mandate (e.g. the United Nations, UN; the Organization for Security and Co-operation, OSCE; the Council of Europe, CoE; etc.) are beyond the purview of this thesis and thus not considered unless specifically mentioned. In line with the definition presented in the preceding chapter in which norms were understood*"(...) as a standard of appropriate behavior for actors with a given identity (...)"* (Katzenstein 1996b, 5; Finnemore

1996a, 22; and Klotz 1995b cited in Finnemore & Sikkink, 1998, p. 891), this thesis conceptualises "norms" in a similarly broad manner covering behaviours that further organisational objectives such as cyber standards, shared values, principles, best practices and regulatory alignments in regards to cybersecurity. Thus, in the context of NATO, cyber norms can, among other things, refer to the principle of collective cyber defence, the principles and values of the NATO Cyber Defence Pledge, the integration of "cyber" into military operations (including exercises and trainings), commitment to the application of international law in cyberspace, global cooperation and information sharing (see for example NATO, 2022, pp. 6-7, 10; NATO, 2016; NATO, 2023a). Similarly, in the context of the EU, cyber norms may refer to values and principles that guide the Union's approach to cybersecurity and are enshrined in various strategic EU documents. Examples of such norms include: *"existing international law and norms apply in cyberspace"; "rights-based and gender-sensitive by design"; "multi-stakeholder Internet governance model; "open access to the Internet for all"; "shared responsibility approach"; "international cooperation"* (EU CyberNet, 2023, p. 14); *"[s]ustainable, secure, trustworthy technology and internet infrastructure; [o]pen, human-centric digital economy and trade* (ibid, p. 44); *"an Internet that is open, stable, free, inclusive, global, interoperable, reliable, secure, and green (...)"* (ibid, p. 81); cyber resilience through the adoption of the NIS Directive; cyber diplomacy engagements including EU's cyber diplomacy toolbox; advancing responsible state behavior in cyberspace; bolstering global cyber capacities; cyber defence in the context of CSDP; information sharing (European Commission, Directorate-General for Communications Networks, Content and Technology, 2020, pp. 5-6, 16-17, 18-19, 22-23).

3.2. Research Design & Strategy

This thesis uses a qualitative small-n comparative case study approach to examine how the three countries have engaged in international cybersecurity cooperation with NATO and the EU as small non-member states and how that engagement provides them shelter. In contradistinction to quantitative research, qualitative research puts emphasis on words / verbal descriptions than numerical values in the data collection / data analysis process. It is also interpretivist. The qualitative approach is a suitable approach for this study as it allows for a detailed examination of specific cases. (Bryman 2012, pp. 12, 45, 66, 380) In that context, Crandall (2014) notes that *"[w]hen doing a case study, or a series of case studies, we can go into detail and test a theory on a single country"* (p. 34; see also Bryman 2012, p. 74). The theory that will be tested is shelter

theory through the prism of Burton's conceptual framework which allows for a structured analysis. The comparative nature of this study aims to shed light on how Georgia-, Moldova- and Ukraine-EU / NATO engagements provide them shelter as small states. In that way, case specific peculiarities among the countries can be highlighted.

3.3. Case Selection

This sub-section will draw from the insights that are presented in other sections of this thesis unless mentioned otherwise. Georgia, Moldova, and Ukraine share intriguing similarities but also differences that make a comparative study about them relevant and timely. First, as will be discussed in Chapter 4 in more detail, the three states have similar relations with the EU. All three are part of the EaP, have signed Association Agreements, and have been granted candidate status. However, their relations with NATO differ. For example, while Moldova seeks close working relations with the alliance, the country does not aim to become a full member. Moreover, all three have been exposed to severe cyber-attacks in the past that have been attributed to the Russian Federation (National Cyber Security Centre, 2018; Gallagher, 2023; RFE/RL, 2020). In other words, the three states share the same external threat. Furthermore, the changing nature both in terms of geopolitics and cybersecurity makes this study relevant.

3.4. Data Collection & Data Analysis

This research relies on publicly available primary sources as well as secondary ones that were accessible on the Internet at the time of writing. Primary sources in this setting refer to valid strategic documents such as cyber- / information security strategies and their accompanying action- / implementation plans, digital transformation strategies, foreign policies, association agreements / association agendas, national security strategies, military / defence strategies, and other cybersecurity- / NATO- / EU documents. Importantly, highly specific documents such as sectoral or local strategies which, among other things, touch upon cybersecurity cooperation are not considered. Secondary sources in this context encompass official reports and assessments published by reputable sources, press releases and similar third-party accounts. Official English translations of the documents were used whenever available. Where such translation did not exist, the author utilised the translation tool *Google Translate*. In an attempt to avoid potential inaccuracies stemming from non-official translations, statements were cross-checked with other

available official English sources where needed. The data collection process of the primary sources was guided by the principle that the respective documents had to be valid. For the purposes of this thesis, a document has been deemed valid as long as it was available on an official webpage (e.g. ministry's website) and had not been replaced by a succeeding strategy, policy or similar. According to this, a document may have been deemed valid even though the timeframe, as indicated on the document, had expired at the time of writing (e.g. strategy indicates that the implementation period ended in 2022). This is because of the common practice that certain polices and strategies are not immediately succeeded by new ones without temporal interruptions. However, expired documents that were available on official websites for purely archival purposes or were it was evident that they had been replaced/ succeeded by renamed policies/ strategies were not considered.

The data analysis method of this study is framework analysis which enables the researcher to analyse large volumes of qualitative data and ensures flexibility and a structured approach. Framework analysis is based on a five-stage process: 1) familiarisation, 2) the identification of a thematic framework, 3) indexing, 4) charting, 5) mapping and interpretation. (Smith, & Firth, 2011; Furber, 2010; Delve, n.d) Accordingly, after an initial familiarisation stage, the author commenced with a preliminary coding phase in which patters in the data sources were identified and coded. This included assessing strategic documents, reports, agreements and other primary / secondary sources for explicit statements and activities indicating cooperation in the cyber domain with EU/ NATO. From this coding stage, two main categories emerged for both "alliance" (NATO) and "institution" (EU). In other words, the preliminary codes were grouped into two broader categories, namely "strategic alignment" and "regulatory alignment". Key patterns for the category strategic alignment included explicit references to EU / NATO cooperation and the actualisation of such cooperation objectives such as joint exercises, trainings, capacity building initiatives, formal links with EU / NATO entities, dialogue formats, special agreements and cooperation in cyber threat intelligence sharing. Key patterns for the category regulatory alignment included adherence to NATO / EU standards and Directives such as EU's NIS Directive. In regard to Burton's (2013) third frame "norms" (besides "alliance" and "institution") two main categories were identified: "norm reinforcement" and "norm entrepreneurship". These two categories indicate a more active role on the part of the trio as opposed to being merely the recipient of certain NATO-/EU norms as will be demonstrated in the alliance and institution section when it comes to societal shelter. The author will use for both categories the overarching term: norm building activities. The patterns have been conceptualised in the following way: Norm reinforcement refers

to instances where the countries have either (co-)organised conferences or aligned themselves with statements that the EU and / or NATO deem crucial. Norm entrepreneurship refers to instances, where one of the three countries either advocates for potentially new norms as evidenced in strategic documents, draws from its own unique experiences to alter or strengthen existing norms and / or seeks to become a regional leader. Following this, the next important stage was charting. In line with the framework applied for the analysis section – i.e. Burton's (2013) conceptual framework based on alliance, institution, and norms – three matrices were developed that helped the author to compare and contrast the findings. Ultimately, in the mapping and interpretation stage, the charted data was assessed through the lens of shelter theory. Each country's approach to the identified categories – i.e. strategic alignment, regulatory alignment (for alliance / NATO; institution / EU) and norm reinforcement, norm entrepreneurship (for "norms") – was assessed for indications of political, economic, and societal shelter. Throughout the framework analysis, the author adhered to the concept of theoretical saturation as a guiding principle. Theoretical saturation refers to the *"(…) point when emerging concepts have been fully explored and no new theoretical insights are being generated"* (Bryman, 2012, p. 717). In other words, potential new data that was analysed through the prism of established categories.

3.5. Limitations and Challenges

This subsection addresses some of the limitations and challenges inherent in the applied methodology of the thesis. First, as Bryman (2012) notes, that one of the most recurring criticisms of the case study approach is that its results cannot be generalised (p. 71). Although the insights gained from this study might be valuable on its own right, the unique geopolitical realities of these countries suggest that the findings cannot be readily applied to other smaller states. Moreover, because of the rapidly changing geopolitical and cybersecurity environment, the findings may have a provisional character and should be tested again after a certain period of time. Second, even though steps were taken to systematically code and categorise the data, as outlined above, qualitative analysis has the inherent risk that its findings are subjective and biased (Bryman, 2012). The author of this study acknowledges the potential risk of personal biases that might have influenced the findings. To address such potential biases, the author tried to challenge his assumptions and pre-judgements on an ongoing basis. Third, while interviews with key national cybersecurity experts might have given additional insights, their exclusion was a deliberate

decision which relates to the overall secretive nature of the domain. It is questionable whether their inclusion would have given additional insights beyond publicly available information.

4. Background Information

This chapter will provide further context for the ensuing analytical chapter. It does not intend to be exhaustive but seeks to provide background information on the cooperation mechanisms both organisations have with the trio along with some other crucial aspects (key entities, legal instruments etc.).

4.1. NATO

NATO's relations with the trio are driven by the countries' national objectives towards the alliance. Ukraine and Georgia seek to become full members of NATO eventually (National Security and Defense Council of Ukraine, 2020, Section I, no. 6.; Ministry of Defence of Georgia, n.d.-b). These ambitions are reflected in NATO's partnership tools. Both Ukraine and Georgia have so-called Annual National Programmes (ANP) in place. ANPs are cooperation documents that are updated on annual basis and touch upon, among other things, security and defence reforms. ANPs in turn are open to Membership Action Plans (MAP), which are tailored programmes for countries that seek to become part of NATO (NATO, 2023g; NATO, 2023h). However, it should be mentioned that during the summit in Vilnius in 2023, NATO allies decided that *"(…) Ukraine's path to full Euro-Atlantic integration has moved beyond the need for the Membership Action Plan"* (NATO, 2023a, para 11). The Moldovan relations with the alliance are more measured. Because of the country's permanent neutrality, as enshrined in Article 11 of its Constitution, the country does not intend to become a full member of the alliance (see Constitution of the Republic of Moldova, 2022). After the full-scale invasion against Ukraine, Moldova has reiterated its stance regarding potential membership but also stressed that it seeks to strengthen its ties with NATO (RFE/RL, 2022). Its relations with the alliance are marked by the PfP and the Individual Partnership Action Plan (IPAP) (NATO, 2023i). As mentioned earlier int the previous section during NATO's 2014 Summit in Wales allies agreed upon the applicability of international law in cyberspace and also that certain cyber-attacks can trigger Article 5 of the North Atlantic Treaty. It should be noted that the latter has also been re-emphasised by the Secretary General of NATO in 2023 (Clasen, 2023).

NATO's cybersecurity engagements are facilitated through the Cooperative Cyber Defence Centre of Excellence (CCDCOE). The CCDCOE engages in, among other things, cyber defence research and organises annual cybersecurity exercises (CCDCOE, n.d.-d).

4.2. EU

The EU's partner relations with Georgia, Moldova and Ukraine are guided by the European Neighbourhood Policy and its eastern dimension, the Eastern Partnership (EaP). The EaP was established in 2009 and constitutes a joint undertaking in which the EU and its Member States as well as Armenia, Azerbaijan, Belarus (at the time of writing suspended), Georgia, and Moldova and Ukraine collaborate to enhance their political and economic ties. (European Commission, n.d.-b; European External Action Service, 2022a; Council of the European Union, n.d.-a) Georgia, Moldova, and Ukraine have also signed Association Agreements along with Deep and Comprehensive Free Trade Area Agreements (DCFTA) with the EU. These Agreements can serve as basis for the accession process. In June 2022, the EU granted Ukraine and Moldova candidate status while signalling its readiness to give Georgia the same status once certain priorities have been addressed. (Ahamad Madatali & Jansen, 2022, pp. 1-2) In December 2023 Georgia eventually received candidate status (Council of the European Union, n.d.-b) and accession talks were approved for Ukraine and Moldova the same month (DW, 2023). In the field of cybersecurity, the EU is guided by its Cyber Security Strategy for the Digital Decade from December 2020 (European Commission, 2020) and by its Cyber Defence Policy from 2022 (European External Action Service, 2022c). The Union's main agency in the cybersecurity field is the European Agency for Cybersecurity (ENISA) which, among other tasks, cooperates with EU Member States along with other EU bodies and engages in capacity building and awareness raising activities (ENISA, n.d.-a). The EU's engagement in the cyber domain also takes place under the framework of the Common Security and Defence Policy (CSDP). *"The CSDP enables the EU to use civilian, police and military instruments to cover the full spectrum of crisis prevention, crisis management and post-crisis rehabilitation"* (Federal Foreign Office, n.d.). The Permanent Structured Cooperation (PESCO) is a component of the CSDP and serves as a legal framework through which the armed forces of the 26 participating Member States can collaborate in specific areas. The European Defence Agency is associated with PESCO and facilitates these defence cooperation efforts (European Defence Agency, n.d.-a; European Defence Agency, n.d.-b). At the EaP Summit in 2021 it was decided that cooperation in the field of CSDP should be strengthened (European

Parliament, 2022, p. 9). Through PESCO, the EU can retrieve cybersecurity experts from its Member States and assist partner countries in times of crisis upon request (Duguin & Pavlova, 2023, pp. 16-17). Among one of the most important EU legal instruments in the field of cybersecurity is the so-called Network and Information Security Directive (NIS Directive). As will be discussed below, the trio has made efforts to align its national legislation with the NIS Directive. The NIS Directive was first adopted in 2016 and aimed to establish EU-wide rules in the field of cybersecurity and touched upon issues such as the need to develop NCSSs, national CSIRTs, and notification requirements for certain operators that provide essential services (Kert-Saint Aubyn, n.d.). In January 2023, the NIS Directive was updated (henceforth: NIS2) and introduced new sectors and entities that fall under its scope along with numerous other crucial additions and amendments (ENISA, n.d.-b; European Commission, n.d.-c).

5. Analysis

The analysis section is divided up into three bigger sub-sections based on Burton's (2013) framework, namely alliance (5.1.), institution (5.2), and norms (5.3). These subsections are divided into further sub-categories. In the case of alliance (5.1.) and institution (5.2), the author is first going to compare and contrast the various strategic alignment aspects as evidenced in the country's strategies and other documents ("Strategic alignment"). The second subcategory evaluates the goals and objectives of the trio in regard to regulatory alignment ("Regulatory Alignment"). Following this, the findings are analysed through the prism of shelter theory ("Shelter Analysis"). The subsections conclude with a summarised paragraph ("Interim Results"). The subcategories of sub-section 5.3. differ in the sense that focus is put on instances of norm reinforcement ("Norm reinforcement") and then on norm entrepreneurship ("Norm Entrepreneurship"). Apart from this, subsection 5.3. follows the same pattern. i.e. shelter analysis and interim results.

5.1. Alliances

5.1.1. Strategic Alignment

When assessing the National Cyber- / Information Security Strategies of Georgia, Moldova, and Ukraine, and other strategic documents in regard to NATO cooperation in the cyber defence domain, a consistent pattern of strategic alignment with the alliance emerges. In its National Security Strategy from 2020, Ukraine speaks of the goal of a *"special partnership"* with NATO and eventual full membership with the alliance (National Security and Defense Council of Ukraine, 2020, Section I, no. 6.). This special relationship is also addressed in a similar way in Ukraine's current National Cyber Security Strategy (2021) in which emphasis is put on the need for *"(...) the development of strategic relations in the field of cyber security with key foreign partners, primarily with (...) and other NATO member states"* (National Security and Defense Council of Ukraine, 2021, Section 4, para 5; see also Ministry of Foreign Affairs of Ukraine, 2018) Georgia also seeks to deepen its cybersecurity cooperation with NATO as evidenced in the National Cyber Security Strategy of Georgia and its Action Plan (2021-2024) as well as in the Cyber Security Strategy of the Ministry of Defence of Georgia (2021-2024) (Government of Georgia, 2021, "Strength", Goal 4; Cyber Security Bureau, Ministry of Defence of Georgia, 2021,

pp. 14-15). Moldova's Information Security Strategy and its accompanying Action Plan for the years 2019-2024 appear to be more measured when it comes to cyber defence cooperation with the alliance. The strategy itself mentions NATO twice and in the Action Plan just once while referring to establishing links with NATO Centres of Excellence, namely the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and NATO Strategic Communications Centre of Excellence (NATO StratCom COE) (Parliament of the Republic of Moldova, 2018, Annex I, 94, (6); Parliament of the Republic of Moldova, 2018, Annex II, objective 17 no. 6). However, the Action Plan touches upon cyber defence cooperation in a more general manner by calling for the *"[i]ntensification of cooperation with external development partners regarding the exchange of information and experience (...)"* and *"(...) collaboration agreements (mutual assistance) in the field of cyber defence"* (Parliament of the Republic of Moldova, 2018, Annex II no. 25 no. 2-3). This is consistent with Moldova's Action Plan regarding the implementation of the National Strategy of Defense for the years 2018–2022, which among other things, foresees NATO cooperation within the confines of the PfP format (Ministry of Defense of the Republic of Moldova, 2018, Action no. 2.12.3; see also Republic of Moldova, 2018, Action no 1.1.10.2; Parliament of the Republic of Moldova, 2002). However, it should be noted that the 2022-2023 Individual Partnership Action Plan (IPAP), which guides Moldova's cooperation with the alliance, clearly indicates the desire to cooperate with NATO on cyber defence issues, pertaining critical (information) infrastructure protection but also in the fields of cyber defence education, information sharing, exercises and awareness raising activities (Republic of Moldova & NATO, 2022, Action 1.7.1-1.7.2).

Having discussed the more general aspects of strategic alignment, the author will now delve deeper into the practical implementation of certain actions Georgia, Moldova and Ukraine have made to actualise their alignment with the alliance in the field of cyber defence. In the recent past, all three states have participated in NATO supported cyber exercises. For example, Georgia and Ukraine, as partner countries, took part in the 2023 edition of *Cyber Coalition*. Among other focus areas, this exercise centred around cyber-attacks against critical infrastructures. (NATO, 2023b) Moldovan cybersecurity experts have participated in the 2023 edition of *Locked Shields* (National Cyber Security Directorate, 2023). Ukraine and Georgia have also been represented in past editions of the same annual exercise which is organised by the CCDCOE (Stupp, 2022; Agenda.ge, 2022a; CCDCOE, n.d.-a). Both countries also emphasise the need for such exercises in their respective cybersecurity strategies and Action Plans (Government of Georgia, 2021, Action Plan, no 4.2.1.; Cyber Security Bureau, Ministry of Defence of Georgia, 2021, p. 14; National Security and

Defense Council of Ukraine, 2021, Section 6, para 6; National Security and Defense Council of Ukraine, 2022, Objective C.1. no. 5, Objective C3 no 24). Georgia stands out in that context because of the NATO-Georgia Joint Training and Evaluation Center (JTEC) which is a key component of the Substantial NATO-Georgia Package (SNGP), and among several other purposes, offers Georgian Defence Forces (GDF) and other NATO allies and partner countries cyber defence related exercises and trainings under NATO's guidance (NATO, 2015; Ministry of Defence of Georgia, 2021, p. 69; Menabde, 2019). The three countries have benefited from NATO's Science for Peace and Security (SPS) Programme in multiple domains, including cybersecurity. For example, the Programme supported the establishment of a Cyber Defence Research and Education Laboratory at the Technical University of Moldova and another project that enhances cyber defence capacities within the armed forces including the Moldovan Armed Forces Cyber Incident Response Capability (MAFCIRC) (IDC on NATO in Moldova, 2020b; Republic of Moldova & NATO, 2022, pp. 7, 9; NATO Communications and Information Agency, 2021), in Georgia the Georgian Research and Educational Networking Association Computer Emergency Response Team (GRENA CERT-GE) (CERT-GE, n.d.), and in Ukraine a cyber defence training course (Institute for Security and Safety, 2017). When it comes to cooperation with NATO's Centres of Excellence, links have been established in all three cases with the CCDCOE via the cyber exercise *Locked Shields*, as elaborated above. In 2023, Ukraine even became a so-called Contributing Participant of the Centre (CCDCOE, n.d.-b; CCDCOE, n.d.-c). That status has not been granted to Georgia or Moldova at the time of writing. Links have also been established with Hybrid CoE and StratCom COE via the participation of all three countries in the Countering Disinformation War Game in 2022 and 2023 (European Council, 2023, p. 4). Georgia, Moldova, and Ukraine also receive NATO assistance through the Defence Education Enhancement Programme (DEEP) which supports partner countries with the development of capabilities and institution building in military education and aims to identify gaps and needs. Through DEEP, cybersecurity curricula in military educational institutions have been updated. (NATO, 2023c; NATO, 2017b; NATO, 2023d) Also, it is worth highlighting that as part of NATO's SNGP, the Defence Institution Building School was established in 2016 in Georgia and is supported by NATO. The school provides courses on cyber warfare and other cybersecurity related subjects. (NATO, n.d.-b) Cyber threat intelligence sharing between NATO is another crucial component of cybersecurity cooperation with the alliance. In March 2020, the Georgian Cyber Security Bureau of the MoD joined NATO's Malware Information Sharing Platform (MISP) (Ministry of Defence of Georgia, 2020). Since February 2022, i.e. since the full-scale war against Ukraine started, cooperation in cybersecurity matters has markedly increased. NATO augmented its cyber threat intelligence sharing capabilities ever since

(Cerulus, 2022). The Security Service of Ukraine joined the NATO's Platform in 2022 shortly after the full-scale invasion (Security Service of Ukraine, 2022).

5.1.2. Regulatory alignment

Georgia, Moldova, and Ukraine demonstrate a clear commitment to align their internal procedures and regulatory frameworks with NATO standards and best practices to achieve interoperability (Republic of Moldova & NATO, 2022, p. 7, Action 1.7.2; National Security and Defense Council of Ukraine, 2022, Objective C.1., no. 5; National Security and Defense Council of Ukraine, 2021, Section 6, para 6; Law of Ukraine, 2017, Article 8 (6); Cyber Security Bureau, Ministry of Defence of Georgia, 2021, p. 3, 15; Ministry of Defence of Georgia, 2021, p. 64). Besides the already aforementioned various activities (CCBs, trainings, exercise) and programmes (SPS, DEEP) this is assisted through NATO's additional cooperation mechanisms such as the Partnership for Peace Planning and Review Process (PARP), Defence and Related Security Capacity Building Initiative (DCB), Building Integrity Programme (BI), and Interoperability Platform (IP) (NATO, 2023e; NATO, 2023f , NATO, 2021; see also Republic of Moldova & NATO, 2022, pp. 2, 6-7, Action 1.4.1, 2.1.2.).

5.1.3. Shelter analysis

Through strategic- / regulatory alignments, it can be argued that all three states are seeking political shelter under NATO's guidance. The full-scale invasion against Ukraine has accelerated this trend and cooperation in the cyber defence domain has been intensified. Due to the alliance's various support mechanisms (CCBs, trainings and exercises, information sharing, etc.) the trio is receiving political shelter from the organisation. Furthermore, the trio gains access to strategic goods because of this cooperation – both immaterial goods such expertise through knowledge-/ skill transfers and in some cases physical goods (equipment, laboratory, training centre, school, etc.) – which suggests economic sheltering. As a consequence of these various support mechanisms, the three countries arguably have to spend less resources on their own for cyber defence matters. In other words, Georgia, Moldova, and Ukraine may have additional funds available to invest in their national cyber defence capabilities or can allocate funds to other pressing policy objectives. Thus, besides political shelter, all three states are economically sheltered through the assistance measures. Ultimately, as a result of these various cooperation undertakings (e.g. trainings, exercises, etc.), NATO (cyber) values are disseminated to national cyber defence stakeholders and

the respective societies more generally. For example, individuals that may have received NATO supported training or participated in exercises, pass their gained knowledge to other national cybersecurity experts. This suggest that the countries are also indirectly sheltered in the societal domain. This type of shelter is further realised via national Information Centres. The main task of Georgia's NATO-EU Information Centre in Tbilisi is to inform and educate its citizens about NATO and EU activities. This Centre has been engaged in various cyber-security related projects and events in the past (see Agenda.ge, 2016; Information Center on NATO and EU, n.d.; Information Center on NATO and EU, 2022). Similarly, the NATO Information and Documentation Centre (IDC) in Ukraine and the IDC on NATO in Moldova promote the alliance's values and have engaged in cyber-security related activities in the past (see NATO, 2017a; Canadian NATO Parliamentary Association, 2018, para 12-13; IDC on NATO in Moldova, 2015a; IDC on NATO in Moldova, 2020a; IDC on NATO in Moldova, 2015b).

5.1.4. Interim results

When it comes to cybersecurity engagements with NATO, all three states have aligned themselves both strategically and in regulatory aspects with the alliance. As NATO partner countries, cybersecurity cooperation takes place in the shape of NATO-supported exercises, trainings, education activities, Centres of Excellences, information sharing and other CCB activities. Their engagements are influenced by their cooperation statuses with the alliance. The full-scale invasion against Ukraine has also impacted that engagement. To date, Ukraine's cybersecurity cooperation with the alliance appears to be the most mature. When interpreting the examined materials, it can be argued that all three states receive external shelter due to their engagements with the alliance. Expectedly, political shelter constitutes the most dominant form of shelter, however, the trio is also sheltered in economic and societal respects. Economic shelter is achieved through the access to immaterial as well as physical strategic goods. Societal shelter may be accomplished through knowledge transfers and national Information Centres.

5.2. Institutions

5.2.1. Strategic alignment

Georgia, Moldova, and Ukraine demonstrate a clear commitment in their policies and strategies to cybersecurity cooperation with the EU and have strategically aligned themselves with the supranational institution. This paragraph will highlight a selection of that type of alignment. Moldova sees cooperation in its Information Security Strategy as crucial for information sharing and *"(…) the purpose of preventing, detecting and countering hybrid security threats in the information space"* (Parliament of the Republic of Moldova, 2018, Annex II, objective 24 no. 2; see also ibid, Annex I, 101 (2)). Similarly, Ukraine and Georgia in their respective NCSSs and Action Plans regard cybersecurity cooperation with the EU, in addition to several other aspects, as vital for achieving cyber resilience, incident response, information sharing and trainings (National Security and Defense Council of Ukraine, 2021, Section 2, para 7; National Security and Defense Council of Ukraine, 2022, Objective C3 no 24, Goal C.4, no. 33; Government of Georgia, 2021, "Strength", Goal 4, Action Plan, no 4.2.5; Cyber Security Bureau, Ministry of Defence of Georgia, 2021, p. 14). In the course of examining the countries' documents, an intriguing pattern emerged, namely the trio's pronounced desire to engage in enhanced cooperation under EU's CSDP framework. For example, Ukraine's Action Plan of the current NCSS aims to establish permanent links with EU's military CERT (National Security and Defense Council of Ukraine, 2022, Objective C1, no 6). In the Georgian case, besides in the NCSS itself (see Government of Georgia, 2021, "Strength") and the county's Association Agenda with the EU for the period 2021-2027 (EU–Georgia Association Council, 2022, L 218/57), the need for CSDP cooperation in the domain of cyber defence is also addressed in the Strategic Defence Review 2021-2025: *"The MoD will continue cooperation (…) in the frames of the Common Security and Defence Policy (CSDP). This includes (…) deepening cooperation in the field of cybersecurity (…). The MoD will explore additional opportunities (…), including initiation of formal cooperation with EU's relevant agencies (EDA, ENISA) and cooperation mechanisms/programs (PESCO, EPF, SAFE, TAIEX and etc.) (…)"* (Ministry of Defence of Georgia, 2021, p. 81). Moldova, while not specifically referring to cybersecurity, addresses CSDP cooperation as a priority area in its Action Plan of the National Strategy of Defense for the years 2018–2022 (Ministry of Defense of the Republic of Moldova, 2018, Action no. 2.12.2) and similarly in its Action Plan of the Military Strategy, among other documents (see Republic of Moldova, 2018, Action no 1.1.10.1; see also Parliament of the Republic of Moldova, 2011, Section 3, 3.1).

Following this exploration of national strategic goals, the focus will now be placed on how some of these objectives have been achieved in the past. In 2021, the EU and Ukraine launched a new format to discuss cyber resilience and cybersecurity legislation related topics, the UA-EU Cybersecurity Dialogue (EU Neighbours East 2021b). The second edition of that dialogue took place in September 2022 in the context of the ongoing full-scale war against Ukraine (European External Action Service, 2022b). Similar formats but with a broader scope have been established with Moldova (i.e. the EU-Republic of Moldova High-Level Political and Security Dialogue) and Georgia (EU–Georgia Strategic Security Dialogue) (European External Action Service, 2023c; European External Action Service, 2021a). Some noteworthy EU-funded and/ or EU-organised exercises with a cyber component include the *Fourth Regional Cyber Cooperation Exercise* in 2022 held in Istanbul, Türkiye which focused on inter-domain cooperation among cybersecurity experts and criminal justice authorities. Participants from all three countries took part in this EU co-founded exercise. (Council of Europe, n.d.). Also, the EU, through the EU4DigitalUA initiative, and in conjunction with Ukraine's State Service for Special Communications and Information Protection of Ukraine (SSSCIP), organised a cybersecurity exercise titled *CIREX.CYBER.Ransomware* in 2023. The exercise focused on how Ukrainian cities can better prepare and respond to a certain type of cyber-attack, namely ransomware attacks (FIIAPP, 2023). The EU's Advisory Mission to Ukraine also organised a cybersecurity table-top exercise in November 2023 which focused on inter-agency cooperation (EU Advisory Mission Ukraine, 2023). As part of EU's EPF assistance measure, eGA and CybExer Technologies OÜ carried out a three-day live fire cybersecurity exercise for the Moldovan Armed Forces in November 2023. The exercise focused on prevention, detection, and incident response. (eGA, 2023a)

When it comes to CSDP and cyber defence cooperation more generally, then it is worth noting that the EU's EPF projects have been implemented in all three states. Via an EPF, national military actors can receive trainings, exercises, equipment, and IT infrastructure from the EU. For instance, due to EPF, Ukraine has been the beneficiary of a cyber classroom and cyber lab for the Ukrainian Armed Forces. (eGA, 2023b; eGA, n.d.-a; eGA, n.d.-b) Moreover, Ukraine, unlike Georgia and Moldova, has a so-called Administrative Arrangement with EU's European Defence Agency (EDA) through which the country can participate in certain EDA activities (European Defence Agency, 2022, p. 26). On an annual basis, EU-Georgia consultations take place, in which inter alia, cybersecurity cooperation issues under EU's CSDP framework are being discussed with the Georgian MoD (Ministry of Defence of Georgia, n.d.-a). Moreover, as part of EU's SAFE

programme and in partnership with the UN Office for Project Services (UNOPS), the Cyber Security Bureau of the MoD of Georgia received cybersecurity equipment and solutions (hardware and software) worth in the amount of more than 200.000 USD in 2021 (EU Neighbours East, 2021a).

It is crucial to highlight that since the full-scale invasion of the Russian Federation against Ukraine, cybersecurity cooperation between the EU and the trio has been significantly strengthened through numerous additional support mechanisms. Besides the already mentioned EPF projects, for example, via PESCO-funded Cyber Rapid Response Teams that were activated to assist in Ukraine in February 2022 (European Parliament, 2022, p. 14; European Defence Agency, 2023). Such Rapid Response Teams were also activated in Moldova the same year (European Defence Agency, 2023) and according to some accounts, preparations were made for a second deployment in 2023 (Grossman, 2023, p. 31; Bendiek & Bund, 2023, p. 5). From March 2022 until February 2023, the EU funded a project called *EU Support to Strengthen Cyber Security in Ukraine* that had a budget of over 10 million EUR and was implemented by eGA. The project focused, inter alia, on secure public service provisions, the protection of critical infrastructures and provided equipment to Ukrainian state authorities (ERR, 2022; EU4Digital, 2022). ENISA also signed a working arrangement with Ukraine in November 2023, which draws from the previous EU-Ukraine Cybersecurity Dialogue. The arrangement centres around CCBs (exercises, trainings etc.), the distribution of best practices (in particular EU's NIS2 Directive), and situational awareness. (ENISA, 2023b) Shortly after the start of the war, the EU adopted an eight million EUR crisis response measure for Moldova. Among other things, the action of that measure covers the enhancement of cybersecurity infrastructure protection. (Service for Foreign Policy Instruments, 2022) At the request of Moldovan authorities, an EU Partnership Mission with the aim to bolster crisis management structures and to increase cyber resilience was formally established in April 2023. The EU mission seeks to identify gaps for capacity building and offer advice to Moldovan stakeholders. (European External Action Service, 2023b). Ultimately, it should be stressed that inter-organisational cooperation between the EU and NATO has also increased as a consequence of the war. For instance, representatives from both organisations met in September 2023 to discuss future actions in regard to Russian cyber threats and how to intensify cooperation in the areas of cybersecurity. (European External Action Service, 2023a) When it comes to economic assistance, one key aspect to mention is the European Commission's decision in September 2022 to formalise an agreement to integrate Ukraine into the so-called Digital Europe Programme. This Programme gives Ukraine the opportunity to seek financial aid and support for projects in vital areas such as

artificial intelligence, digital skills, supercomputing and so forth. (European Commission, 2022) As per its Digital Transformation Strategy (2023-2030), Moldova perceives the Programme also a potential funding opportunity for its objectives (Government of the Republic of Moldova, Ministry of Economic Development and Digitalization of the Republic of Moldova, & United Nations Development Programme, 2023, p. 41).

5.2.2. Regulatory alignment

The Association Agreements of Georgia, Moldova, and Ukraine with the EU call for the *"gradual approximation"* in various areas of national legislation with EU legislation (see e.g. EU & EAEC, 2023a, Article 55, 75, 87, 103; 126 EU & EAEC, 2023b, Article 230, 240; EU & EAEC, 2023c, Article 84, 337, 442). As elaborated above, one of the most important Directives in the field of cybersecurity within the EU is the NIS Directive, which has been revised recently. All three states aim to align their national legislation in the cybersecurity field with EU best practice and make references to the NIS Directive and EU standards in their strategic documents as can be seen in their Cyber-/ Information Security Strategies and accompanying Action-/ Implementation Plans, but also Association Agendas (see e.g. National Security and Defense Council of Ukraine, 2022, Goal B.3, no. 87; EU–Georgia Association Council, 2022, L 218/48, L 218/72; Cyber Security Bureau, Ministry of Defence of Georgia, 2021, p. 15; Republic of Moldova & NATO, 2022, Action 1.7.1; EU-Republic of Moldova Association Council, 2022, L 273/110, L 273/118, L 273/122; Parliament of the Republic of Moldova, 2018, Annex II, objective 1 no. 5, objective 5 (3), Annex I, 78 (5), 82 (3)). When it comes to the practical implementation of the NIS Directive, Moldova has made strides since 2023. The Moldovan Parliament adopted a new Cybersecurity Law which will enter into force in 2025 and is aligned with the NIS Directive. The drafting process was funded by EU's Rapid Assistance Project. (eGA, 2023c) Georgia has been assisted in a similar manner through EU's Twinning project called Strengthening Cybersecurity Capacities in Georgia (EU for Georgia, n.d; European Commission, n.d.-a) and Ukraine, among other initiatives as the before mentioned working arrangement with ENISA, through EU's EU4Digital initiative. The latter also assisted Georgia and Moldova in its alignment efforts with the Directive (eGA, n.d.-c; EU4Digital, n.d.). In conclusion, the findings demonstrate concerted effort of the trio to align their national regulations with EU standards in the cybersecurity field, in particular with the NIS Directive.

Beyond the NIS alignments efforts of the trio, it is worth mentioning that Ukraine's National Cyber Security Strategy from 2021 specifically mentions that the Strategy has been developed by

considering *"(...) the provisions of the EU Cyber Security Strategy for the Digital Decade, cyber security strategies of individual EU member states and NATO member states"* (National Security and Defense Council of Ukraine, 2021, Section 2, para 14). Moreover, the Strategy's Implementation Plan indicates that Ukraine aims to establish a procedure *"(...) harmonized with the Euro-Atlantic community to the application of sanctions in response to subversive activities in cyberspace (...) the introduction of restrictive measures in the form of economic sanctions, in response to destructive cyber activity"* (National Security and Defense Council of Ukraine, 2022, Goal C.4, no. 31). This suggest that the country is aiming to establish a sanctions regime akin to EU's Council Decision and Regulation pertaining restrictive measures against cyber-attacks threating EU Member States and the EU as a whole. These measures and legal acts have been devised based on EU's so-called Cyber Diplomacy Toolbox (Botek, A, n.d.; Council of the European Union, 2019a; Council of the European Union, 2019b; Council of the European Union, 2017).

5.2.3. Shelter analysis

In line with the previous alliance-focused sub-section, it can be argued that Georgia, Moldova, and Ukraine, are economically sheltered in the cybersecurity domain due to the Union's various CCB initiatives. Such initiatives give the trio access to physical (e.g. equipment, cyber lab etc.) as well as immaterial strategic goods (e.g. knowledge transfers through exercises and trainings). As a result, the three countries are not just recipients of state-of-the-art EU cyber expertise but are also put in a position where they can allocate domestic funds for additional national cybersecurity efforts or have more leeway in their national budgets for other urgent policy objectives. Moreover, Ukraine gains enhanced economic shelter through its access to the Digital Europe Programme. By harmonising national legislation with EU's NIS Directive, the trio not just demonstrates a clear commitment to EU's cybersecurity standards but also creates a more secure economic environment for the private sector and the society as a whole. For example, a significant portion, and in some cases the majority of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) is privately owned (Edwards, 2017; Bovis, 2015; Dugulin, 2015; Anglmayer, 2021, p. 3). The NIS Directive imposes certain cybersecurity measures that such entities need to comply with. The countries benefit significantly from cybersecurity cooperation with the EU, as numerous EU-funded projects also assist them in these harmonisation efforts. In line with the Association Agreements and the Deep and Comprehensive Free Trade Areas (DCFTA), national NIS harmonisation efforts are a sign of the trio's integration ambitions with the EU. Also, as regulatory

alignments with EU acquis and various other strategic activities (trainings, exercises etc.) ensure the dissemination of ideas (e.g. EU cyber norms) to a broader constituency, the trio is also sheltered in the societal sphere. The strategic alignment under CSDP's framework suggests that the EU is not just perceived as an entity through which Georgia, Moldova and Ukraine can receive shelter in the economic and societal spheres but also in the political one. In other words, despite the fact that the EU, as of today, does not constitute a military alliance (for example the EU treaties do not foresee similar security guarantees as NATO's collective defence clause which, under certain circumstances, can trigger Article 5 in the event of a severe cyber-attack), it is nevertheless perceived as a stabilising force in the cybersecurity realm through which the countries' MoDs and national armed forces can benefit from.

5.2.4. Interim results

When it comes to cybersecurity engagements with the EU, all three states have aligned themselves in strategic as well in regulatory aspects with the Union. Akin to the trio's engagement with NATO, cybersecurity cooperation with the EU also takes place through EU-assisted exercises, trainings, information sharing and CCB initiatives but also through established dialogue formats and the CSDP framework. The full-scale war against Ukraine has significantly intensified this engagement. This has also true for joint EU-NATO cooperation mechanisms. Just as with NATO's engagement, Ukraine's cooperation in the cybersecurity domain with the EU appears to have reached a more mature stage. When interpreting the analysed materials, it is possible to assert that the trio receives external shelter from the EU in all three shelter domains. The dominant shelter here appears to be economic shelter. As with NATO, economic shelter with the Union is achieved through the provisions of strategic goods but also via favourable funding opportunities in the digital realm, as with the Digital Europe Programme in the case of Ukraine. Interestingly, while the EU does not constitute a military alliance, the three EaP countries nevertheless perceive the EU as a stabilising factor also in the (military) cyber defence domain, primarily through the framework of CSDP. This suggest that the countries are also politically sheltered. Societal shelter is also achieved here through various CCB initiatives and similar undertakings that allow for the spread of EU cyber norms to a broader constituency.

5.3. Norms

In the previous two sub-sections the author has discussed how Georgia, Moldova and Ukraine cooperate with the EU and NATO in the cybersecurity domain below the threshold of full membership and how this engagement indicates that the three countries are sheltered. As a consequence of the various cybersecurity engagements, the countries are also NATO-/ EU (cyber) norm recipients. This has been partly reflected in the "interim results" sub-sections regarding societal shelter. However, besides being passive recipients of cyber norms, this section suggest that the trio also plays a more active role in NATO-/ EU cyber norm promotion. Both "norm reinforcement" as well as "norm entrepreneurship", as discussed in the Research Methods section of this thesis, can be seen as a display of the trio's enhanced commitment to the cybersecurity values and objectives of both organisations.

5.3.1. Norm Reinforcement

Georgia, Moldova, and Ukraine have all organised regional- / international forums on cybersecurity. Such conferences and similar meetings usually gather key cybersecurity stakeholders from all sectors to elaborate on legal, political, technical, and educational issues (Neuneck, 2013, p. 92). Since 2020, Georgia hosts the government-backed annual "Georgian Cybersecurity Forum" (Government of Georgia, 2021, "strength", para 16). In the edition of 2022, the Georgian Minister of Defence called for the dissemination of EU and NATO best practices and positioned the country as *"part of the European security architecture"* (Agenda.ge, 2022b). In the 2023 iteration, both the Georgian Prime Minister as well as the Georgian Minister of Internal Affairs acknowledged the good working relationships with Georgia's *"strategic partners"*, including NATO and the EU in its effort to increase the country's cybersecurity capacities (Agenda.ge, 2023; National Security Council of Georgia, 2023). The Prime Minister also highlighted the infrastructure and technological connections that are being developed with Europe with the goal to position the country as a digital hub. The key themes of the 2023 edition centred around CCBs, the difficulties in achieving cyber resilience, cyber diplomacy, and international collaboration (National Security Council of Georgia, 2023). In November 2023, the EU-sponsored "Regional Cybersecurity Symposium" took place in Moldova. The Symposium covered various topics, including how to strengthen cybersecurity and resilience in the region; cybersecurity cooperation in the region; how governments can balance cybersecurity and individual freedoms; and *"[b]uilding cyber resilience: the prism of the EU normative"* (Regional Cybersecurity

Symposium, 2023; eGA, 2023d). Previously, Moldova held similar annual conferences under the title "Cyber Week" (EU4Digital, 2020). Ukraine has also hosted an annual cybersecurity forum titled "International Forum on Cyber Security" until 2021. While the focus of the 2021 edition, in which the EU has been represented as a partner through the EU Advisory Mission to Ukraine, was predominantly on cybercrime, past editions have touched upon broader cyber issues such as cybersecurity of the state, protection of systems and technologies, secure business activities in times of COVID-19 and cybersecurity culture (Prosecutor General's Office of Ukraine, 2021; International Information Academy, 2020). It should be noted that "Kyiv's Security Forum", which constitutes a platform for the exchange of ideas about the most urgent security issues in Europe and the Black Sea Region and in which one of the facilitating partners is NATO's Information and Documentation Centre (NIDC), has also touched upon hybrid threats and cybersecurity issues in past editions (Open Ukraine Foundation, 2023; Open Ukraine Foundation, 2016). The themes covered in the conferences as well statements made by governmental officials suggest that both EU and NATO cyber norms are reinforced in all three cases to a broader constituency that transcend national borders (e.g. cooperation; EU / NATO best practices; CCB; open digital economy; secure and trustworthy technology and internet infrastructure etc.). Another avenue through which the trio is reinforcing norms that the EU (but also NATO) deem crucial, are alignments with EU statements in regard to the applicability of international law in cyberspace. Such statements are regularly made on behalf of the EU towards the United Nations Open-Ended Working Group. Georgia, Moldova, and Ukraine have aligned themselves with these statements in the past (e.g. European External Action Service, 2023d; Delegation to the UN in New York, 2023; European External Action Service, 2021b; European External Action Service, 2021c).

5.3.2. Norm Entrepreneurship

The analysed materials also reveal instances that go beyond mere norm reinforcement and indicate an even more active form of norm promotion, namely norm entrepreneurship. For instance, in its Information Security Strategy and Action Plan, Moldova aims to prohibit the use of "information weapons". The Strategy sees these types of weapons *"(…) as an essential component of hybrid threats, [that] is used by subversive external centres (special services, NGOs guided by state and non-state actors, controllable media institutions, etc.) in the implementation of informational operations or cyber attacks subordinated to a certain strategic goal"* (Parliament of the Republic of Moldova, 2018, Annex I, 59). Consequently, Moldova aims to promote at an international stage the need to reach a consensus regarding the concept of "information weapons" with the

overarching objective to forbid *"(...) its development, dissemination and application in relations between states"* (Parliament of the Republic of Moldova, 2018, Annex I, 101 (3), Annex II Objective 24 (3)). Based on this evidence, and in line with Finnemore & Sikkink's (1998) concept of norm life cycles, it can be argued that Moldova is trying to convince a substantial number of states to support the new norm (prohibition of information weapons) and therefore be situated in the first stage of the norm life cycle, i.e. norm emergence. Because of the already established close working relationships with both the EU and NATO in the cybersecurity domain as evidenced in the two previous sub-sections, the country arguably will also try to reach a consensus with EU and NATO states. Ukraine's Foreign Policy from 2021 states that the country's unique experiences in combatting disinformation and cyber-attacks make cooperation with the EU *"(...) mutually beneficial"* (President of Ukraine, 2021, para 86). The Policy further mentions that cooperation in the fields cybersecurity as well as countering Russian disinformation and propaganda in the EaP region should be intensified (President of Ukraine, 2021, para 87). Such a mutually beneficial relationship has also been recognised by the Director of NATO's CCDCOE at that time, when the decision was made to accept Ukraine as a Contributing Participant to the Center of Excellence: *"(...) Ukraine could bring valuable first-hand knowledge of several adversaries within the cyber domain to be used for research, exercises and training,"* (CCDCOE, n.d.-c). Similarly, the Estonian Minister of Defence during that same period stated: *"Capability and knowledge comes from experience, and Ukraine definitely has valuable experience from previous cyber-attacks to provide significant value to the NATO CCDCOE"* (ibid). By prioritising a set of foreign policy goals along with the country's unique first-hand experiences on the cyber "battlefield", Ukraine positions itself as a cyber norm entrepreneur. Ukraine's exclusive insights contribute to the strengthening of the existing EU/-NATO cyber norms but at the same time might also create new or adjusted norms. These in turn would have to be adopted by a substantial number of EU-/NATO states to reach the second stage of the norm cycle. A similar positioning can be observed in the Georgian case. As per Georgia's NCSS, the Georgian Cybersecurity Forum is perceived as a *"(...) high-level event (...)"* with the objective to *"(...) serve as a platform for sharing ideas regarding the challenges and opportunities facing the country (and the Black Sea region) in cyberspace"* (Government of Georgia, 2021, sub-section strength, para 16) This is in line with Georgia's ambitions of becoming a *"regional leader"* in the cyber domain (Government of Georgia, 2021, Goal 4). In 2022, the Georgian Minister of Defence also stressed the regional importance of the Forum and the desire to expand it with the assistance of the EU and NATO. (Agenda.ge, 2022b). This suggest that Georgia has internalised EU/NATO cyber norms and intends to play a more active role in the dissemination of these by taking into account national experiences.

5.3.3. Shelter Analysis

Both "norm reinforcement" as well as "norm entrepreneurship" can be construed as strong political messages towards the EU and NATO and serve as an avenue through which the trio can maintain and strengthen its ties with both organisations. Moreover, it can be argued that supporting EU-/ NATO cyber norms are in the trio's inherent national interests. The three states have been exposed to malicious cyber activities attributed to the Russian Federation in the past. The EU and NATO have previously signalled their support to all three states after such crisis situations. For example, the EU condemned malicious cyber activities, attributed to Russia, shortly after the full-scale war began and assured Ukraine its support (European Union Council, 2022a; European Union Council, 2022b). Similar assurances have been made towards Moldova by the President of the European Council (European External Action Service, 2023e) as well as through a resolution by the European Parliament in 2023 (European Parliament, 2023). The EU has also condemned the cyber-attacks against Georgia in 2019 and signalled its support to the country (European Union Council, 2020). Similarly, NATO has condemned cyber hostilities attributed to Russia and has signalled its continued support for the trio in its Vilnius Summit Communique of 2023 (NATO, 2023a, para 18, 66, 80-81, 88). By demonstrating political will in regard to cyber norms that the EU and NATO consider important, the trio can arguably expect enhanced assistance in times of crisis as has been the case in the aftermath of the full-scale invasion against Ukraine, in which particularly Ukraine, but also Moldova benefited from considerable support measures in the cybersecurity domain. This is in line with shelter theory, according to which shelters are important for small states to mitigate risks before crises materialise, and equally importantly, during and after such crisis situations. In other words, by organising cybersecurity-related conferences, aligning with EU statements, developing cyber norms, and / or potentially adjusting existing EU-/ NATO norms, the three countries are leveraging diplomatic means to further their own national interest in the context of EU-/ NATO engagement. In this way, norm reinforcement and norm entrepreneurship amplify primarily their political shelter vis-à-vis the EU and NATO, however, potentially also their economic and societal shelter.

5.3.4. Interim Results

Norm reinforcement and norm entrepreneurship are diplomatic efforts that aim to solidify the trio's EU and NATO engagement in the cybersecurity domain. EU-/ NATO cooperation here is marked

by the inclusion of both organisations in cybersecurity conferences, the propagation of EU-NATO norms in these conferences, through alignment statements, as well as norm entrepreneurship activities such as advocacy for certain cyber norms that correspond with the values of both organisations. Georgia, Moldova, and Ukraine ensure through these activities continued political shelter from both the EU and NATO.

6. Conclusion

The author of this thesis has scrutinised how Georgia, Moldova and Ukraine cooperate with NATO and the EU as partner states below the threshold of full membership in the cybersecurity domain and how this engagement provides them shelter as small states. Cooperation among the trio and the alliance is accomplished through strategic alignment efforts such as NATO-supported exercises, trainings, educational activities, Centres of Excellences, information sharing, other support mechanisms as well as regulatory alignment. Similarly, cooperation on cybersecurity issues with the EU is also achieved via EU-assisted exercises and trainings, information sharing mechanisms, CCB initiatives as well as established EU dialogue formats and regulatory alignment. It is worth highlighting that cooperation through the CSDP framework is perceived as a priority area by the trio. Indirect forms of cooperation include EU-supported conferences as well as alignment statements and other norm building activities. The findings further indicate that cybersecurity cooperation has been intensified since the full-scale war against Ukraine began in February 2022. This is also true for inter-organisational cooperation between the EU and NATO. The study also implies that Ukraine's engagement with both organisations appears to have reached a more mature level when compared with the two other countries.

The findings of this thesis suggest that Georgia, Moldova, and Ukraine are also sheltered as a result of their engagements. They receive predominantly political shelter from NATO through the alliance's various support mechanisms (CCBs, trainings and exercises, information sharing etc.). However, it can be argued that as a result of such support initiatives, they are also economically sheltered as they receive access to both material as well as immaterial goods of strategic value. Moreover, societal shelter may be assured via knowledge transfers and national Information Centres. The dominant shelter category in the case of EU cybersecurity cooperation is economic shelter. As with NATO's engagement, the countries receive goods of strategic value as a result of their engagements; besides physical goods (e.g. equipment, cyber lab), also immaterial goods such as expertise in their regulatory alignment efforts with the NIS Directive. Strategic alignment under CSDP's framework demonstrates that the EU is also perceived as an entity through which the

countries can be politically sheltered. In line with the findings for NATO, the EU provides also societal shelter for the three EaP countries as regulatory and strategic alignment efforts ensure the spread of ideas and people to a broader constituency. Finally, norm building activities, which were conceptualised by the author as norm reinforcement and norm entrepreneurship activities, can be construed as an avenue through which the countries receive primarily political shelter.

The combination of small state studies and cybersecurity issues to date is markedly understudied. This gives researchers ample opportunities for further research avenues. The author will highlight just a selection of potential research areas by considering the context of this study. First, cybersecurity engagements and potential sheltering aspects of other small states could be an intriguing avenue for future research. The results of such studies could either solidify the findings of this study or complement them. This could include other small states with similarly close ties to both the EU and NATO below the threshold of full organisational membership or a combination thereof, i.e. states that are EU-/ NATO members and non-member states. Second, another potential research approach could be to broaden the overall scope of the study by incorporating additional international organisations with a cybersecurity mandate such as the OSCE, CoE, other regional organisations and the UN. This would allow for an even more comprehensive analysis of the cooperation aspects of small states in regard to international organisations and potentially give insights how these states are sheltered by other organisations. Third, further diversification of the scope could also include other closely related cybersecurity phenomena such as cybercrime and cross-border law enforcement cooperation. Ultimately, it is crucial to re-emphasise that the findings of this thesis might have a provisional character and potentially become dated in the medium-term. This has to do with the rapidly changing nature of the cyber field as well as geopolitical aspects that shape the trio's relations vis-à-vis the EU and NATO. It could be beneficial to revisit this research topic with a similar design and similar research questions after a certain period of time. For example, when one of three countries or all of them have joined the EU and/ or when either Ukraine and/ or Georgia have been potentially granted NATO membership or when the cybersecurity strategies of all three have been updated. This could give further insights on how the cybersecurity cooperation with both organisations has changed over time and whether certain aspects of sheltering have been reinforced.

LIST OF REFERENCES

Adamson, L., & Homburger, Z. (2019). Let them roar: small states as cyber norm entrepreneurs. European Foreign Affairs Review, 24(2), 217-234. https://doi.org/10.54648/eerr2019014

Agenda.ge. (2016, September 8). New NATO-EU Information Centre opens in Tbilisi. Agenda.ge. Retrieved December 4, 2023, from: https://agenda.ge/en/news/2016/2101

Agenda.ge. (2022a, April 26). Georgian Cyber Security Bureau earns third spot in NATO exercise. Retrieved December 4, 2023, from: https://agenda.ge/en/news/2022/1437

Agenda.ge. (2022b, October 17). Georgian defence minister says Georgia sharing "best EU, NATO practices" in cybersecurity at opening of int'l forum. Retrieved December 9, 2023, from: https://agenda.ge/en/news/2022/4034

Agenda.ge. (2023, June 21). Georgian PM highlights Gov't's "significant" results in developing cybersecurity. Retrieved December 9, 2023, from: https://agenda.ge/en/news/2023/2414

Ahamad Madatali, H., & Jansen, T. (2022). Peace and Security in 2022: EU Association Agreements with Georgia, Moldova, and Ukraine – The roads to EU membership. European Parliamentary Research Service, Ex-Post Evaluation Unit, PE 730.340. European Parliament. Retrieved December 10, 2023, from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/730340/EPRS_IDA(2022)730340_EN.pdf

Anglmayer, I. (2021, February). European critical infrastructure: Revision of Directive 2008/114/EC. European Parliamentary Research Service. PE 662.604. Retrieved December 9, 2023, from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

Årnes, A. (2022). Introduction. In A. Årnes (Ed.), *Cyber Investigations* (1st ed.). John Wiley & Sons Ltd.

Bailes, A. J. K., Thayer, B. A., & Thorhallsson, B. (2016). Alliance theory and alliance 'Shelter': the complexities of small state alliance behaviour. Third World Thematics A TWQ Journal, 1(1), 9–26. https://doi.org/10.1080/23802014.2016.1189806

Baldacchino, G., & Wivel, A. (2020). Small states: concepts and theories. In G. Baldacchino & A. Wivel (Eds.), *Handbook on the Politics of Small States* (pp. 2–19). Edward Elgar Publishing. https://doi.org/10.4337/9781788112932

Bendiek, A., & Bund, J. (2023, September 25). Shifting Paradigms in Europe's Approach to Cyber Defence. Stiftung Wissenschaft und Politik (SWP). Retrieved from: https://www.swp-berlin.org/publikation/shifting-paradigms-in-europes-approach-to-cyber-defence

Bladaitė, N., & Šešelgytė, M. (2020). Building a Multiple 'Security Shelter' in the Baltic States after EU and NATO Accession. Europe-Asia Studies, 72(6), 1010–1032. https://doi.org/10.1080/09668136.2020.1785396

Botek, A. (n.d.). European Union establishes a sanction regime for cyber-attacks. CCDCOE. Retrieved December 9, 2023, from: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/

Bovis, C. (2015). Risk in Public-Private Partnerships and Critical Infrastructure. European Journal of Risk Regulation, 6(2), 200-207. doi:10.1017/S1867299X00004505

Brady, A.-M., & Thorhallsson, B. (2021). Small States and the Turning Point in Global Politics. In A.-M. Brady & B. Thorhallsson (Eds.), *Small States and the New Security Environment* (pp. 1-11). Springer. https://doi.org/10.1007/978-3-030-51529-4

Bryman, A. (2012). *Social Research Methods*, 4th Edition (4th ed.). Oxford University Press.

Burton, J. W. (2013). Small states and cyber security. *Political Science*, *65*(2), 216–238. https://doi.org/10.1177/0032318713508491

Całus, K. (2023). The Russian hybrid threat toolbox in Moldova: Economic, political and social dimensions (Hybrid CoE Working Paper 23). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-23-the-russian-hybrid-threat-toolbox-in-moldova-economic-political-and-social-dimensions/

Canadian NATO Parliamentary Association. (2018). Report of the Canadian NATO Parliamentary Association respecting its participation in the Ukraine-NATO Interparliamentary Council (UNIC), the Sub-Committee on transition and development (ESCTD) and the Sub-Committee on NATO Partnerships (PCNP). Odesa, Ukraine. Retrieved from https://www.parl.ca/Content/Diplomacy/Publications/Visits/9959548/Report/VR(9761935)-E.PDF

CCDCOE. (n.d.-a). Locked Shields. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved December 5, 2023, from: https://ccdcoe.org/exercises/locked-shields/

CCDCOE. (n.d.-b). The NATO CCDCOE welcomes new members Iceland, Ireland, Japan, and Ukraine. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved December 5, 2023, from: https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/

CCDCOE. (n.d.-c). Ukraine to be accepted as a Contributing Participant to NATO CCDCOE. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved December 5, 2023, from: https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/

CCDCOE. (n.d.-d). About us. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved December 5, 2023, from: https://ccdcoe.org/about-us/

CERT-GE. (n.d.). About Us. Retrieved December 12, 2023, from: https://cert.ge/eng/about

Cerulus, L. (2022, March 24). NATO steps up intelligence-sharing 'in preparation' for Russian cyberattacks. POLITICO. Retrieved December 5, 2023, from: https://www.politico.eu/article/nato-steps-up-intelligence-sharing-in-preparation-of-russian-cyberattacks/

Clasen, A. (2023, November 13). New NATO cyber forum to support collective response to cyberattacks. EURACTIV. Retrieved December 12, 2023, from: https://www.euractiv.com/section/cybersecurity/news/nato-defence-can-be-sparked-by-digital-strikes-stoltenberg-tells-berlin-summit/

Constitution of the Republic of Moldova. (2022). Constitutional Court. Retrieved from: https://presedinte.md/eng/constitutia-republicii-moldova

NCS Guide. (2021). The guide to developing a national cybersecurity strategy. Retrieved September 30, 2023, from https://ncsguide.org/the-guide/

Council of Europe. (n.d.). CYBEREAST: Fourth Regional Cyber Cooperation Exercise. Retrieved December 5, 2023, from: https://www.coe.int/en/web/cybercrime/-/cybereast-fourth-regional-cyber-cooperation-exercise

Council of the European Union. (2017, June 19). Cyber attacks: EU ready to respond with a range of measures, including sanctions. Consilium of the European Union. Retrieved December 9, 2023, from https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Council of the European Union. (2019a). Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. EUR-Lex. Retrieved December 9, 2023, from https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797

Council of the European Union. (2019b). Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union. Retrieved December 9, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:129I:TOC

Council of the European Union. (n.d.-a). EU relations with Belarus. Retrieved December 9, 2023, from: https://www.consilium.europa.eu/en/policies/eastern-partnership/belarus/

Council of the European Union. (n.d.-b). Georgia. Retrieved December 18, 2023, from: https://www.consilium.europa.eu/en/policies/enlargement/georgia/

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies*, *14*(1), 30–55. https://doi.org/10.1080/14702436.2014.890334

Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary Security Policy*, 36(2), 346–368. https://doi.org/10.1080/13523260.2015.1061765

Cyber Operations Tracker. (n.d.). Council on Foreign Relations. Retrieved October 14, 2023, from: https://www.cfr.org/cyber-operations/

Cyber Security Bureau, Ministry of Defence of Georgia. (2021). *Cyber Security Strategy of the Ministry of Defence of Georgia 2021-2024*. Retrieved from https://mod.gov.ge/en/page/134/cyber-security-strategy-of-the-ministry-of-defence-of-georgia

Delegation to the UN in New York. (2023, March 8). EU Statement – UN Open-Ended Working Group on ICT: International Law. European External Action Service. Retrieved December 9, 2023: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-international-law-0_en?s=63

Delve. (n.d.). Understanding Framework Analysis: An Introductory Guide. Retrieved from December 9, 2023, from: https://delvetool.com/blog/frameworkanalysis.

Denning, D. E. (2015). Rethinking the Cyber Domain and Deterrence. Joint Forces Quarterly, 77(2), 8–15. Retrieved September 27 , 2023, from https://nsarchive.gwu.edu/sites/default/files/documents/4367805/Dorothy-Denning-Joint-Force-Quarterly-Rethinking.pdf

Domingo, F.C. (2022). Making Sense of Cyber Capabilities for Small States: Case Studies from the Asia-Pacific (1st ed.). Routledge. https://doi.org/10.4324/9781003208679

Duguin, S., & Pavlova, P. (2023, September). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament, SEDE Subcommittee. PE 702.594. Retrieved December 15, 2023, from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

Dugulin, R. (2015, May 17). The private sector's vital role in the protection of critical infrastructure. Global Risk Insights. Retrieved December 9, 2023, from https://globalriskinsights.com/2015/05/the-private-sectors-vital-role-in-the-protection-of-critical-infrastructure/

DW. (2023, December 14). EU approves Ukraine and Moldova accession talks. Retrieved December 17, 2023, from: https://www.dw.com/en/eu-approves-ukraine-and-moldova-accession-talks/live-67717211

Edwards, C. (2017, June 1). Who Owns U.S. Infrastructure? Cato Institute. Retrieved December 9, 2023, from https://www.cato.org/tax-budget-bulletin/who-owns-us-infrastructure

eGA. (2023a, November 16). EGA and CybExer conducted live fire cybersecurity exercise for the Moldova's Ministry of Defence. Retrieved December 8, 2023, from: https://ega.ee/news/cyber-exercise-moldova-ministry-defence/

eGA. (2023b, October 3). Opening of a cyber classroom for the Ukrainian Armed Forces. e-Governance Academy. Retrieved December 8, 2023, from: https://ega.ee/news/cyber-classroom-ukrainian-armed-forces/

eGA. (2023c, May 15). Moldova adopted the EU-backed Cybersecurity Law with the assistance of Estonian experts. e-Governance Academy. Retrieved December 8, 2023, from: https://ega.ee/news/moldova-cybersecurity-law/

eGA. (2023d, November 14). eGA co-hosted the Regional Cybersecurity Symposium in Moldova. Retrieved December 9, 2023, from: https://ega.ee/news/regional-cybersecurity-symposium-moldova/

eGA. (n.d.-a). European Peace Facility Assistance on Cyber Defence in Georgia. e-Governance Academy. Retrieved December 9, 2023, from https://ega.ee/project/enhancing-georgia-cyber-defence/

eGA. (n.d.-b). European Peace Facility Assistance on Cyber Defence in Moldova. e-Governance Academy. Retrieved December 9, 2023, from: https://ega.ee/project/european-peace-facility-moldova/

eGA. (n.d.-c). EU4Digital: Improving Cyber Resilience in the EaP Countries. e-Governance Academy. Retrieved December 9, 2023, from https://ega.ee/project/eu4digital-improving-cyber-resilience-eap-countries/

ENISA. (2023a, October 19). ENISA Threat Landscape 2023. Retrieved December 8, 2023, from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2023b, November 13). Enhanced EU-Ukraine cooperation in Cybersecurity. ENISA. Retrieved December 8, 2023, from: https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity

ENISA. (n.d.-a). About ENISA - The European Union Agency for Cybersecurity. Retrieved December 12, 2023, from: https://www.enisa.europa.eu/about-enisa

ENISA. (n.d.-b). NIS Directive. Retrieved December 12, 2023, from: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

ERR. (2022, October 21). Estonia leading EU project to secure Ukraine's cyber, data security. Retrieved December 8, 2023, from: https://news.err.ee/1608760573/estonia-leading-eu-project-to-secure-ukraine-s-cyber-data-security

EU & EAEC. (2023a, March 6). Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014A0830(02)-20230306

EU & EAEC. (2023b, October 6). Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the

Republic of Moldova, of the other part. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014A0830(01)-20231006

EU & EAEC. (2023c, April 24). Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014A0529(01)-20230424

EU Advisory Mission Ukraine. (2023, November 30). Building resilience to fence the evolving cyber threats. Retrieved December 8, 2023, from: https://www.euam-ukraine.eu/news/building-resilience-to-fence-the-evolving-cyber-threats/

EU CyberNet. (2023). *Operational guidance: The EU's international cooperation on cyber capacity building.* Service for Foreign Policy Instruments, European Commission. Joon OÜ Printing House. Retrieved from https://www.eucybernet.eu/operational-guidance/

EU for Georgia. (n.d.). Strengthening Cybersecurity Capacities in Georgia. EU for Georgia. Retrieved December 9, 2023, from https://eu4georgia.eu/projects/eu-project-page/?id=1458

EU Neighbours East. (2021a, July 8). EU enhances cybersecurity in Georgia providing new integrated cyber security solution. Retrieved December 8, 2023, from: https://euneighbourseast.eu/news/latest-news/eu-enhances-cybersecurity-in-georgia-providing-new-integrated-cyber-security-solution/

EU Neighbours East. (2021b, June 8). Cyberspace: EU and Ukraine launch dialogue on cyber security. Retrieved December 8, 2023, from: https://euneighbourseast.eu/news/latest-news/cyberspace-eu-and-ukraine-launch-dialogue-on-cyber-security/

EU4Digital. (2020). Moldova Cyber Week 2020. Retrieved December 9, 2023, from: https://eufordigital.eu/moldova-cyber-week-2020/

EU4Digital. (2022, October 21). EU supports cybersecurity in Ukraine with over €10 million. Retrieved December 8, 2023, from: https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/

EU4Digital. (n.d.). Ukraine - EU4Digital. Retrieved December 9, 2023, from https://eufordigital.eu/countries/ukraine/

EU–Georgia Association Council. (2022). *Recommendation No 1/2022 of the EU-Georgia Association Council of 16 August 2022 on the EU-Georgia Association Agenda 2021-2027 [2022/1422]*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2022.218.01.0040.01.ENG

EU-Republic of Moldova Association Council. (2022). *Recommendation No 1/2022 of the EU-Republic of Moldova Association Council of 22 August 2022 on the EU-Republic of Moldova Association Agenda [2022/1997]*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22022D1997

European Commission, Directorate-General for Communications Networks, Content and Technology, (2020). *The EU's cybersecurity strategy for the digital decade*, Publications Office. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

European Commission. (2020, December 16). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Retrieved December 10, 2023, from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Commission. (2022, September 5). Solidarity with Ukraine: Digital Europe Programme open to Ukraine for access to calls for funding. European Commission. Retrieved December 8, 2023, from: https://digital-strategy.ec.europa.eu/en/news/solidarity-ukraine-digital-europe-programme-open-ukraine-access-calls-funding

European Commission. (n.d.-a). Annex C1: Twinning Fiche - Strengthening Cybersecurity Capacities in Georgia. Beneficiary administration: LEPL Data Exchange Agency, Ministry of Justice of Georgia. Twinning Reference: GE 18 ENI JH 01 20. Publication notice reference: EuropeAid/168-164/ACT/GE. Retrieved December 9, 2023, from: https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150

European Commission. (n.d.-b). European Neighbourhood Policy. Directorate-General for Neighbourhood and Enlargement Negotiations. Retrieved December 9, 2023, from: https://neighbourhood-enlargement.ec.europa.eu/european-neighbourhood-policy_en

European Commission. (n.d.-c). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Retrieved December 12, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Council. (2023). Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017. Retrieved December 9, 2023, from: https://www.consilium.europa.eu/media/65080/230616-progress-report-nr8-eu-nato.pdf

European Defence Agency. (2022). *EDA annual report 2021*. https://eda.europa.eu/docs/default-source/brochures/eda-annual-report-2021.pdf

European Defence Agency. (2023, July 11). PESCO projects adapt and accelerate amid shifting European security landscape, EU report finds. Retrieved December 8, 2023, from: https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds

European Defence Agency. (n.d.-a). Permanent Structured Cooperation (PESCO). Retrieved December 15, 2023 from: https://eda.europa.eu/what-we-do/EU-defence-initiatives/permanent-structured-cooperation-(PESCO)

European Defence Agency. (n.d.-b). Mission. Retrieved December 15, 2023, from: https://eda.europa.eu/who-we-are/Missionandfunctions

European External Action Service. (2021a, November 26). European Union and Georgia hold their fourth Strategic Security Dialogue. EEAS. Retrieved December 8, 2023, from:

https://www.eeas.europa.eu/delegations/georgia/european-union-and-georgia-hold-their-fourth-strategic-security-dialogue_en?s=221

European External Action Service. (2021b, December 13). EU Statement – United Nations Open-Ended Working Group on ICT: General exchange of views. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-united-nations-open-ended-working-group-ict-general-exchange-views_en

European External Action Service. (2021c, December 15). EU Statement – United Nations Open-Ended Working Group on ICT: International Law. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-united-nations-open-ended-working-group-ict-international-law_en

European External Action Service. (2022a, March 17). Eastern Partnership. Retrieved December 9, 2023, from https://www.eeas.europa.eu/eeas/eastern-partnership_en

European External Action Service. (2022b, September 29). Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue. EEAS. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en

European External Action Service. (2022c, November 11). Cyber Defence: EU boosts action against cyber threats. Retrieved December 10, 2023, from https://www.eeas.europa.eu/delegations/montenegro/cyber-defence-eu-boosts-action-against-cyber-threats_en

European External Action Service. (2023a, September 22). The European Union and NATO intensify cooperation in addressing cyber threats. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en#:~:text=To%20strengthen%20cooperation%20and%20intensify,cyber%20security%20and%20cyber%20defence

European External Action Service. (2023b, May 31). About EU Partnership Mission in the Republic of Moldova. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en?s=410318

European External Action Service. (2023c, March 24). Moldova: second High-Level Political and Security Dialogue with the European Union takes place. EEAS. Retrieved December 8, 2023, from: https://www.eeas.europa.eu/eeas/moldova-second-high-level-political-and-security-dialogue-european-union-takes-place_en?s=223

European External Action Service. (2023d, May 25). EU statement – UN Open Ended Working Group on ICTs: regular institutional dialogue. Retrieved December 9, 2023, from: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-icts-regular-institutional-dialogue_en

European External Action Service. (2023e, March 28). The EU stands in full solidarity with the people of Moldova in these challenging times. Retrieved December 9, 2023, from https://www.eeas.europa.eu/node/427637_ru

European Parliament. (2022, May 30). Report on security in the Eastern Partnership area and the role of the common security and defence policy (2021/2199(INI)). Committee on Foreign Affairs. Rapporteur: Witold Jan Waszczykowski. A9-0168/2022. Retrieved December 8, 2023, from: https://www.europarl.europa.eu/doceo/document/A-9-2022-0168_EN.pdf

European Parliament. (2023, April 19). European Parliament resolution on the challenges facing the Republic of Moldova, 19 April 2023. Retrieved December 9, 2023, from https://www.europarl.europa.eu/delegations/en/product/product-details/20230504DPU36113

European Union Council. (2020, February 21). Declaration by the High Representative on behalf of the European Union: Call to promote and conduct responsible behaviour in cyberspace. Retrieved December 9, 2023, from: https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/

European Union Council. (2022a, May 10). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. Retrieved December 9, 2023, from https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

European Union Council. (2022b, July 19). Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine. Retrieved December 9, 2023, from: https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

Farrugia, C. J. (1993). The special working environment of senior administrators in small states. World Development, 21(2), 221–226. https://doi.org/10.1016/0305-750x(93)90017-4

Federal Foreign Office. (n.d.). Common Security and Defence Policy (CSDP). Retrieved December 16, 2023, from: https://www.auswaertiges-amt.de/en/aussenpolitik/europe/gsvp-start/209178

FIIAPP. (2023, June 27). The European Union ensures cyber security in Ukraine. Retrieved December 8, 2023, from: https://www.fiiapp.org/en/noticias/european-union-ensures-cyber-security-in-ukraine/

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, 52(4), 887-917. doi: https://doi.org/10.1162/002081898550789

Furber, C. (2010). Framework analysis: a method for analysing qualitative data. African Journal of Midwifery and Women's Health, 4(2), 97–100. https://doi.org/10.12968/ajmw.2010.4.2.47612

Gallagher, R. (2023, April 20). Russian Cyberattacks Target Moldova Amid Ukraine War. Bloomberg. Retrieved December 14, 2023, from: https://www.bloomberg.com/news/articles/2023-04-20/russian-cyberattacks-target-moldova-amid-ukraine-war?embedded-checkout=true

Gordon, S., & Rosenbach, E. (2022). America's Cyber-Reckoning: How to Fix a Failing Strategy. Foreign Affairs, 101(1), 10-21.

Government of Georgia. (2021). *Resolution of the Government of Georgia on the approval of the 2021-2024 national cyber security strategy of Georgia and its action plan (Document No. 482)*. Received by Government of Georgia on September 30, 2021. [Original title: საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ] Retrieved from https://matsne.gov.ge/ka/document/view/5263611?publication=0

Government of the Republic of Moldova, Ministry of Economic Development and Digitalization of the Republic of Moldova, & United Nations Development Programme. (2023). Digital Transformation Strategy 2023-2030. Retrieved from https://mded.gov.md/en/transparency/digital-transformation-strategy-2023-2030/

Grossman, T. (2023, November). *Cyber Rapid Response Teams: Structure, Organization, and Use Cases*. Center for Security Studies (CSS), ETH Zürich. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf

IDC on NATO in Moldova. (2015a, February 9). What is IDC on NATO. Retrieved December 4, 2023, from: https://infocenter.md/en/ce-este-nato/what-is-idc-on-nato/

IDC on NATO in Moldova. (2015b, July 29). Public lecture at the "Onisifor Ghibu" Lyceum in Orhei. Retrieved from https://infocenter.md/en/public-lecture-at-the-onisifor-ghibu-lyceum-in-orhei/

IDC on NATO in Moldova. (2020a, May 12). #3 Dialogue with experts: Disinformation during crisis: the impact on human security. Retrieved December 4, 2023, from: https://infocenter.md/en/3-dialogue-with-experts-disinformation-during-crisis-the-impact-on-human-security/

IDC on NATO in Moldova. (2020b, July 7). Stages, areas and framework of cooperation. Retrieved December 5, 2023, from: https://infocenter.md/en/istoric-si-cadrul-de-cooperare/

Information Center on NATO and EU. (2022, May 10). The seminar "European and Euro-Atlantic integration of Georgia" was held for young people within the framework of "Europe Days 2022" [Original title: ევროპის დღეები 2022-ის ფარგლებში ახალგაზრდებისთვის სემინარი საქართველოს ევროპული და ევროატლანტიკური ინტეგრაცია ჩატარდა]. Retrieved from https://infocenter.gov.ge/news/evropis-dgheebi-2022-is-farglebshi-akhalgazrdebisthvis-seminari-saqarthvelos-evropuli-da-evroatlantikuri-integracia-chatarda/

Information Center on NATO and EU. (n.d.). [Original title: საინფორმაციო ცენტრი ნატოსა და ევროკავშირის შესახებ]. Retrieved from https://infocenter.gov.ge/?s=%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0&lang=ka

Information System Authority. (2023). Cyber Security in Estonia 2023. Retrieved September 30, 2023, from: https://www.ria.ee/en/media/2702/download

Institute for Security and Safety. (2017). NATO SPS Course: "Cyber Defence in the Context of Energy Security", Kiev/Ukraine. UNISS. Retrieved December 5, 2023, from: https://uniss.org/news-events/nato-sps-course-cyber-defence-in-the-context-of-energy-security-kiev-ukraine/

International Information Academy. (2020). The Third Annual International Forum "Cybersecurity - Protect Business, Protect the State" took place, which was attended by experts of the International Information Academy – members of the Anti-Crisis Center for Cyber Protection of Business, Ukrainian Chamber of Commerce. Retrieved December 9, 2023, from: https://interacademy.info/en/the-third-annual-international-forum-cybersecurity/

International Telecommunication Union. (n.d.). National Cybersecurity Strategies repository. Retrieved October 2, 2023, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Jugl, M. (2018). Finding the golden mean: country size and the performance of national bureaucracies. Journal of Public Administration Research and Theory, 29(1), 118–132. https://doi.org/10.1093/jopart/muy044

Kello, L. (2013). The Meaning of the Cyber Revolution Perils to Theory and Statecraft. International Security, 38(2), 7–40. doi: https://doi.org/10.1162/ISEC_a_00138

Kert-Saint Aubyn, M. (n.d.). EU Adopts Network and Information Security Directive that Sets Security Rules on National Critical Infrastructure. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved December 12, 2023, from: https://ccdcoe.org/incyder-articles/eu-adopts-network-and-information-security-directive-that-sets-security-rules-on-national-critical-infrastructure/

Knudsen, O. F. (1996). Analysing Small-State Security: The Role of External Shelter. In W. Bauwens, A. Clesse, & O. F. Knudsen (Eds.), Small States and the Security Challenge in the New Europe (pp. 3-20). Brassey's.

Law of Ukraine. (2017). On the Basic Principles of Cybersecurity in Ukraine. The Official Bulletin of the Verkhovna Rada (BVR), No. 45, Article 403. Version from August 17, 2022. Retrieved November 17, 2023, from https://zakon.rada.gov.ua/laws/show/2163-19?lang=en

Maigre, M. (2023). Empowering cyber capacity building: View from Estonia. Baltic RIM Economies. Safety and Security, (2), 55-56. The Centrum Balticum Foundation. Retrieved September 30, 2023, from https://www.centrumbalticum.org/files/5712/BRE_2_2023.pdf

Marusic, S. J. (2022). North Macedonia banks targeted by notorious Greek hackers. Balkan Insight. Retrieved October 3, 2023, from https://balkaninsight.com/2022/02/23/north-macedonia-banks-targeted-by-notorious-greek-hackers/

McGlinchey, S. (Ed.). (2022). *Foundations of International Relations*. London: Bloomsbury Publishing.

Menabde, G. (2019, April 1). NATO again demonstrates strong support for Georgia. Eurasia Daily Monitor, 16(45). Jamestown Foundation. Retrieved December 5, 2023, from: https://jamestown.org/program/nato-again-demonstrates-strong-support-for-georgia/

Microsoft. (2022a). *Microsoft Digital Defense Report 2022: Illuminating the threat landscape and empowering a digital defense*. Retrieved October 2, 2023, from https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

Microsoft. (2022b, September 8). Microsoft investigates Iranian attacks against the Albanian government. Retrieved October 3, 2023, from https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Microsoft. (2023, May 2). Iran turning to cyber-enabled influence operations for greater effect. Microsoft Threat Intelligence. Retrieved October 3, 2023, from https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf

Ministry of Defence of Georgia. (2020, March 5). LEPL Cyber Security Bureau of MOD has joined NATO's Malware Information Sharing Platform (MISP), making Georgia as the second non-NATO country with such membership. Shared important information will strengthen the bureau's capacity to provide effective cybersecurity. [Tweet]. Twitter. https://twitter.com/ModGovGe/status/1235522761277214720

Ministry of Defence of Georgia. (2021). *Strategic Defence Review 2021-2025*. Retrieved from https://mod.gov.ge/en/page/73/strategic-defence-review

Ministry of Defence of Georgia. (n.d.-a). Cooperation with the European Union. Retrieved December 8, 2023, from: https://mod.gov.ge/en/page/39/cooperation-with-the-european-union

Ministry of Defence of Georgia. (n.d.-b). NATO-Georgia Cooperation. Retrieved December 12, 2023, from: https://mod.gov.ge/en/page/38/nato-georgia-cooperation

Ministry of Defense of the Republic of Moldova. (2018). Action Plan regarding the implementation of the National Strategy of Defense for the years 2018–2022, Appendix No. 2. Retrieved from https://www.army.md/?lng=2&action=show&cat=157

Ministry of Foreign Affairs of Ukraine. (2018). Annual national programme under the auspices of the NATO-Ukraine Commission for 2018. NATO.

https://nato.mfa.gov.ua/en/documents/annual-national-programme-under-auspices-nato-ukraine-commission-2018

Mirel, P. (2021). The Eastern Partnership, between resilience and interference. Foundation Robert Schuman. European Issues n°589.

Montevideo Convention on the Rights and Duties of States. (1933). University of Oslo. Retrieved September 3, 2023, from: https://www.jus.uio.no/english/services/library/treaties/01/1-02/rights-duties-states.html

National Cyber Security Centre. (2018, February 14). Russian military almost certainly responsible for destructive 2017 cyber attack. Retrieved from December 14, 2023, from https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

National Cyber Security Directorate [Directoratul Național de Securitate Cibernetică]. (2023, April 21). Press release: The Romanian National Cyber Security Directorate (DNSC) participated in the NATO Locked Shields 2023 international exercise. Retrieved from December 4, 2023, from: https://dnsc.ro/vezi/document/press-release-the-romanian-national-cyber-security-directorate-dnsc-participated-in-the-nato-locked-shields-2023-international-exercise-pdf

National Cyber Security Index. (n.d.). Retrieved October 2, 2023, from https://ncsi.ega.ee/

National Security and Defense Council of Ukraine. (2020). On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine" (Decree No. 392/2020). [Original title: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»] President of Ukraine. Retrieved from https://www.president.gov.ua/documents/3922020-35037

National Security and Defense Council of Ukraine. (2021, August 26). On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" (Decree No. 447/2021) [Decree]. [Original title: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"] President of Ukraine. https://www.president.gov.ua/documents/4472021-40013

National Security and Defense Council of Ukraine. (2022, February 1). About the Cyber Security Strategy Implementation Plan of Ukraine [Original title: Про План реалізації Стратегії кібербезпеки України] (Decree No. 37/2022). President of Ukraine. https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

National Security Council of Georgia. (2023, June 21). Georgia Cybersecurity Forum 2023 was opened. Retrieved December 9, 2023, from: https://nsc.gov.ge/en/NEWS/georgia-cybersecurity-forum.html

NATO Communications and Information Agency. (2021, January 21). NATO assists Moldova in improving its cyber security capabilities. Retrieved December 9, 2023, from: https://www.ncia.nato.int/about-us/newsroom/nato-assists-moldova-in-improving-its-cyber-security-capabilities.html

NATO. (2015, August 27). NATO-Georgian Joint Training and Evaluation Center (JTEC) [Fact Sheet]. Retrieved December 5, 2023, from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20150827_150827-jtec-georgia.pdf

NATO. (2016, July 8). *Cyber Defence Pledge*. NATO. Retrieved from December 2, 2023, from: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2017a, May 19). The NATO Information and Documentation Centre in Ukraine celebrates its 20th anniversary. Retrieved from https://www.nato.int/cps/en/natohq/news_143930.htm

NATO. (2017b, December 12). Defence Education Enhancement Programme (DEEP). Retrieved December 5, 2023, from: https://www.nato.int/cps/en/natohq/139182.htm

NATO. (2021, December 9). Building Integrity. Retrieved December 9, 2023, from https://www.nato.int/cps/en/natohq/topics_68368.htm

NATO. (2022). Strategic Concept. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2023a, July 11). Vilnius Summit Communiqué: Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius. NATO. Retrieved December 10, 2023, from: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO. (2023b, December 4). NATO's flagship cyber exercise concludes in Estonia. NATO. Retrieved December 4, 2023, from: https://www.nato.int/cps/en/natohq/news_220993.htm

NATO. (2023c, October 5). Defence Education Enhancement Programme (DEEP). Retrieved December 5, 2023, from: https://www.nato.int/cps/en/natohq/topics_139182.htm

NATO. (2023d, March 22). Cybersecurity - A Generic Reference Curriculum. Retrieved December 5, 2023, from: https://www.nato.int/cps/em/natohq/topics_157591.htm

NATO. (2023e, April 25). Partnership Interoperability Initiative. Retrieved December 9, 2023, from https://www.nato.int/cps/en/natohq/topics_132726.htm

NATO. (2023f, June 5). Defence and Related Security Capacity Building Initiative. Retrieved December 9, 2023, from https://www.nato.int/cps/en/natohq/topics_132756.htm

NATO. (2023g, April 19). Membership Action Plan (MAP). Retrieved December 12, 2023, from https://www.nato.int/cps/en/natohq/topics_37356.htm

NATO. (2023h, August 16). Partnership Tools. Retrieved December 12, 2023, from: https://www.nato.int/cps/en/natohq/topics_80925.htm#:~:text=The%20Annual%20National%20Programme%20,case%20for%20Georgia%20and%20Ukraine

NATO. (2023i, May 26). Relations with the Republic of Moldova . Retrieved December 12, 2023, from: https://www.nato.int/cps/en/natohq/topics_49727.htm

NATO. (n.d.-a). Cyber defence. NATO. Retrieved August 31, 2023, from https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (n.d.-b). Defence Institution Building School: An Initiative of the Substantial NATO-Georgia Package [Fact Sheet]. Retrieved December 5, 2023, from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160628_1607-dib-georgia-en.pdf

Naylor, E., Painter, C., & Hakmeh, J. (2022, February 7). How does capacity-building make cyberspace better? Chatham House – International Affairs Think Tank. Retrieved December 14, 2023, from: https://www.chathamhouse.org/2022/02/how-does-capacity-building-make-cyberspace-better

Neljas, A. (2020). Russia's Recent Foreign Policy toward its Neighbours in EU Eastern Neighbourhood. Estonian Centre of Eastern Partnership, pp.1-26

Neuneck, G. (2013). Assessment of international and regional organizations and activities. In: Lewis, J.A. & Neuneck, G. *The Cyber Index – International Security Trends and Realities*. Geneva: UN Institute for Disarmament Research. Retrieved October 5, 2023, from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

NIST. (n.d.). Computer Security Incident Response Team (CSIRT). Retrieved December 14, 2023, from: https://csrc.nist.gov/glossary/term/computer_security_incident_response_team

Open Ukraine Foundation. (2016, April 15). Michal Boni: Ukraine's cybersecurity strategy should be as close to the European model as possible. Retrieved December 9, 2023, from: https://ksf.openukraine.org/en/categories/news/strategija-kiber-bezpeky-ukrainy-povynna-bude-maksymalno-nablyzhena-do-evropejskoji-modeli-mihal-boni

Open Ukraine Foundation. (2023). 15th Annual Kyiv Security Forum Agenda 2023. Retrieved December 9, 2023, from: https://ksf-openukraine.s3.eu-central-1.amazonaws.com/15th_Annual_Kyiv_Security_Forum_Agenda_2023_2_f89363a3e5.pdf

Osula, A.-M., & Kaska, K. (2013). *National Cyber Security Strategy Guidelines*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf

Panke, D. (2012). Small states in multilateral negotiations. What have we learned? Cambridge Review of International Affairs, 25(3), 387–398. https://doi.org/10.1080/09557571.2012.710589

Parliament of the Republic of Moldova. (2002). Decision No. 1315 of 26-07-2002 regarding the approval of the Military Reform Concept. [Original Title: *HOTĂRÂRE Nr. 1315 din 26-07-2002 cu privire la aprobarea Concepţiei reformei militare*]. Retrieved from https://www.legis.md/cautare/getResults?doc_id=30396&lang=ro

Parliament of the Republic of Moldova. (2011). Decision No. 153 for the approval of the National Security Strategy of the Republic of Moldova (Amended version of March 24, 2023). Official Gazette, No. 170-175, art. 499. [Original Title: Republica Moldova PARLAMENTUL HOTĂRÂRE Nr. 153 din 15-07-2011 pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova. Publicat : 14-10-2011 în Monitorul Oficial Nr. 170-175 art. 499] Retrieved from https://www.legis.md/cautare/getResults?doc_id=136241&lang=ro#

Parliament of the Republic of Moldova. (2018). Decision No. 257 regarding the approval of the Information Security Strategy of the Republic of Moldova for the years 2019–2024 and the Action Plan for its implementation. Official Gazette No. 13-21, Art. 80 (Published 18-01-2019). [Original Title: Republica Moldova PARLAMENTUL HOTĂRÂRE Nr. 257 din 22-11-2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia] Retrieved from https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

Pedi, R. (2020). Small states in Europe as a buffer between East and West. In G. Baldacchino & A. Wivel (Eds.), Handbook on the Politics of Small States (pp. 168–188). Edward Elgar Publishing. https://doi.org/10.4337/9781788112932

Pevcin, P. (2020). Government size and quality of governance: Does state size matter? International Journal of Business and Economic Sciences Applied Research. https://doi.org/10.25103/ijbesar.133.01

Poireault, K. (2023, August 3). Cyber-attacks targeting government agencies increase 40%. Infosecurity Magazine. Retrieved October 2, 2023, from https://www.infosecurity-magazine.com/news/cyberattacks-government-agencies/

President of Ukraine. (2021, July 30). Decree No. 448/2021 on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Ukraine's Foreign Policy Activity". [Original title: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №448/2021 Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року "Про Стратегію зовнішньополітичної діяльності України"] Retrieved from https://www.president.gov.ua/documents/4482021-40017.

Prosecutor General's Office of Ukraine. (2021). International Forum on Cyber Security (IFCS). Retrieved December 9, 2023, from: https://ifcs.gp.gov.ua/#about

Randma-Liiv, T., & Sarapuu, K. (2019). Public governance in small states: From paradoxes to research agenda. In A. Massey (Ed.), A Research Agenda for Public Administration (pp. 162–179). Edward Elgar Publishing. https://doi.org/10.4337/9781788117258.00016

Regional Cybersecurity Symposium. (2023). RCS. Retrieved December 9, 2023, from: https://rcs.md/

Republic of Moldova & NATO. (2022). Individual Partnership Action Plan (IPAP) 2022-2023. Ministry of Foreign Affairs of the Republic of Moldova. Retrieved December 9, 2023, from: https://mfa.gov.md/sites/default/files/individual_partnership_action_plan_ipap_republic_of_moldova_-_nato_for_2022-2023.pdf

Republic of Moldova. (2018). Action Plan regarding the implementation of the Military Strategy for the years 2018-2022, Appendix No. 2 to Government Decision No. 961/2018. [Original title: PLAN DE ACȚIUNI privind implementarea Strategiei militare pentru anii 2018-2022, Anexa nr.2 la Hotărîrea Guvernului nr.961/2018] Retrieved from https://www.army.md/?lng=2&action=show&cat=157

Reuters. (2022, September 1). Montenegro blames criminal gang for cyber attacks on government. Retrieved October 3, 2023, from Reuters. https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/

RFE/RL. (2020, February 20). U.S., U.K. Blame Russia For 2019 Cyberattack On Georgian Websites. Radio Free Europe/Radio Liberty. Retrieved from https://www.rferl.org/a/tbilisi-washington-blame-russia--cyberattack-georgian-websites/30445595.html

RFE/RL. (2022, November 30). Moldova Not Pursuing NATO Membership But Aims To Strengthen Cooperation With Alliance. Radio Free Europe/Radio Liberty. Retrieved December 12, 2023, from https://www.rferl.org/a/moldova-nato-membership-cooperation-alliance/32155800.html

Security Service of Ukraine. (2022, April 5). SSU and NATO step up cooperation in cybersecurity: threat monitoring systems integrated. Retrieved December 9, 2023, from: https://ssu.gov.ua/en/novyny/sbu-ta-nato-posylyly-spivpratsiu-u-sferi-kiberbezpeky-vidbulasia-vzaiemna-intehratsiia-system-monitorynhu-zahroz#:~:text=The%20Security%20Service%20of%20Ukraine,by%20the%20Alliance%20since%202012.

Service for Foreign Policy Instruments. (2022, May 2). New support to the Republic of Moldova on cyber-security, addressing disinformation and social cohesion. European Commission. Retrieved December 8, 2023, from: https://fpi.ec.europa.eu/news-1/new-support-republic-moldova-cyber-security-addressing-disinformation-and-social-cohesion-2022-05-02_en

Significant Cyber Incidents. (n.d.). Center For Strategic & International Studies. Retrieved October 14, 2023, from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Smith, J., & Firth, J. (2011). Qualitative data analysis: the framework approach. Nurse Researcher, 18(2), 52–62. https://doi.org/10.7748/nr2011.01.18.2.52.c8284

SonicWall. (2023). 2023 SonicWall Cyber Threat Report. Retrieved October 2, 2023, from https://www.sonicwall.com/2023-cyber-threat-report/

State Service of Special Communications and Information Protection of Ukraine. (2022). Russia's Cyber Tactics: Lessons Learned 2022. Retrieved September 30, 2023, from https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

Streeten, P. (1993). The special problems of small countries. World Development, 21(2), 197–202. https://doi.org/10.1016/0305-750x(93)90014-z

Stupp, C. (2022, April 20). NATO Cyber Exercise Proceeds Against Backdrop of Ukraine War. *WSJ*. Retrieved December 4, 2023, from: https://www.wsj.com/articles/nato-cyber-exercise-proceeds-against-backdrop-of-ukraine-war-11650480793

Tan, E. E. G. (2019). A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore. *PRISM, 8*(3), 158–171. https://www.jstor.org/stable/26864282

Thorhallsson, B. (2006). The size of states in the European Union: Theoretical and conceptual perspectives. Journal of European Integration, 28(1), 7–31. https://doi.org/10.1080/07036330500480490

Thorhallsson, B. (2011). Domestic buffer versus external shelter: Viability of small states in the new globalised economy. *European Political Science, 10*(3), 324–336. https://doi.org/10.1057/eps.2011.29

Thorhallsson, B. (2015). How Do Little Frogs Fly? Small States in the European Union. Norwegian Institute of International Affairs. Policy Brief, 12, 1-4.

Thorhallsson, B. (2018). Studying small states: A review, *Small States & Territories*, *1*(1), 17-34.

Thorhallsson, B., & Steinsson, S. (2017). Small state foreign policy. Oxford Research Encyclopaedia of Politics. https://doi.org/10.1093/acrefore/9780190228637.013.484

Thorhallsson, B., & Steinsson, S. (2018). THE THEORY OF SHELTER. Paper presented at the Conference: 'Small States and the New Security Environment', University of Iceland, Reykjavik. Policy brief no. 1. SSANSE. https://uni.hi.is/baldurt/files/2018/07/The-Theory-of-Shelter3909.pdf

Thorhallsson, B., & Steinsson, S. (2021). Shelter Theory and Smallness in International Relations. In B. Thorhallsson (Ed.), *Iceland's Shelter-Seeking Behavior. From Settlement to Republic* (pp. 7-20). Cornell University Library Ithaca, New York. (ISLANDICA LXIII)

Valeriano, B & Maness, R.C. (2018) International Relations Theory and Cyber Security. In Brown, C., & Eckersley, R. (Eds.). *The Oxford Handbook of International Political Theory*. Oxford University Press.

Veenendaal, W., & Corbett, J. (2014). Why small states offer important answers to large questions. Comparative Political Studies, 48(4), 527–549. https://doi.org/10.1177/0010414014554687

Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved October 14, 2023, from https://www.belfercenter.org/publication/national-cyber-power-index-2022

World Economic Forum. (2023a). *Global Cybersecurity Outlook 2023*. Retrieved October 2, 2023, from https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

World Economic Forum. (2023b). *The Global Risks Report 2023* (18th ed.). Retrieved October 2, 2023, from https://www.weforum.org/reports/global-risks-report-2023/

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Hauke Claus Schulz

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis: *Georgia's, Moldova's, and Ukraine's cybersecurity engagements with the EU and NATO*

supervised by Radu Antonio Serrano Iova, MSc

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

19.12.2023

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period*