University of Macedonia

Department of International and European Studies

BACHELOR THESIS

Cyber Security and Defence Strategy of EU's Small States:

The cases of Greece & Estonia

Author

Maria Sotiropoulou ies18094@uom.edu.gr

Supervisor

Dr. Revecca Pedi rpedi@uom.edu.gr

Submitted in fulfillment of the requirements for a bachelor's degree in the field of International and European Studies.

Θεσσαλονίκη, Φεβρουάριος 2023

Υπεύθυνη Δήλωση

«Δηλώνω υπεύθυνα ότι όλα τα δεδομένα στην παρούσα εργασία αποκτήθηκαν, επεξεργάστηκαν και παρουσιάστηκαν σύμφωνα με τους κανόνες και τις αρχές της ακαδημαϊκής δεοντολογίας, καθώς και με τους νόμους που διέπουν την έρευνα και την πνευματική ιδιοκτησία. Όπως απαιτείται από τους κανόνες αυτούς, αναγνωρίζω και αναφέρω τις πηγές όλων των δεδομένων που χρησιμοποιώ και τα οποία δεν αποτελούν δική μου πρωτότυπη δημιουργία. Δίνω επίσης τη συγκατάθεσή μου ώστε το ηλεκτρονικό αντίγραφο της διατριβής μου να υποβληθεί σε ηλεκτρονικό έλεγχο για τον εντοπισμό τυχόν ενδείξεων παραβίασης πνευματικών δικαιωμάτων».

Μαρία Σωτηροπούλου

Thessaloniki, February 2023

Declaration

"I declare responsibly that all data in this paper were obtained, processed, and presented in accordance with the rules and principles of academic ethics, as well as the laws governing research and intellectual property. As required by these rules, I acknowledge and cite the sources of all data I use that do not constitute my original creation. I also give my consent for an electronic copy of my thesis to be subjected to an electronic check to identify any evidence of copyright infringement."

Maria Sotiropoulou

Abstract

It is common knowledge that societies are moving forward to their digitalization notably in the aftermath of the Covid-19 outbreak, a process that has induced further shifts in the global security environment. The sophisticated challenges in cyberspace require a modern and cutting-edge approach that will achieve the protection of grids and data. The ongoing war in Ukraine, in which offensive cyber operations have also been conducted orchestrated by Russia, verifies that hybrid weapons have entered the conventional battlefields, proving that the Internet has evolved into a battlefield for geopolitical conflicts.

In this anarchic and antagonistic nature of the international system, small states strive to cope with the vulnerabilities that derive from their petit size, i.e. limited resources, influence, power and more, in order to endure and advance their country's interests. In this line, they often join cooperation entities and coalitions so to promote their demands and savor the benefit of these structures. European Union is an institution that provides its member-states with a variety of legal framework and mechanisms to fight security menaces, boost the European economy, and strengthen its credibility. As cyberspace has been recognized as the fifth domain of action, it is vital for the Union to safeguard and simplify its citizens' digital aspects of life based on fundamental human rights.

In this thesis, two European small states will be examined with a view to demonstrate the way they perceive cybersecurity and the gravity it has at the national level in proportion to their strategic environment and capabilities. In particular, Greece and Estonia have been selected because of their prominent security value as both of them invest highly in this field in general (they devote 2% of GDP to defence). The main purpose is to result in the conclusion that despite their rather palpable "weak points", small powers are indeed able to antagonize the great powers and implement smart strategies that will increase their influence and place them in the centre of the game.

Key words: Cybersecurity, Cyberthreats, Small States, Greece, Estonia, EU, Strategy

Table of contents

1. Introduction

In this day and age, power politics have been propagated on the internet, beyond the traditional boundaries of the international arena. All types of actors (individuals, states, non-state bodies, regional and international organizations and more) are called upon to confront the cyber challenges that generate during the unfolding digitalization of the world. Being a piece of the multipolar puzzle, the European Union has adopted policies and has orchestrated actions in order to protect its grids, and consequently its people, from the cyberthreats that are gaining ground as technology advances. Its endgame is to move towards its political, economic, and societal integration that will in turn result in the fulfillment of its ambitions: increase its power and become strategically autonomous (Miró, 2022). The war in Ukraine has reinvigorated hacktivism, i.e. the practice of illegally accessing software systems to accomplish political goals (Cambridge Dictionary, n.d.), another illustration of the online transition of geopolitics. Indeed, cyber security and defence rank among the EU's highest priorities, because of the additional troubles provoked by the Covid-19 pandemic and the broaden use of digital devices and the web (Carrapico & Farrand, 2020). From the standpoint of the criminal ecosystem, it appears that the level of competition has decreased (Krusten, 2019), and less technical abilities are required to begin perpetrating cybercrimes, besides the fact that they are of limited risk but of high earnings especially after the trend of cryptocurrency. As it is mentioned in the EU Cyber Defence Policy Framework document 2014 (Council of the European Union 15585/14), cyberspace is the fifth domain of operations. The latest document of Common Security and Defence Policy or CSDP, the Strategic Compass 2022 quotes (Strategic Communications, 2022):

"We recognize that enhancing our cybersecurity is a way to increase the effectiveness and security of our efforts on land, in the air, at sea, and in outer space."

All the above highlight one of the EU's strategic priorities, as it is also described in Europe's Digital Decade: digital targets for 2030.

In the anarchic and antagonistic international system, all the EU Member States – henceforth MS – play a unique role in the "European integration" process, in proportion to their material capabilities and national interests. Most of the group of the 27 are in fact small powers, which have accessed the Union so to enjoy the benefits of belonging into a cooperation body and thus, survive in the system of the "great ones"(Pedi & Sarri, 2021). As cyberspace has no limits, small states are often vulnerable in front of hybrid threats such as cyber-attacks and suffer immense losses, but at the same time, it is a domain where no hard power is needed to prevail. Because of

that, small states have the potential to become powerful players of the game, augmenting their influence and antagonizing the great powers on their rules. This idea is the primary reason for elaborating this thesis. To put it in other words, its purpose is to demonstrate the motives and examine the practices of small states in combating cyberthreats and scrutinize whether the already existing in the literature view that "small does not necessarily mean weak" applies in cybersecurity. To streamline the process, two case-studies were selected, Greece and Estonia. Both of them are of great research interest regarding the concept of European security and defence, due to their unique dynamic in their regional systems of Eastern Mediterranean and Northern Europe respectively (Karyoti, 2022, Veebel & Ploom, 2022). Moreover, the fact that they face conventional and non-conventional menaces produces a genuine interest to study how small states manage cyberthreats in turbulent environments. In addition, it is pretty intriguing to analyze the cyber strategies of these states and the reasons why Greece and Estonia differ in this field despite their strong concern around security and defence.

The structure has been organized with the aim of providing a concrete image of cybersecurity strategy in Greece and Estonia. To begin with, it is essential to be familiarized with the perception the Union has for security and cybersecurity. In Chapter 2, a brief analysis of the historical evolution of CSDP will be presented, alongside the measures and mechanisms that the EU has taken in order to protect its MS from the risks in cyberspace. Then the way this paper defines and comprehends the small states' concept is illustrated in Chapter 3, because there is not a particular definition upon the term of small states; on the contrary there is a plethora of them that vary in line with the criteria that fulfill the goal of each and every paper/research. Moving on to Chapters no. 4 and no. 5, the case-studies will be examined separately, accompanied by two sub-chapters in which their respective strategic environment with a bunch of reported cyber incidents and their action-plans in addressing cyberthreats will be analyzed. These will provide a better understanding of the main purpose of the paper and wish to provoke further critical thinking regarding the topic to the reader. Last but foremost, the conclusions will be produced in Chapter 6 alongside a brief comparison of the two national strategies that underlines their key-differences. Except for those, it is important to mention that the literature of this thesis is solely based on public evidence resources with open access, preferably journals, dissertations, books, reports, national and European gazettes, press releases, websites and online newspapers. As far as the Tables are concerned, the pieces of information were collected mainly by online newspapers and magazines, due to the lack of large-scale databases in terms of time apropos of the confirmed cyber-attacks.

1.1 Definitions

At this point, it is considered appropriate by the author to provide some basic definitions of specific cyber-attacks' types in order to facilitate the reader's better familiarity with the topic before proceeding to the main analysis. These are provided here as presented in the ENISA Threat Landscape 2022 report (Ardagna et al., 2022).

Ransomware: *ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. It has been, once more, one of the prime threats during the reporting period, with several high profile and highly publicised incidents.*

Threats against availability: Denial of Service: *availability is the target of a plethora of threats and attacks, among which DDoS stands out. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure.*

Supply Chain Attacks: *an attack is considered to have a supply chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets.*

2. From European Security to European Cyber Security

2.1 The evolution of European Security and Defence Policy

In the aftermath of WWII, European leaders realized for good that the only way to prevent another bloody and destructive conflict was if they were united and committed to strong legal bindings that none would dare to encroach because of the interdependence. This was the vision of the founding fathers of the EU. It all started with the Treaty of Rome in 1957 that launched the European Economic Community. The 1960s and 1970s that followed, were two decades of turmoil, with events that determined the course of today's international system. Despite the great number of security threats against the then EEC, it was no sooner than the year the Soviet Union collapsed, in 1992, when the Maastricht Treaty was signed, that endorsed the new name of the European Union (*Treaty on European Union*, p.4, 1992) and revised the charter establishing an economic and monetary union and the European citizenship. In addition, it implemented radical changes, starting with the three fundamental pillars on which it still works: a) European Communities, b) Justice and Home Affairs, c) Common Foreign and Security Policy (CFSP). In

particular, the MS of the Western European Union[1] introduced the Petersberg Tasks (Publications Office of the European Union, 2017) in the spirit of NATO, which stated their readiness status to provide military forces in unstable and hostile environments. During the uproarious years of the dissolution of Yugoslavia, the Treaty of Amsterdam (1997) entered into force in 1999 to incorporate the Petersberg Tasks to the EU, while it clarified the role and authority of the High Representative for Common Foreign and Security Policy. Nonetheless, NATO would continue to be the main mechanism of collective defence for Europe, influencing the EU's security decision-making.

The 21st century found the European Union in a mood to boost its vision for a safer environment, bearing in mind the shift of the threat-concept from conventional to unconventional after 9/11 and the wars that followed in Afghanistan and Iraq. Therefore, in 2003, the first European Security Strategy was adopted[2], presenting the security status of the time, the threats that Europe had to deal with and possible solutions to encounter them, while calling for the creation of a more capable and cohesive political environment, strong enough to handle the external issues and protect European citizens. Furthermore, the empowered EU after the enlargement of 2004 and 2007, put into effect the Treaty of Lisbon (2007) in 2009, covering among others, a percentage of the gap in European security and defence. According to article 28A, the Common Security and Defence Policy (CSDP) was compounded as the EU's integrated approach in foreign policy issues, giving a boost to its operational capabilities in fragile environments, under the MS military and civilian support. Additionally, the European External Action Service (EEAS) i.e., the diplomatic service of the EU was founded and the Global Strategy for European Foreign and Security Policy (EFSP) was introduced in 2016 (European External Action Service, 2016). On the road towards European strategic autonomy that is crucial for its integration, the Permanent Structured Cooperation (PESCO) was added to the toolbox in 2017, offering an upgraded level of mutual cooperation in MS' defence, aiming to enhance EU capabilities missions (Council decision (CFSP) 2017/2315). PESCO framed the European Defence Fund and the Coordinated Annual Review on Defence (CARD). One of the latest developments of the CSDP, is the European Peace Facility (Council Decision (CFSP) 2021/509), an off-budget financial tool that is in force since March 2021

[1] Western European Union succeeded the Western Union in 1955 https://www.cvce.eu/en/collections/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/9059327f-7f8a-4a74-ac7e-5a0f3247bcd3/Resources#73277207-d250-41c5-8960-1d8bce9f11aa_en&overlay

[2] The official document is in hardcopy only.

that aims to assist the Union's action in conflict prevention and peacebuilding procedures through its operation and assistance measures pillars.

With regard to the contemporary EU strategic environment, this is illustrated in Strategic Compass 2022 (Strategic Communications, 2022), a document that renders the EU with an action plan on how to empower its security and defence policy until 2030. Its approval by the Council corresponded with the war in Ukraine, adding further value to the Union's ambitions. In particular, it sets 4 work strands on its agenda, aiming to communicate among its MS a common understanding of the challenges and the purposes of its actions, in order to function coherently and effectively: Act, Secure, Invest and Partner. Among the plethora of risks that the Union is confronting, cyberthreats hold a significant position. Indeed, cybersecurity is a paramount aspect of CSDP due to the direct affection to the security of European society and the growing demand to defend the European and MS grids that emanates from the high numbers of cyber-attacks in combination with advanced technologies. In the following chapter, the EU's strategy on fighting cybercrime will be analyzed alongside some remarkable cyber incidents that have plagued it throughout the years.

2.2 EU's Digital Transition

The 447 million European citizens (Eurostat, 2022) enjoy the privileges that technology has bestowed upon them, which have facilitated their daily routine to a certain extent. Nonetheless, the more widespread the use of the internet gets, the greater the threats are. The European Union per se is familiar with cyber risks and breaches, in terms of affecting one or more of its MS; albeit, its experience goes beyond that impact, reaching incidents that have occurred in its own institutions, bodies and agencies (in this thesis cases concerning individuals will be excluded). Table 2.2 which follows depicts some notified cyber-attacks that the EU has suffered from. These pieces of information were found on separate open sources (mainly on reports published in think-tanks and online press articles) and were placed in the form of a table by the author, in order to offer the reader a better understanding of the evolution of the EU's cybersecurity strategy.

Table 2.2 Indicative reported cyber-attacks against European Union.

Date	Attribution	EUIBAs[3]	Details
November 2022	-	European Parliament' services	A DDoS attack struck Parliament's services (in an effort to cut access in websites)for a few hours. It is believed the hackers to be linked to Killnet, a pro-Kremlin hacking group, yet there is not any official claim of responsibility (Sant and Goujard, 2022).
April 2021	-	European Commission and other institutions	EU institutions, agencies and IT infrastructure were affected by an "IT security incident", while there were warnings for possible phishing attempts (Paganini, 2021).
March 2021	-	European Banking Authority (EBA)	The Microsoft Exchange Service of EBA was attacked as part of a global hit, leading to possible access on personal data. The aggressor is possible to be a Chinese-state sponsored one called Hafnium, but the country rejects such allegations(Tidy, 2021).
December 2020	-	European Medicines Agency (EMA)	EMA (2021) suffered from a cyber robbery of records that were projected in darknet forums, aiming to decrease faith in vaccines of Covid-19.
Autumn 2019	Russia-linked hackers	6 EU agencies	The supply chain attack occurred in SolarWinds Orion IT monitoring platform, via a malware addition to versions of the app(Cimpanu, 2021) .
July 2014	-	European Central Bank	Hackers breached data (email and streets addresses, contact information, phone numbers) and asked for a ransom (Carnegie Endowment, n.d.).

In conformity with Enisa's Threat Landscape analysis of 2022, cyber threats have declined in numbers in 2022 in contrast to those of 2021, yet they have not vanished. Russia appears to be one of the major cyber rivals of the EU, as it may be noted in Table 2.2. In particular, the cyber-attack of November 2022 against the Parliament's website could be connected with the hackers of Killnet for two reasons. Firstly, Russia has suffered 9 European sanctions packages until the moment of the cyber hit on account of its invasion of Ukraine, including various restrictions and prohibitions against individuals and services of any kind (European Commission, n.d.); this creates a mutually hostile mood and an incentive to conduct the attack. Secondly, this aggression happened after the Parliament voted for the adoption of a resolution that designated Russia as a

[3] EU Institutions, Bodies and Agencies

state supporter of terrorism because it targeted civilians in Ukraine(Sant and Goujard, 2022). Needless to say, China, the number one cyber threat - state for the western world (Sabbagh, 2021), has been accused of committing a cyber-crime against the European Banking Authority, thus highlighting the vulnerability of the relations between the EU and the Asian superpower along with their antagonism in the international system. These cases reveal that even well-established organizations like the EU, are susceptible to hybrid actions of belligerence. It is lucid that improving European resilience is necessary to oversee the security issues of today. This argument could be further reinforced if the lack of precise details regarding the reported incidents is to be considered.

As a response to cyber peril, the Union has gradually embraced a legal framework that keeps enhancing, in an effort to protect its infrastructure, its values and above all, its citizens. It all started in 2004 when the European Network and Information Security Agency or ENISA was founded (Regulation (EC) No 460/2004)[4]; the headquarters are in Greece (Heraklion and Athens) and it is the main European bureau which cooperates with the private sector to advance national and regional cyber strategies and capacity building for safeguarding private data and technology of the MS. Notwithstanding, it is not more than ten years since the Union has included cybersecurity in its agenda in earnest. The cyber-attacks that Estonia suffered from in 2007 (will be examined in Chapter 5) were a big shock for the Union as well because there has not happened a crime of that scale against a state, never before. NATO had done already enough in order to protect its ally state; therefore, it was time for the European Union to act. In 2013, the first Cybersecurity Strategy of the EU was introduced (JOIN(2013) 1 final) which required from the MS, among others, to establish their national Computer Emergency Response Team (CERT)[5] and Competent Representative Authorities. It was the first official document to frame the term “Cybersecurity”. The EU Cyber Defence Policy Framework was adopted by the Council of the European Union (15585/14) in 2014 and contributed to a better understanding of the Strategy, while it set the priorities of CSDP in the cyber domain; it was updated in 2018 in order to become contemporary, in compliance with the challenges back then, and enclosed quite a few of the initiatives and regulations that followed thence (Council of the European Union 14413/18).

[4] Regulation (EC) No 460/2004 has been replaced by Regulation (EU) 2019/881 (2019) on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act).

[5] The Union owns its CERT- EU institution-wide provider that cooperates with ENISA in mitigating cyber threats. Its legal framework was constructed under the Interinstitutional Arrangement 2018/C 12/01.

The invasion of Russia in Crimea in 2014 brought to the surface the hybrid warfare concept, which contained cyber strikes except for other hybrid weapons (Klečková, 2021). The increasing number of attacks in cyberspace had consolidated the cyber war that the EU should fight and defend from. A milestone towards this was the Directive (Directive (EU) 2016/1148) on security on network and information systems – the NIS Directive. It was adopted in 2016 and offered a legal basis, under which MS should be prepared and equipped properly to handle any cyber threats, enhancing strategic cooperation among them in the established Cooperation Group (ibid art. 11) coordinated by ENISA, and growing a cybersecurity narrative in vital societal and financial domains. The famous Directive 2016/1148 has been repealed by NIS2 Directive (Directive (EU)2022/2555) that is in force since the 16th of January 2023. It introduces new tools to assist cyber defence such as the creation of the necessary cyber crisis management structure (CyCLONe). Another legislative addition of that year was the General Data Protection Regulation, mostly known as GDPR (Regulation (EU) 2016/679). Though its application was no sooner than that of May 2018, it is the EU's most strict policy (financial sanctions can be imposed in case of infringement of the legislation) and demonstrates a set of liabilities that organizations and enterprises of any kind shall meet, in order to secure their user's personal data. This specific regulation proved to be much needed notably after the hacking incident of July 2014 of the European Central Bank.

To further bolster the EU's cyber resilience, the EU Cyber Diplomacy Toolbox (Council Conclusions 10474/17) was put into effect in 2017 as part of the European approach to Cyber Diplomacy (Council Conclusions 6122/15) in the framework of its CFSP. Within the extensive legislative framework relating to cybercrimes of all kinds, the Council Regulation (EU) 2019/796 of May 2019 regarding limiting actions against cyber-attacks is worthy of mention because it veiled significant components of the Toolbox. A month earlier, the EU Cybersecurity Act (Regulation (EU) 2019/881) was added to the Union's cyber arsenal. It amended and reinforced the legal status and responsibilities of ENISA, while it introduced the European Cybersecurity Certification Framework with the aim of granting certification schemes for ICT products and services, including a bunch of principles, guidelines and technical prerequisites, which will lead to a safer and reliable digital environment. Furthermore, it established the Stakeholder Cybersecurity Certification Group (ibid art. 22) to enable the certification framework presented earlier.

After the supply chain attack which hit 6 EU agencies in 2019, European Union entered the 2020's with an eye to its digital future. The 2nd EU Cybersecurity Strategy (JOIN (2020) 18 final) was released in December 2020, illustrating 3 main key domains of action: a)*resilience, technological*

sovereignty and leadership, b)*building operational capacity to prevent, deter and respond* and, c)*advancing a global and open cyberspace through increased cooperation*. As cyber warfare was expanded in pivotal for humanity sectors, like the fight against coronavirus, the Union realized that it should shield its institutions in proportion to hybrid provocations of the modern era. Indeed, numerous Acts have been adopted concerning several domains such as AI, cryptography, roaming, data, chips, digital market, digital goods and services and more, in order to reach the goal of becoming and functioning digitally 100% by 2030[6]. This transition in tandem with the Union's ambition to reinforce its defence, especially after the Russian invasion of Ukraine in February 2022, resulted in the approval of a proposal for a Regulation (COM(2022) 349 final) on establishing the European Defence Industry Reinforcement through common Procurement Act (EDIRPA), to function as an ephemeral financial tool able to boost common mutual procurement among MS.

In drawing things to a close, the ongoing discussion regarding the EU's strategic autonomy, in combination with the cyber means that Russia uses in its aggression contra Ukraine, led to the release of the EU Policy on Cyber Defence on November 10, 2022, a document with a special focus on enhancing military and civilian cooperation in cyber crisis management (JOIN(2022) 49 final), upon the four general pillars of the Strategic Compass (act, secure, invest, partner) adapted in cyber issues. On the same date, the Commission introduced the Action Plan on Military Mobility 2.0 (JOIN(2022) 48 final) that will last until 2026 and will operate towards a more digital, rapid and effective mobile military network. It is conspicuous that the Union seeks to tailor its policies and take further measures to safeguard its citizens, considering the contemporary challenges.

3. Small States Theory

The European Union is comprised of a wide range of states, big and small, powerful and weak, all of them with their own unique dynamic. Small European states, which actually outweigh in number the great ones, contribute to Union's policy and decision-making procedures in any way possible, aiming to advocate their pivotal interests. More specifically, Greece and Estonia, are two different small states, with numerous diversifications (geographic position, capacities, economic indicators, social cohesion, and so forth) but with one thing in common; both of them invest heavily in the security and defence principle, despite the fact that they exist in different security environments. Eventually, being small does not mean being invisible.

[6]As presented in Commission's Digital Compass. Find out more here: https://commission.europa.eu/document/download/9fc32029-7af3-4ea2-8b7a-4cd283e8e89e_en?filename=cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

In a bid to study the role that Greece and Estonia play in the EU's cyber security and defence strategy, the starting point needs to be set; that of the definition of small states. In this chapter, the controversies around the concept of smallness are addressed, in order to answer the question: In what context are these case-studies considered small states?

3.1 Definition of smallness

It is true that academic scholars cannot find common ground as regards the definition of small states, employing various yardsticks depending on their perception. Pedi chooses the approaches method to present the disparate opinions about smallness(Pedi, 2016). She begins with the "I know one when I see one" method and continues with the quantitative criteria. The latter is rather a dubious approach because variables like population, sovereignty, political size, GDP, military capabilities, governance, soft power and others (Thorhallsson and Wivel, 2006), are difficult to be studied and counted in order to produce a regular and complete definition. She then juxtaposes the perceptions approach, i.e., the way global leaders and the leader of the state in question perceive its power. This concept highlights the importance of perceptions because they illustrate an image for each international actor(Wrange and Bengtsson, 2019), yet they may not be that objective and pragmatic. Perceptions are followed by the behavioral approach which alleges that it is a state's behavior (either as a natural characteristic or as the outcome of a bunch of elements) that defines it as small or big. For many scholars, a small state is a state with such determinate capabilities that it cannot have a strong presence in international affairs. As a result, its vulnerability generates insecurities that lead to a sub-category of this approach, the one that describes small states as "security consumers" who yearn for external aid from a great power (Pedi, 2016). In this context, it is probable to join an alliance in an effort to find shelter from its rivals (Bailes et al., 2016). Nonetheless, there are small states that perform strategies that upgrade them to economic powers, they "punch above their weight", become "small but smart", norm entrepreneurs (Corbett et al., 2019), status-seekers (Thorhallsson, 2018) or states-lobbyists(Grøn and Wivel, 2011).

On the other hand, all the more European scholars seem to adopt the relational approach when referring to smallness, underlining the element of comparison and emphasizing in power(Kurecic et al., 2017). In other words, smallness can be equalized with weakness in a given space and time, tangling the resources and interests' elements, thus providing a variety of outcomes that can lead to different definitions (Wivel & Baldacchino, 2022). Last but not least, Pedi stresses the concept of residual approach. This one encompasses the negative approach that names a state as small,

the one that it will not come into conflict with a great state, the one that it is unable to "*pursue dominant power politics"*.

3.2 In what context are Greece and Estonia considered small states?

The variety in criteria offers a variety of options regarding the circumscription of smallness, either by selecting one category or by making combinations. For the purpose of this thesis, there will be a mix of the approaches presented above, in particular those of perceptions, relational and residual. They were selected as the author considers that they will provide a more integrated and modern definition of small states, rather than the other ones, in order to answer the question posed at the beginning of the chapter.

To begin with, the "I know one when I see one" is not that representative, while the quantitative size cannot solely form the term of smallness because it is not sufficient and diversifies on a case – by – case basis. For instance, the population of Greece and Estonia rank under 10 million people (Worldpopulationreview.com, n.d.), yet they adhere to NATO's directive to devote at least 2% of national GDP to defence (Defence Statistics, 2022). Additionally, the behavioral concept is capable to describe the strategies that some states follow, without being able to provide a definition applicable to each and every scenario. Estonia for example, behaves like a leading state in cyber security issues and aspires to enhance its reputation in this field, in disproportion to its material capabilities and small size in numbers. Moreover, both of them are perceived by global leaders as small states of limited influence in the international scene, as well as in the EU. Even in the case of the Berlin talks for the Libyan crisis, Greece did not receive an attendance (Michalopoulos, 2020), despite the fact that the conflict is of utmost importance because of the MoU between Libya and Turkey which violates the Greek territory. As regards Estonia, it is recognized as a valuable MS due to its contribution to the cyber security sector, though it achieves more when "speaking in one voice" alongside Latvia and Lithuania (Wrange and Bengtsson, 2019).

As far as the relational approach is concerned, this is identified in the Union's regional subsystem. To put it in another way, the two case-studies are considered as small states within this territorial framework and in comparison to the other MS. They may be treated as even smaller or bigger powers at the regional and/or international level, however, their size in the EU exclusively is examined. Ultimately, as the residual approach countenances, neither Greece nor Estonia is possible to provoke offensive actions against their more powerful contenders. This argument can be supported by the alliance and shelter theories; both of them became EU MS and NATO allies in

order to advocate their highest national interests and protect their sovereignties from the insecurities that they suffer from (due to Turkey's and Russia's aggressive rhetoric), as small states. This is the primary goal of Athens and Tallinn that has led them to act in a unique style, proportionally to their material and diplomatic resources and national threats. Thorhallsson (2000) recognizes smallness as a vantage in adaptation procedures, while sets his speculation about the influence of small states upon larger ones. He mentions that small states' literature about security varies and clarifies the need for a better understanding of their role in integration. As a result, the need for further study upon each unique state arises. In the next two chapters, there will be examined to what extent Greece and Estonia support the Union's integration process in the field of cybersecurity and defence, emphasizing the analysis of their respective national strategic environment, their national cyber action-plans, and their contribution to European cybersecurity.

4. Greece

Greece counts 42 years as a member state of the European Union (*Treaty*, 1979). Its location in the South-eastern part of the European neighborhood (not the most peaceful region) and its internal troubles (mostly those related to its financial and migration crisis) have shaped an image of a country incompetent of dealing with its own difficulties(Papadopoulos & Fratsea, 2019; Pedi, 2017). This negative view indeed, has cost on its reputation and influence at regional, European and international levels. Despite that, Greece's credibility in the sector of security and defence cannot be doubted, since 3.9% of its 2021 GDP share was spent on military expenditure (SIPRI, n.d.), effectuating NATO's 2% defence spending requirement, a notable number for a small state. Furthermore, one of the five EU Operation Headquarters locates in the city of Larissa, with the purpose of drawing plans, managing, and monitoring operations conducted under the Petersberg Tasks framework (European Union External Action, 2021), highlighting the country's important strategic position.

Security and defence were dominant areas during the last two Presidencies of the Council of the European Union. In the first semester of 2003, one of the two priority areas concerned the reconstruction and integration process of the fragile Western Balkans (Ministry of Foreign Affairs, 2020). Their high level of criminality that could plague the EU due to the geographical proximity and their economic perspective (almost 50 million potential clients) constructed the main argument of assisting in any way possible (Bunse, 2009). It was then, that the first civilian ESDP mission EUPM in Bosnia and Herzegovina, and the first military ESDP operation CONCORDIA in North Macedonia were deployed. Just as importantly, another accomplishment of Greece was

marked in the course of its most recent Presidency in 2014, when the European Maritime Security Strategy was adopted; the first holistic and cross-sectoral approach to MS' security at sea (Ministry of Foreign Affairs, 2020). Overall, the country has a dynamic presence in the EU civilian and military projects, as it is the head state of seven out of eleven Battlegroups (Blavoukos and Politis-Lamprou, 2021) while it participates in seven active CSDP missions and operations (civilian and military) in the Balkan peninsula, Eastern Europe, the Mediterranean and Africa (Ministry of Foreign Affairs, 2017). The involvement in these actions represents Greece's direct and indirect national interests, as well as the ambition to build its brand name as a 'stabilizer' in the wider region. Far as cybersecurity is concerned, the augmentation of cyber-attacks against the country during the last couple of years, resulted in the realization of the severity of the situation and the need to address cyberthreats. Hence, it has developed its national strategy to a very satisfactory level; as reported by the Global Cyber Security Index[7] 2020 (International Telecommunication Union, 2021), Greece ranks 28th out of 194 countries worldwide in how committed it is to cyber policies. More specifically, the country gained this position after its actions and practices in five fundamental domains of cybersecurity were measured and evaluated by the Index: a)the establishment and enforcement of legal framework, b) the application of technical competencies, c) the establishment and implementation of national strategies and relevant organizations, d) the capability to implement capacity building such as raising awareness and instruction on cybersecurity issues and finally, e) the existing level of cross-border cooperation schemes and collaborations between private/public companies and states.

4.1 Strategic Environment

In geographic terms Greece's strategic environment is composed primarily by its national interests and those of its neighbors: the Balkan states, states in the eastern Mediterranean area, and those in the MENA region. At the moment, the supreme geopolitical goal is to safeguard its territorial integrity which is being constantly questioned by Turkey (Ifantis & Güvenç, 2022). Security dilemmas prevail on account of the perpetual revisionist narrative of Ankara against Athens, the violations of national airspace, the contestation of sovereignty rights in Greek Aegean islands, the illegal settlement in Northern Cyprus (ibid), and the Turkish-Libyan memorandum with which President Erdogan aspires to fulfill the doctrine of "Blue Homeland" infringing the Greek territorial waters (Ntousas, 2021). The ongoing civil war in Syria and the migration flows that have been begotten, especially in 2015,(Heisbourg, 2015) exacerbate the volatility. On the northern borders,

[7] A reliable resource that assesses states' commitment to global cybersecurity in order to highlight the significance and range of the problem.

Turkey's support of Albanian and Bosnian Muslims (Mazis and Troulis, 2020) affects as an inhibitor actor in Greece's strategy to further empower the Western Balkans towards their accession to the Union, and strengthen its status as a reliable partner that promotes peace and prosperity. Additionally, the war in Ukraine found Greece on the side of the defenders, confronting the energy insecurity, a condition that both European small and great powers are experiencing by dint of the EU's dependency on Russia's natural gas. In the existing non-conventional threat landscape, cyber-attacks are an extra type of hybrid aggression, that occasionally proved to cause greater and latent damage than the traditional ones. Table 4.1 illustrates a list of reported cyber incidents that have occurred in Greece and are worthy of mention.

Table 4.1 Indicative reported Cyber-attacks against Greece.

Date	Attribution	Target	Details
August 2022	The hacking group called "Ragnar Locker".	National Gas System Operator (DESFA)	Hackers conducted a cyber-attack in a part of DESFA's IT infrastructure and leaked data and documents. After that, Ragnar Locker claimed responsibility for this action (Toulas, 2022).
April 2022	-	Hellenic Post ELTA	A ransomware brought down the computer systems, suspending numerous services and causing delays in the external shipping of products, transactions, simple mailing, to name but a few. Albeit no sensitive data have been violated. The case is still under investigation(Jeremic, 2023).
January 2022	-	Greek Parliament	About 60 email addresses, including the legislature's web mail, were suspended for a short time because an exterior IP attempted to gain access to these accounts (ToVima Team, 2022).
January 2022	-	Sotiria and Asklipieio Voulas hospitals in the Attika region	Cyber blackmailers made use of the same ransomware of the attack against ELTA, and hit the servers of these two hospitals, without gaining access to private patient's data, but to information regarding visitors and invoices.

			Investigation is still ongoing (Jeremic, 2023).
July and September 2021	-	Municipality of Thessaloniki	The attackers displayed insulting messages on screens and released a few stolen documents after the denial of the officials to pay the requested ransom (Papadopoulos, 2022).
February 2021	-	Hellenic Defence Systems	150 computers of the Hellenic Defence Systems were attacked by a malware called Avaddon (via email phishing), which locked contracts, emails, and documents involving financial and legal information (Papadopoulos, 2022).
August 2020	A Turkish hacking group called "Akincilar".	The Hellenic Army General Staff and the Foundation for Research and Technology – Hellas (FORTH)	The cyber-attacks caused multiple strikes against servers linked to both institutions. In particular, websites ending in army.gr and forth.gr were shut down and pictures of the seismographic ship "Oruc Reis" were illustrated in the frontpages (Souliotis, 2020).
February 2020	A Turkish hacking group called "Anka Neferler".	Greek State Websites	According to Turkish media, the Anka Neferler hacking group targeted several governmental websites (such as those of the Ministry of Foreign Affairs, the Ministry of Finance, the Greek Parliament, the stock market, to name but a few). The attack corresponded the visit of the Libyan Marshal Khalifa Haftar to Athens(Papakonstantinou, 2020).
2018	A Turkish hacking group called "Akincilar".	Greek Ministry of Foreign Affairs and Greek News Agency	A Turkish group called "Akincilar" hacked the websites of the Ministry and news agency and published a recorded video of its action against the first target, as retaliation in opposition to the Greek government for not releasing the Turkish officers who have fled to the Greece's territory after the failed coup against President Erdogan in 2016 (Papadimitriou, 2018).

As presented in Table 4.1, that it is a compilation of information found in think-tank analyses, online magazines, and national newspaper articles and composed by the author for the purposes of this thesis, 2022 appears to be the most intense year, with remarkable number of cybercrimes in variable domains, while a rise in ransomware attacks with hackers demanding some cryptocurrency payout in some cases was observed (Papadopoulos, 2022, Jeremic, 2023), following the general trend. It is hardly surprising that plenty of these troubles are connected to Turkish hackers; the regional dispute has indeed passed in cyberspace as the tension between the two parties is escalating. However, the targets now may diversify and extend from the typical ones (public and military administration) to substantial for society infrastructure of services such as hospitals, the post office, and natural gas distributors. More particularly, the most recent strike against DESFA could be highly hazardous as: a) Greece tries to reduce its reliance on Russian natural gas, in the spirit of punishing Putin for his hostile invasion of Ukraine(Koutantou and Maltezou, 2022); causing harm in the energy system would make this effort much more difficult, and b)Prime Minister Mitsotakis and his government aspire for the country to transform into an energy hub to supply its needs and those of Europe with liquified natural gas, and become a mediator between North Africa and Central Europe, ameliorating its geopolitical stance in combination with the green transition (Lacqua, 2022).

4.2 In what way does Greece combat cyber threats?

In recent years Greece has increasingly sought to integrate a comprehensive approach in crisis management, where both the national military and political sectors shall evolve simultaneously, utilizing all the tools provided by the EU. As years went by, the decision-makers gradually recognized the significance of secure cyberspace, as information and communication technologies make the world more complex than ever. By and large, the country may have not experienced a large-scale cyber-attack such as the one Ukraine suffered from in 2017, yet the gravity and the rise of the facts demonstrated earlier gave a boost towards the adoption of countermeasures.

A year after the EU adopted its first Cybersecurity Strategy, the Cyber Crime Division as a branch of Hellenic Police (P.D. 178/2014) was founded, with the aim of impeding, scrutinizing, and ceasing crime and antisocial behaviour when they occur online or in other electronic media. In line with the initial NIS Directive the National Cyber Security Authority or NCSA was instituted (P.D. 82/2017), serving as the country's National Competent Authority for cybersecurity (N. 4577/2018). Furthermore, Greece substituted its 2016 Ministry of Digital Policy, Communication and Media with the "renovated" Ministry of Digital Governance in 2019 (P.D. 81/2019). Among its primary

goals is to promote the digital transformation of the public sector, simplify bureaucracy, unify digital policy with e-governance and citizens' services, and finally, improve interoperability at all levels. This conversion, in combination with the Covid-19 outbreak, increased the demand for widespread internet use for all activities, which generated the familiarity of Greek society with the Internet and the digital modernization of services. At the same time, an amplification in cyber-attacks was observed. The necessity of tackling these troubles in a more orchestrated way emerged especially after the Akincilar's attack in August 2020, at a tense moment for the Creek-Turkish relations due to the presence of the seismic vessel "Oruc Reis" in waters claimed by Greece (*Deutsche Welle*, 2020). As a result, in December 2020, Greece set into force its National Cyber Security Strategy 2020-2025; an updated version of 2017's cybersecurity strategy, that was drafted by the NCSA and outlined the strategic objectives goals, key-areas, rules, and other requirements for securing the civil, private, and critical infrastructure sectors, pursuant to ENISA. In other respects, another service connected to data, confidentiality of communication and security of grids, is the Hellenic Authority for Communication Security and Privacy – a.k.a. ADAE (N. 3115/2003). What is more, a crucial cybersecurity authority is the National Intelligence Service known as EYP, which is in charge of examining information in order to protect the country from espionage, terrorism, cybercrimes and any other threat against democracy, fundamental human rights, national security and territorial integrity. Moreover, EYP is the national CERT[8] or NCERT-GR (*RFC2350 - National CERT operation - nis.gr*, n.d.), yet it is not accredited by the TI[9]. The only CERT to be authorized since 2003, is the GRNET-CERT (n.d.) hosted by the National Infrastructures for Research and Technology. In the last six months EYP is quite "popular", due to its involvement in a data interception using the spyware Predator to gain access to mobile phones of politicians, journalists and entrepreneurs (Stamouli, 2022). Despite its cyber aspect, this case will not be further examined in this thesis as the investigation around it is still ongoing and it is a domestic matter, accusing and affecting individuals in the first place. This internal affair seems to have positively influenced the latest statute that was added to the Greek constitution regarding the topic. The law N. 5002/2022 concerns the declassification of communications, the optimization of EYP's action, the safeguarding of the privacy of communications from monitoring software, the enhancement of the national overall and operational cyber security, and the provision of the best citizens' protection against the processing of their personal data.

[8] Computer Emergency Response Team

[9] The European CERT community established the Trusted Introducer Service, often known as TI, in 2000 to meet shared needs and create a service infrastructure that would be essential to all security and incident response teams.

On a more practical level, in September 2010, Athens hosted one of the five preparatory workshops for the first Pan-European Cyber Security Exercise on Critical Information Infrastructure Protection (CIIP) "Cyber Europe 2010", supported by ENISA and the Joint Research Centre (ENISA, 2011), aiming to encourage cooperation among European countries in an effort to counter wide-ranging attacks. Except for that, this small state is the coordinator of two PESCO Projects regarding cybersecurity; the Cyber Threats and Incident Response Information Sharing Platform, and the One Deployable Special Operations Forces (SOF) Tactical Command and Control (C2) Command Post (CP) for Small Joint Operations (SJO) – (SOCC) for SJO (PESCO, n.d.). In 2022, the escalation of cyber-attacks against critical infrastructure and the conduct of cyber-attacks in the war in Ukraine have brought new means of coping with cyber risks, such as the creation of an autonomous operational system called Thorax that will be part of the Third Division of the Hellenic National Defence General Staff. The purpose is to use big data, artificial intelligence applications, and different types of algorithms to enable a central, hybrid system to filter the enormous amount of information that is available on a daily basis in order to isolate a threat and automate a response (Nedos, 2022). Besides this, the Technical Assistance and Information Exchange Instrument of the European Commission organized alongside the Greek Ministries of Foreign Affairs and Digital Governance a workshop on "The role of the EU's Cyber Ecosystem in the global cyber security stability", in Thessaloniki in June 2022 (ENISA, 2022a). The conference was initiated by the European Security and Defence College, ENISA and partners from the Western Balkans, offering room for a fruitful dialogue among experts and decision-makers of the regions represented. Actions like this, foster mutual trust and resilience, while assisting two strategic objectives of the EU and Greece: cyber security and integration of the Western Balkans. Last of all, the International Fair of Thessaloniki 2022 hosted ENISA for the first time, in order to assist the activities of the European Year of Youth 2022, intended to create a more inclusive and digital future and to raise awareness of cybersecurity skills and capabilities (ENISA, 2022b).

In winding up, Greece has made sundry steps towards the digitalization of society and has prioritized cybersecurity, in particular after the cyber-attacks of the last year and the sophisticated EYP scandal. However, there is an evident lack of cyber-culture which has prevented the establishment of successful and effective cyber policies and the correct implementation of the EU legal framework. So far, infrastructure has been largely unaffected by Turkish or other hackers strikes, leading to the conclusion that most cyber-attacks are conducted to terrorize rather than cause widespread damage. Albeit this does not prevent the Greeks from preparing for a potential

large-scale blow, starting with the cultivation of the idea of secure cyberspace and advanced technologies, an effort that is reflected in the last two events.

5. Estonia

As a Baltic state, Estonia was part of the Union's enlargement in 2004 (*Treaty*,2003), the largest one in terms of the number of countries, population, and domain. The country's turn to the West, resulting from the collapse of the Soviet Union, has established its strategic environment. Despite its smallness, this former Soviet state has managed to become a pioneer in the digital transition of Estonian society and a promoter of sustainability and green technologies (Estonian Convention Bureau, 2022), building its good reputation in the field of cybersecurity. An example worthy of mention is that Estonia was the first to conduct online voting in the local government council elections in 2005, as an alternative option to the traditional process (Madise and Martens, 2006). Nevertheless, the country has recognized the magnitude of active participation in cooperation blocks and alliances, especially with the existing international antagonism and the increasingly threatening Russian rhetoric over the past decade. For these reasons, the major parties in the government have agreed, since 2012, to bolster and preserve the national defence budget at a 2% GDP expenditure in order for long-term planning and effective use of taxpayer funds to be enabled (Ministry of Defence, 2022), which highlights the internal cohesion of the parliament in matters of security, an extremely important asset for any small state in terms of managing any crisis.

With the motto 'Unity through balance', Estonia assumed the Presidency of the Council of the European Union in 2017. In this six months period (EU2017EE, n.d.), among its key objectives that were accomplished with success was the agreement to reinforce further the eu-LISA (Proposal 2017/0145 (COD)), an EU Agency that generates a long-term solution for the operational management of large-scale IT systems which are crucial tools in the implementation of the EU's asylum, border control, and migration policies, which shall assist database interoperability[10]. At large, Estonia is a fervent supporter of the evolution of CSDP, as the EU is one of the leading guarantors of its security, stability and prosperity. According to the official websites of the Ministry of Foreign Affairs (2021) and the Estonian Defence Forces (2021), the country participates in 6 civilian missions and has joined 4 military operations orchestrated by the EU in Eastern Europe, the Mediterranean and the Horn of Africa. The conclusions to be drawn by this kind of engagement illustrate partially its areas of interest, nonetheless, this does not decrease the country's primary goals to maintain and ameliorate its cybersecurity, especially when it received

[10] This procedure led to the implementation of Regulation (EU) 2018/1726 a year later.

2,237 incidents with impact in 2021 (Information System Authority, 2022). The Global Cyber Security Index 2020 has put Estonia in the third place (International Telecommunication Union, 2021) out of 194 included states, bringing this small power to the spotlight to the extent that it is devoted to cyber policies. It appears that this Baltic state excels at the five key sectors set by the Index, which were mentioned earlier at the end of the introductory part of Greece.

5.1 Strategic Environment

Placed close to St Petersburg and Kaliningrad and surrounded by the Gulf of Finland, the Baltic Sea and the Gulf of Riga, Estonia locates between a bunch of small states with whom it embraces the western culture (in politics, economy and more) and a great, revisionist power, Russia. The traditional historical linkages with its eastern neighbor, in conjunction with the Russian ethnic minority that constitutes 23,7% of the total population (Statistics Estonia, 2022), explain, yet not justify by some means Putin's ambitions to regain his state's influence and interference towards former Soviet lands. The most direct territorial threat against Estonia so far was the military drills within spitting distance from the borders that simulated a missile attack against Estonia's grounds in June 2022(BNN, 2022). However, the state has experienced various unconventional threats, such as the illegal migrants from Belarus last year, who are believed to be a weaponizing method of the Kremlin aiming to provoke instability in the countries of the former USSR (BNS, ERR News, 2021). Furthermore, the war in Ukraine has begotten serious security threats related to the number of refugees (by the middle of June there were some 43,000 reported Ukrainians) and the notable impact on the economy (Foresight Centre, 2022), and the way these two will affect Estonian society as far as the Russian population is concerned. Tackling disinformation and propaganda (Hardy, 2021) is among the state's strategic priorities, due to the mighty effect that Russian media have on the Estonian Russophones, intensifying ethnic chasm, and deranging social cohesion, thus inflicting blows to its resilience – particularly when in turmoil times (Duxbury, 2022). National and European officials and experts (Bendel, 2018) consider hybrid threats in all of their guises to be more perilous for the country, especially in the aftermath of the frozen conflicts of Georgia (2008) and Ukraine (2014). For instance, the most remarkable cyber-attack of the state, which is a type of irregular violence, is connected to ethnic differences; the Bronze Night which will be examined in the next lines. In Table 5.1 that follows, some severe cyber strikes are presented in order for the merit of cybersecurity for Estonia to be fully highlighted. It should be mentioned that this table has been synthesized by the author, too. The findings of the research on

the incidents were spotted primarily in scholarly reports and online articles in magazines and national newspapers.

Table 5.1 Indicative reported Cyber-attacks against Estonia.

Date	Attribution	Target	Details
August 2022	Pro-Kremlin cyber group Killnet	Public and private institutions and companies	A malware infected 24 websites and 137 devices and internet service suppliers. Numerous DDoS attacks were conducted against public and private sector's organizations, services and enterprises, achieving limited impact. Moreover, some phishing hits were indicated (Wright, 2022b).
May 2022	-	The Estonian Ministry of Foreign Affairs	The Ministry of Foreign Affairs' website suffered DDoS blocking attacks for a couple of hours, yet the shutdown did not affect other parts of the ministry's functions(Wright, 2022a).
April 2022	Pro-Kremlin cyber group Killnet	Estonian State Websites	Hackers attempted to break down the websites of the President, the Ministry of Foreign Affairs, the train company Elron, to name but a few, using DDoS. In particular, as RIA's director stated, some 75 million queries strove to overload the portals, a tremendous number (Whyte, 2022).
July 2021	-	Information System Authority (RIA) database	A hacker managed to infringe RIA's system and obtain illegally Individuals' 286,438 personal data (ID codes, personal names and pictures) using a malware network (Whyte & Wright, 2021).
November 2020	-	Three Government Ministries	The Ministry of Economic Affairs and Communications (2020), Ministry of Foreign Affairs and Ministry of Social Affairs were hit; serious intrusions of private data were reported.
April 2007	Sergey Markov and his associates, Konstantin Goloskokov and	Estonian public and private institutions' servers(Cfr, 2007)	"The Bronze Night" i.e., the riots regarding the relocation of a Red Army war monument led to numerous Denial-of-Service strikes (such as DDoS, DNS, mass e-mails, spam comments and more) lasted for 22 days. These aggressive cyber actions

	his associates from Nashi, and Dmitriy Galushkevich		were orchestrated by Russia , paralyzing administrative (parliamentary and ministerial servers), banking, media and public services' computer systems, as well as private enterprises' websites and communications (Samsoerizal et al., 2022). The landscape is quite murky as to who organized and carried out the attacks; experts have identified some of the evidence with the statements of Markov and Goloskokov.

It is evident that there is a reduced number of cyber incidents, compared to Greece's, which is tangible proof of the high-quality shielding of Estonia's hardware and software systems. Nevertheless, the cyber-attacks that it has suffered from unveil the fact that conventional threats can be transferred in cyberspace as well. By way of illustration, the event of April 2007 against critical infrastructure that was provoked after the "Bronze Night" upheaval(Koeller, 2015), was a clear endeavor of Russia to regain influence and power towards former Soviet states, even more after the Baltic states accessed the EU and NATO in 2004, with any possible means. Following Moscow's invasion of Ukraine in February of last year, Tallinn, Riga and Vilnius constitute a frontline in the cyberwar between European countries and Russian hackers. Putin's ambition to reshape the regional landscape has been reinforced by the increasing cyberthreats against Estonia (and other states) such as the one of August 2022 (Wright, 2022b) that was conducted in order to cause damage and distort Estonia's digital credibility at national and European level, in a very turbulent time. It is probable that Killnet wanted to produce a shockwave similar to that of 2007 because this cyber-attack was followed by the removal of the Soviet T-34 tank from the city of Narva; though there was not such social reaction compared to that of "Bronze Night". As far as the attack of April 2022 is concerned, it was not a coincidence(Whyte, 2022); the strikes occurred on the last two days of NATO's international cyber defence exercise "Locked Shields", hosted by Estonia, and continued for three more days. This is a sample of the confrontation of two great powers, the US and Russia, and it can be assumed that this was a well-organized action in order to create feelings of dread inside the coalition.

5.2 In what way does Estonia combat cyber threats?

Being a small state in the West, Estonia faces a variety of threats, all of them plugged into Russia in a way, while it heavily relies on the collective defence concept of the EU and NATO. Despite the

lack of material capabilities, the country excels in cybersecurity and has created this brand name, “punching above its weight”, i.e. overcoming its smallness (Wivel and Crandall, 2019). It has a long history in the digital sector that dates back in the 1990s (EAS, n.d.), and since then it functions online from head to toe. The 99% of public services are also in online mode, providing its citizens a high quality of life in its smart cities (Borge et al., 2022). Nevertheless, on the way to success, e-Estonia has been the victim of several cyber-attacks which have gradually strengthened its cyber defence in contemporary hybrid warfare.

The 2007 cyber-attack appears to have redirected national politics and since then, Estonia is constantly seeking to evolve its cyber practices and act proactively to enhance its resilience. In the aftermath of this incident, the country adopted the first Cyber Security Strategy document in 2008, which has been updated twice. At the present day, the 2019-2022 document is in force. It is a horizontal approach towards cybersecurity that specifies the key priorities and long-term goals in the domain (Ministry of Economic Affairs and Communications, n.d.), always in accordance with the guidelines of ENISA. The main purpose is to include the public and private sector and academics in order to provide the circumstances for a more thorough and well-orchestrated sectoral action plan, which will engender a cyber-literate society. What is more, the Digital Agenda 2030 (Ministry of Economic Affairs and Communications, 2021) and its three sub-objectives (digital government, connectivity and cybersecurity) are an additional strategic tool aiming to designate the country as an international leader in cybersecurity, which offers high-quality services both to its citizens and to the states with whom it cooperates while strengthens its business and investment value, as well as research. The two official papers have been drafted by the Estonian Ministry of Economic Affairs and Communications, the national ministerial institution responsible for cybersecurity and digital affairs. This constant evolution in the national legal framework represents the solemnity with which the concept of cyberthreats is being treated, as they are carried out using increasingly advanced technology. It is crystal clear that the country pursues to be prepared to manage any challenge, originating from other international actors that have proved to perform cyber strikes, like China, especially after its drop-out of the 17+1 initiative in last August (Lau, 2022).

Moreover, the Cybercrime Unit (C3) in the Central Criminal Police and Border Guard Board (Krusten, 2019) is a supplementary body that operates in the detection of menace and investigations of cybercrimes, while it contributes to the prevention and the legal framework. An additional institution that functions since 2011, under the authority of the Ministry of Economic

Affairs and Communications is the Information System Authority known as RIA (Määrus nr28. RT I, 28.04.2011, 1). It has been structured to monitor reliable e-elections, handle the state Internet network and provide citizens with critical state information by running the State Portal eesti.ee, with the intention to establish a powerful Estonian digital identity with international use. Being a competence hub, RIA publishes the "Cyber Security in Estonia" (Information System Authority, 2022) assessment on an annual basis (as well as other relative documents on a monthly basis), accentuating some major moments and crises in the Estonian cyber world and RIA's measures to preserve cybersecurity. Moreover, as the authority was observing the rise in cyber incidents, it designed its 2021-2025 Strategy to expedite the practice of the Digital Agenda 2030 (Information System Authority, n.d.) . Last but not least, another key-responsibility of RIA is the management of CERT-EE (n.d.) that established in 2006 with the purpose of mitigating potential harm from cybersecurity threats, while reporting. Forsooth, the cyber-attacks in Ukraine (notably in 2017), the deteriorating regional and international security situation of the previous decade and the country's Presidency of the Council of the EU, assisted Estonians to comprehend deeper that cyberthreats were not a theoretical risk and that they had to further improve and expand their cyber defence mechanisms. As a result, the Cybersecurity Act introduced in 2018 (Seadus RT I, 22.05.2018, 1) for the purpose of maintaining crucial to society's function information and network resources-especially the systems of the public sector, and the principles of accountability and oversight, obviation and remediation of cyber-incidents. In an effort to further protect the data, the Estonian government invented the first in the world Data Embassy in Luxembourg in 2015, a system of servers under its management yet beyond its borders (Digital Luxembourg, n.d.).

Without a doubt, there are many arguments regarding the reason Estonia is such an advanced state in cybersecurity, and yes, the plethora of legal frameworks is one of them – especially considering its small size. However, as cyberthreats impact societal security, the state considers its citizens' consciousness to be paramount and despite their familiarity with the digital world (the list of e-services fluctuates from e-health and e-ID cards to childcare, it is frankly endless), it continues to highly invest in raising awareness. Hence, the Centre for Digital Forensics and Cyber Security delivers informal training programs to students of primary education, as an affixing to their curricula (Toome, 2022), while high school students have the opportunity to participate in competitions such as the Cyber Battle of Estonia that simulates cyber-attacks and counter-hacking methods (CTF Tech, n.d.). Another worth-mentioning organization (non-governmental) is the e-Estonia Briefing Centre that offers workshops and trainings to external partners on cybersecurity

since 2009 (e-Estonia, n.d.). This cyber-culture of the country can also be reflected in its advanced cyber enterprises (like Cybernetica, CybExer, Guardtime and more), and activities such as the organization of the annual conference "Tallinn Digital Summit" (n.d.) in which politicians, experts and entrepreneurs are brought together to address the topic of its year. On top of that, the cyber-attack of 2007 that changed Estonia once and for all, generated the urgency to safeguard Estonian cyberspace to a great extent, that the Estonian Defence League's Cyber Unit (Kaitseliit, n.d.) was established that year. It is a nonprofit organization that consists of cyber experts that operates as a supporting tool for civil services and vital facilities, in line with the national cybersecurity strategy.

Estonia highlights at every opportunity the role of the EU in combating cyberthreats and contributes to the Union's endeavor in any way. This is exemplified by the influence it has exercised in a European ministerial meeting, organized in Tallinn by the Ministry of Economic Affairs and Communications, to put the EU's valuable data infrastructure protection strategy into action (Tiirmaa-Klaar, 2010). Besides that, there are indications that the EU's Internal Security Strategy of 2010 incorporated Estonia's views as regards cybersecurity and society's vulnerability to confront cybercrimes (Czina 2013). In addition, this small state is the leading state of the PESCO project "Cyber Ranges Federations (Crf)", while it also participates in the "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)" project (PESCO, n.d.). In May 2010, Tallinn was the host city of the third preparatory workshop of the first pan-European Cyber Security Exercise on Critical Information Infrastructure Protection (CIIP) "Cyber Europe 2010", supported by ENISA and the Joint Research Centre (ENISA, 2011). Finally, yet importantly, the Estonian e-Governance Academy is responsible for the implementation of the "EU Support to Strengthen Cyber Security in Ukraine" project, aiming to safeguard data exchange and public infrastructure and repel cyberthreats during and in the aftermath of the war (EU4Digital, 2022).

To sum up, this small Baltic state is rightfully considered as one of the most advanced countries in cybersecurity in the world. It has established a cyber-culture from an early stage and has developed innovative mechanisms that fit its size; this is why they are successful. Without a doubt, the cyber-attacks of 2007 were determined for the evolution of the domain in the state, but up to a point. Tallinn has never stopped receiving offensive actions on its cyber ecosystem and therefore, it has no other option than to continue to boost its cyber defence tools. Its bigger rival, Russia, implements an unpredicted strategy that contains any available weapon, conventional and

hybrid, to accomplish its goals. Therefore, Estonia should be always ready to fight at all levels, and notable in cyberspace.

6. Conclusions

In a nutshell, in this thesis, the cyber security and defence strategy of Greece and Estonia was examined, considering them as small states of the European Union. After the analysis of the EU's cybersecurity strategy and the definition of the term "small states" by the author, Chapters no4 and no5 followed to present the case-studies' practices and action plans, in line with their respective strategic environment and experience in cyber-attacks. The cognizance that was taken from this study could lead to the conclusion that they could be described as reliable partners inside the EU and in NATO due to their level of commitment in security e.g. by having participated in numerous CSDP missions and operations and, by devoting at least 2% of the national GDP on defence expenditure (SIPRI, n.d.). These may be just two small member states among the rest 25, yet they have proven their value as security guarantors, notably if the instabilities and hybrid and non-hybrid risks in their regional sub-systems are to be taken into consideration.

There is no question that a discrepancy between them can be viewed with the naked eye, which stems mainly from Greece's delay to implement its cyber policies and draft a strategy. On the contrary, Estonia has initiated its digital transformation since its independence from the then USSR in 1991, in order to reconstruct the country as a whole and at the same time to be modern and attractive. As an illustration, the government opted in 1994 to devote 1% of GDP to IT infrastructure and a couple of years later the online banking system was launched (EAS, n.d.). Therefore, the citizens have begun to interact inside the digital environment from an early stage and adapted easier to the e-Tax and e-ID of 2000 and 2001 respectively (ibid). By all means, the cyber-attacks of 2007 caught it by surprise, but this generated the willingness to further boost the state's resilience towards cyberthreats. This decision to actually benefit from the risks in cyberspace was a clever one because this put Estonia in the epicenter of cybersecurity. It "punched above its weight" in spite of its limited resources as a small power in the international system (compared to those of the great powers). Greece on the other hand, has never undergone such a large-scale strike; the cyber incidents are conducted more as a propaganda tool. Its cyber policies have been developed mostly during the last 7-8 years and there is still room for improvement, in the transition of public services to online mode particularly. The progress so far is encouraging, nonetheless, the concept of cybersecurity shall be approached in a more cohesive way, in order to prepare the critical infrastructure properly, before a massive cyber-attack. In the

course of digitalization, it should be noted that Greece can learn from Estonia, but it is essential not to copy its policies and actions, but rather try to tailor them in proportion to its size, its capabilities. Raising awareness, as it has already started to perform, is the first step in society's embracement of cyber policies like digital governance, which will result in the evolution of digital culture.

At this point, it is worth mentioning that the differences between the case-studies are also spotted in their level of conformity with the European strategy on the topic. To be more precise, Estonia has set into force a distinctly greater number of laws and legal documents that are linked to the Union's cyber legislation, than Greece. The reasons may be quite evident; Estonia has a kind of "tradition" on cyber issues that emanates from the beginning of its restoration as a post-soviet democracy back in the 1990s. Furthermore, the cyber-attacks of 2007 brought to the surface technical weaknesses, but at the same time they became the starting point for the adoption of its first national Cyber Security Strategy in 2008 (Cyber Security Strategy Committee, 2008). Thenceforth, cyberthreats remain a matter of high priority in Tallinn's agenda. In spite of its small size, it has managed to influence the EU plenty of times, namely, in establishing a European strategy concerning the shielding of the European facilities and systems of substantial information(Tiirmaa-Klaar, 2010). Another case in point is the responsibility that Estonia has in the execution of the project "EU Support to Strengthen Cyber Security in Ukraine"(EU4Digital, 2022) which is ongoing. The Union has constructed a fiduciary relationship with this small Baltic state, which proves that even smaller powers can become "leaders" in specific fields.

With respect to Greece, it has not suffered from a devastating cyber-attack like Estonia. Thus, there was no special need for Athens to establish cyber law from an early stage, notably if its financial troubles and its territorial threats are to be added to the equation. However, the country has seen a rise in cyber incidents against it and as its experts observe the geopolitical shifts, it has started gradually to apply the EU's practices such as by introducing its first Cyber Security Strategy in 2017 (four years after the launch of the first European document of its kind) (Ministry of Digital Policy, Telecommunications and Media, 2018) and by integrating the NIS Directive on its national law (P.D. 82/2017) via the establishment of the National Cyber Security Authority. In addition, during the recent years, it appears that it has recognized the importance of cybersecurity and that it is a part of its national security. As a result, it is possible to notice in the near future that Greece will emphasize more in this field in its domestic affairs and as far as the European action plan is

concerned because it is paramount to evolve its defence capacities and reliability inside any cooperation scheme that excludes its biggest rival, Turkey (Karyoti, 2022).

It is crystal clear that Greece adapts slower to the digital environment than Estonia. Both of them are small states and EU and NATO members, yet their smallness has a different impact on the path that they follow. While their strategic environments differentiate, so their needs and priorities do. As a consequence, the implementation of the Union's practices and the transformation of their national law according to the European legal framework varies too. Thus, the outcome that provokes is that it is more a matter of prioritization, which will produce expertise and experience that will then engender an image, a brand name like the one of Estonia because cybersecurity is a quite modern sector that has room for plenty of progress and simultaneously, its demands are more limited than those of the regular material defence systems(Myatt, 2021).

The menaces of cyberspace are real and present more than ever before. The war in Ukraine (Bateman et al., 2022) introduces for the first time the wide use of information-based weaponry in a traditional conflict environment. Russia's tactics to hit Ukrainian grids may have appeared not that successful, yet this does not exclude the exercise of these unconventional armaments in future warfare. Therefore, it is of paramount importance for the EU per se and for its MS to be fully capable of combating any peril to come. This is crucial because even in the success story of Estonia, there is still a belief that all the three Baltic powers accomplish more when they act as one. Security and defence will never cease to concern both the state and non-state actors. As long as systemic threats exist, small states like Greece and Estonia can operate wisely and apply smart strategies in order to increase their influence and in the end of the day, serve their prior national interests. This is the only way for them to survive inside the anarchic and antagonistic international system. There is no doubt that cyber security and defence is a matter that will concern all the more as the years go by, and even the smaller powers will begin to pay attention and orchestrate their strategies.

7. Table of Legislation

7.1 Estonian Legislation

Määrus nr 28. RT I, 28.04.2011, 1.
Seadus RT I, 22.05.2018, 1.

7.2 Greek Legislation

N. 3115/2003 FEK A' 47/27.2.2003.
N. 4577/2018 FEK A' 199/03.12.2018.
N. 5002/2022 FEK A' 228/A/9.12.2022.
P.D. 178/2014 FEK A' 281/31.12.2014.
P.D. 82/2017 FEK A' 117/10.08.2017.
P.D. 81/2019 FEK A' 119/08.07.2019.

7.3 EU Legislation

Treaty between the Kingdom of Belgium, the Kingdom of Denmark, the Federal Republic of Germany, the French Republic, Ireland, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the United Kingdom of Great Britain and Northern Ireland (Member States of the European Communities) and the Hellenic Republic concerning the accession of the Hellenic Republic to the European Economic Community and to the European Atomic Energy Community,(1979), OJ L291:9–192.

Treaty between the Kingdom of Belgium, the Kingdom of Denmark, the Federal Republic of Germany, the Hellenic Republic, the Kingdom of Spain, the French Republic, Ireland, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Portuguese Republic, the Republic of Finland, the Kingdom of Sweden, the United Kingdom of Great Britain and Northern Ireland (Member States of the European Union) and the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia, the Slovak Republic, concerning the accession of the Czech Republic, the Republic of Estonia, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic to the European Union, (2003), *Official Journal* L236:17–930.

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, (1997), *Official Journal* C 340, pp. 9-16.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, (2007), *Official Journal* C 306, pp. 34-38.

Treaty on European Union, (1992) , *Official Journal of the European Communities* C 191, pp. 4, 104-108.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L194/1.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). OJ L333: 80–152.

Council decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and Determining the list of participating Member States. OJ L 331:57–77.

Council Decision (CFSP) 2021/509 of 22 March 2021 establishing a European Peace Facility, and repealing Decision (CFSP) 2015/528. OJ L 102: p. 14–62.

Council Conclusions 6122/15 on Cyber Diplomacy.

Council Conclusions 10474/17 on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

Council of the European Union 15585/14 EU Cyber Defence Policy Framework.

Council of the European Union 14413/18 EU Cyber Defence Policy Framework (2018 update).

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. OJ LI129/1:1–12.

JOIN(2013) 1 final. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe And Secure Cyberspace.

JOIN(2020) 18 final. Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade.
JOIN(2022) 48 final. Joint Communication to the European Parliament and the Council. Action plan on military mobility 2.0.
JOIN(2022) 49 final. Joint Communication to the European Parliament and the Council. EU Policy On Cyber Defence.
Proposal for a REGULATION COM(2022) 349 final OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the European defence industry Reinforcement through common Procurement Act.
Proposal 2017/0145 (COD) for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L119: 1-88.
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). OJ L151: 15–69.
Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). OJ L077:1-11.
Publications Office of the European Union (2017) *Petersberg tasks, EUR-Lex*. European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM%3Apetersberg_tasks (Accessed: February 12, 2023).

8. References

Ardagna, C. et al. (2022) *ENISA Threat Landscape 2022*. rep. ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport(Accessed: February 12, 2023).
Bailes, A.J., Thayer, B.A. and Thorhallsson, B. (2016) "Alliance theory and alliance 'shelter': The complexities of Small State Alliance behaviour," Third World Thematics: A TWQ Journal, 1(1), pp. 9–26. Available at: https://doi.org/10.1080/23802014.2016.1189806 .
Bateman, J., Beecroft, N. and Wilde, G. (2022) *What the Russian invasion reveals about the future of Cyber Warfare*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 (Accessed: February 12, 2023).
Bendel, J. (2018) *Estonia's Security: A Case Study of Internal and External Perceptions*. MA Thesis. Lund University.
Blavoukos, S. and Politis-Lamprou, P. (2021) "Executive Summary – The 'Magnificent Seven' of European Defence Integration." Athens. Available at: https://www.eliamep.gr/en/publication/%CF%83%CF%85%CE%BD%CE%BF%CF%80%CF%84%CE%B9%CE%BA%CE%AE-%CE%AD%CE%BA%CE%B8%CE%B5%CF%83%CE%B7-%CE%B1%CE%BC%CF%85%CE%BD%CF%84%CE%B9%CE%BA%CE%AE-%CE%BF%CE%BB%CE%BF%CE%BA%CE%BB%CE%AE%CF%81%CF%89%CF%83/ (Accessed: February 12, 2023).
BNN (2022) "Russia imitates missile attacks on Estonia during military drills," *Baltic News Network*, 22 June. Available at: https://bnn-news.com/russia-imitates-missile-attacks-on-estonia-during-military-drills-235690 (Accessed: February 12, 2023).
BNS, ERR News (2021) "Estonia has caught 5 illegal immigrants from Belarus," *ERR.ee*, 11 November. Available at: https://news.err.ee/1608399215/estonia-has-caught-5-illegal-immigrants-from-belarus (Accessed: February 12, 2023).
Borge, R., Brugué, J. and Duenas-Cid, D. (2022) "Technology and democracy: The who and how in decision-making. the cases of Estonia and Catalonia," *El Profesional de la información*, 31(3). Available at: https://doi.org/10.3145/epi.2022.may.11 .
Bunse, S. (2009) 'The 2003 Greek Presidency: Internal Market and Foreign Policy Priorities

and Achievements.' *Small states and EU governance.* New York: Palgrave Macmillan., pp. 162-181.
Cambridge Dictionary (n.d.) Hacktivism, Cambridge Dictionary. Cambridge University Press 2023. Available at: https://dictionary.cambridge.org/dictionary/english/hacktivism (Accessed: February 12, 2023).
Carrapico, H. and Farrand, B. (2020) "Discursive continuity and change in the time of covid-19: The case of EU cybersecurity policy," *Journal of European Integration*, 42(8), pp. 1111–1126. Available at: https://doi.org/10.1080/07036337.2020.1853122.
Carnegie Endowment (n.d.) *Timeline of cyber incidents involving financial institutions*, *Carnegie Endowment for International Peace*. Carnegie Endowment. Available at: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide (Accessed: February 12, 2023).
CERT-EE (n.d.) *Trusted Introducer : Directory :CERT-EE*. Available at: https://www.trusted-introducer.org/directory/teams/cert-ee.html (Accessed: February 12, 2023).
Cfr . 2007. *Connect the dots on state-sponsored cyber incidents - estonian denial of service incident*, *Council on Foreign Relations*. Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/estonian-denial-service-incident (Accessed: November 17, 2022).
Cimpanu, C. (2021) "SolarWinds hack affected six EU agencies," *The Record*, 15 April. Available at: https://therecord.media/solarwinds-hack-affected-six-eu-agencies/ (Accessed: February 12, 2023).
Corbett, J., Xu, Y.-chong and Weller, P. (2019) "Norm entrepreneurship and diffusion 'from below' in international organisations: How the competent performance of vulnerability generates benefits for Small States," Review of International Studies, 45(04), pp. 647–668. Available at: https://doi.org/10.1017/s0260210519000068 .
Crandall, M. and Varov, I., 2016. "Developing status as a small state: Estonia's foreign aid strategy," *East European Politics*, 32(4), pp. 405–425. Available at: https://doi.org/10.1080/21599165.2016.1221817 .
CTF Tech (n.d.) *Cyber Battle of Estonia 2021*, *CTF Tech*. CTF Tech. Available at: https://www.ctftech.com/cboe2021/ (Accessed: February 12, 2023).
Cyber Security Strategy Committee (2008) *Cyber Security Strategy*. rep. Ministry of Defence. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (Accessed: February 12, 2023).
Czina, V. 2013. 'Small State Influence in the European Union: The Case of 'E-Stonia.' Master of Arts Thesis. Central European University.
Defence Statistics.2022. *Finance and economics annual statistical bulletin: International defence 2022*, *GOV.UK*. Available at: https://www.gov.uk/government/publications/international-defence-expenditure-2022/finance-and-economics-annual-statistical-bulletin-international-defence-2022 (Accessed: February 12, 2023).
Digital Luxembourg (n.d.) *Data Embassy*, *Digital Luxembourg*. Available at: https://digital-luxembourg.public.lu/initiatives/data-embassy (Accessed: February12, 2023).
Duxbury, C. (2022) "Estonia fights back against pro-Russia messaging," *Politico*, 23 March. Available at: https://www.politico.eu/article/estonia-fight-back-pro-russia-propaganda/ (Accessed: February 12, 2023).
Deutsche Welle (2020) "Turkish gas exploration ship leaves contested waters," 13 September. Available at: https://www.dw.com/en/turkey-greece-mediterranean-dispute/a-54912476 (Accessed: February 12, 2023).
EAS (n.d.) *Story - e-estonia*, *e-Estonia*. EAS. Available at: https://e-estonia.com/story/ (Accessed: February 12, 2023).
EMA (2021) *Cyberattack on EMA - Update 6 , European Medicines Agency Sciences Medicines Health* . European Union. Available at: https://www.ema.europa.eu/en/news/cyberattack-ema-update-6 (Accessed: February 12, 2023).
ENISA (2011) *Cyber Europe 2010 – Evaluation Report*. rep. ENISA. Available at: https://www.enisa.europa.eu/publications/ce2010report/@@download/fullReport (Accessed: February 12, 2023).
ENISA (2022a) *Successful conclusion to the 3 Day Workshop: The role of the EU's Cyber Ecosystem in the Global Cyber Security Stability*, *ENISA*. Available at: https://www.enisa.europa.eu/news/enisa-news/successful-conclusion-to-the-3-day-workshop-the-role-of-the-eu2019s-cyber-ecosystem-in-the-global-cyber-security-stability (Accessed: February 12, 2023).
ENISA (2022b) *Enisa joins International Fair of Thessaloniki to promote cybersecurity skills*, *ENISA*. Available at: https://www.enisa.europa.eu/news/enisa-joins-international-fair-of-thessaloniki-to-promote-cybersecurity-skills (Accessed: February 12, 2023).
e-Estonia (n.d.) *The e-Estonia Briefing Centre is at your service*, *e-Estonia*. EAS. Available at: https://e-estonia.com/briefing-centre/about-us/ (Accessed: February 12, 2023).
Estonian Convention Bureau (2022) *Estonia – Sectoral Strengths & Areas of excellence*,

Estonian Convention Bureau. Available at: https://www.ecb.ee/destination/estonia-sectoral-strengths-areas-of-excellence/ (Accessed: February 12, 2023).

Estonian Defence Forces (2021) *Operations abroad*. Estonian Defence Forces. Available at: https://mil.ee/en/defence-forces/operations-abroad/#t-operations-since-1995 (Accessed: February 12, 2023).

European Commission (n.d.) *Sanctions adopted following Russia's military aggression against Ukraine*, *Finance*. European Commission. Available at: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en (Accessed: February 12, 2023).

European External Action Service (2016) *Shared vision, common action A stronger Europe : a global strategy for the European Union's foreign and security policy*. rep. Publication Office of the European Union. Available at: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (Accessed: February 12, 2023).

European Union External Action (2021) *Multinational Joint Headquarters Ulm; experts for EU Crisis response capability*, *Multinational Joint Headquarters Ulm; Experts for EU Crisis Response Capability | EEAS Website*. European Union External Action. Available at: https://www.eeas.europa.eu/eeas/multinational-joint-headquarters-ulm-experts-eu-crisis-response-capability_en#top (Accessed: February 12, 2023).

Eurostat (2022) *Population change - Demographic balance and crude rates at national level*, *Eurostat*. European Union. Available at: https://ec.europa.eu/eurostat/databrowser/view/demo_gind/default/table?lang=en (Accessed: February 12, 2023).

EU2017EE (n.d.) *The results of the Estonian Presidency of the Council of the European Union*. rep. Estonian Presidency of the Council of the European Union. Available at: https://www.consilium.europa.eu/media/56239/2017-jul-dec-ee-results.pdf (Accessed: February 12, 2023).

EU4Digital (2022) *EU supports cybersecurity in Ukraine with over €10 million*. EU4Digital. Available at: https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/ (Accessed: February 12, 2023).

Foresight Centre (2022) *The Long-term Impact on Estonia of the War between Russia and Ukraine*. rep. Foresight Centre. Available at: https://arenguseire.ee/wp-content/uploads/2022/06/2022_the-long-term-impact-on-estonia-of-the-war-between-russia-and-ukraine_report_summary.pdf (Accessed: February 12, 2023).

Grnet-Cert (n.d.) *Trusted Introducer : Directory : GRNET-CERT*. Available at: https://www.trusted-introducer.org/directory/teams/grnet-cert.html(Accessed: February 12, 2023).

Grøn, C.H. and Wivel, A. (2011) "Maximizing influence in the European Union after the Lisbon Treaty: From Small State Policy to smart state strategy," *Journal of European Integration*, 33(5), pp. 523–539. Available at: https://doi.org/10.1080/07036337.2010.546846 .

Hardy, A. (2021) *Securing e-Estonia: Challenges, Insecurities, Opportunities*. Doctor of Philosophy. Royal Holloway, University of London. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4155377 (Accessed: February 12, 2023).

Heisbourg, F. (2015) "The strategic implications of the Syrian refugee crisis," *Survival*, 57(6), pp. 7–20. Available at: https://doi.org/10.1080/00396338.2015.1116144 .

Ifantis, K. and Güvenç, S. (2022) *EU Conditionality: A Sustainable Framework for Good Neighborly Relations between Turkey and Greece?* rep. Stiftung Wissenschaft und Politik (SWP).Available at: https://www.globacademy.org/download/avrupanin-guvenlik-goc-ve-siginma-sistemine-bir-partner-ve-zorluk-olarak-turkiye-m-murat-erdogan-ve-markos-papakonstantis/# (Accessed: February 12, 2023).

Information System Authority (2022) *Cyber Security in Estonia 2022*. rep. Information System Authority. Available at: https://www.ria.ee/en/media/1490/download (Accessed: February 12, 2023).

Information System Authority (n.d.) *Ria strateegia 2021-2025, Information System Authority.* Information System Authority. Available at: https://www.ria.ee/en/media/1296/download (Accessed: February 12, 2023).

International Telecommunication Union (2021) *Global Cybersecurity Index 2020* English. rep. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Accessed: February 12, 2023).

Jeremic, I. (2023) *Cyber Security Archives*, *BIRD*. BIRN Investigative Resource Desk. Available at: https://bird.tools/tag/cyber-security/ (Accessed: February 12, 2023).

Kaitseliit (n.d.) *Estonian Defence League's cyber unit*, *Estonian Defence League*. Estonian Defence League. Available at: https://www.kaitseliit.ee/en/cyber-unit (Accessed: February 12, 2023).

Kalev , S. and Maxime, L., 2019. *Estonian-French Defence Cooperation: Where Estonian Pragmatism Meets French Vision*. International Centre for Defence and Security. Available at: https://icds.ee/wp-content/uploads/2019/08/ICDS_Analysis_Estonian-

French_Defence_Cooperation_Kalev_Stoicescu-Maxime_Lebrun_August_2019.pdf (Accessed: February 12, 2023).
Karyoti, V. (2022) "Shared Values and Common Borders: Why Greece Views European Strategic Autonomy as an Opportunity," in Česnakas, G., and Juozaitis, J. (eds),*European strategic autonomy and small states' security: In the shadow of power*. London, UK: Routledge, pp. 196–208. Available at: https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003324867/european-strategic-autonomy-small-states-security-giedrius-%C4%8Desnakas-justinas-juozaitis.
Klečková, A. (2021) "Does the Russian Intervention in Crimea in 2014 Demonstrate the New Way of War?," *Strife Journal*, (15/16), pp. 51–60. Available at: https://www.strifejournal.org/wp-content/uploads/2021/11/STRIFE_15_16_KLECKOVA_51_60.pdf (Accessed: February 12, 2023).
Koeller, J. (2015) *PUTIN'S GRAND STRATEGY: RUSSIA'S CAMPAIGN OF CONTROLLED INSTABILITY IN UKRAINE AND BEYOND*. thesis. Angelo State University. Available at: https://asu-ir.tdl.org/bitstream/handle/2346.1/30505/KOELLER-THESIS-2015.pdf?sequence=1&isAllowed=y (Accessed: February 12, 2023).
Koutantou, A. and Maltezou, R. (2022) *Greece speeds up gas exploration to help reduce russian reliance*, *Reuters*. Thomson Reuters. Available at: https://www.reuters.com/business/energy/greece-speed-up-gas-exploration-help-replace-russian-gas-pm-says-2022-04-12/ (Accessed: February 12, 2023).
Krusten, M. (2019) Fighting cybercrime in the Digital age - e-estonia, e-Estonia. EAS. Available at: https://e-estonia.com/fighting-cybercrime-in-the-digital-age/ (Accessed: February 12, 2023).
Kurecic, P., Kozina, G. and Kokotović, F., 2017. 'Revisiting the definition of Small State through the use of relational and quantitative criteria.' *Conference: 19th International Scientific Conference on Economic and Social Development*. Melbourne, Australia, February 2017. Available at: https://www.researchgate.net/publication/313675926_REVISITING_THE_DEFINITION_OF_SMALL_STATE_THROUGH_THE_USE_OF_RELATIONAL_AND_QUANTITATIVE_CRITERIA (Accessed: February 12, 2023).
Lacqua, F. (2022) "Prime Minister Kyriakos Mitsotakis' interview on Bloomberg TV, with journalist Francine Lacqua," *Bloomberg Daybreak Europe - TV Shows*. Bloomberg. Available at: https://www.bloomberg.com/news/videos/2022-11-08/-bloomberg-daybreak-europe-full-show-11-08-2022 (Accessed: February 12, 2023).
Lau, S. (2022) "Down to 14 + 1: Estonia and Latvia quit China's club in Eastern Europe," *Politico*, 11 August. Available at: https://www.politico.eu/article/down-to-14-1-estonia-and-latvia-quit-chinas-club-in-eastern-europe/ (Accessed: February 12, 2023).
Made, V., 2011. "Shining in Brussels? The Eastern Partnership in Estonia's Foreign Policy," *Perspectives*, 19(Identity and Solidarity in Foreign Policy: Investigating East Central European Relations with the Eastern Neighbourhood), pp. 67–79.
Madise, Ü. and Martens, T. (2006) "Electronic Voting 2006: 2nd International Workshop," in *Gesellschaft für Informatik*. Bregenz, Austria. Available at: https://dl.gi.de/handle/20.500.12116/29155
Mazis, I. and Troulis, M. (2020) 'Greece's Aegean Policy in the Post-Cold War Period II.'EGE JEOPOLİTİĞİ. Ankara: ATLAS AKADEMİK BASIM YAYIN DAĞITIM Tİ C. LT D. ŞTİ. pp. 851-857
Ministry of Digital Policy, Telecommunications and Media (2018) *National Cyber Security Strategy*. rep. Ministry of Digital Policy, Telecommunications and Media. Available at: https://mindigital.gr/wp-content/uploads/2020/01/NCSSGR.pdf (Accessed: February 12, 2023).
Ministry of Economic Affairs and Communications (2020) *Estonian ministries report cybersecurity incidents and data breach*, *Estonian Ministries Report Cybersecurity Incidents and Data Breach | Majandus- ja Kommunikatsiooniministeerium*. Ministry of Economic Affairs and Communications. Available at: https://www.mkm.ee/en/news/estonian-ministries-report-cybersecurity-incidents-and-data-breach (Accessed: February 12, 2023).
Ministry of Economic Affairs and Communications (2021) *Estonia's Digital Agenda 2030*. Republic of Estonia. Available at: https://www.mkm.ee/media/6970/download (Accessed: February 12, 2023).
Ministry of Economic Affairs and Communications (n.d.) *Cybersecurity Strategy*. Republic of Estonia. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/kyberturvalisuse_strateegia_2022_eng.pdf (Accessed: February 12, 2023).
Ministry of Defence (2022) *Defence budget*, *Kaitseministeerium*. Republic of Estonia. Available at: https://www.kaitseministeerium.ee/en/objectives-activities/defence-budget(Accessed: February 12, 2023).
Ministry of Foreign Affairs (2017) *Common security and defence policy (CSDP)*, *Hellenic Republic - Ministry of Foreign Affairs*. Hellenic Republic. Available at: https://www.mfa.gr/en/foreign-policy/greece-in-the-eu/eu-common-security-and-defence-policy-csdp.html (Accessed: February 12, 2023).
Ministry of Foreign Affairs (2020) *Past Greek presidencies, Hellenic Republic - Ministry of Foreign Affairs*. Hellenic

Republic. Available at: https://www.mfa.gr/en/foreign-policy/greece-in-the-eu/past-greek-presidencies.html (Accessed: February 12, 2023).
Ministry of Foreign Affairs (2021) *Estonia's participation in civilian missions, Estonia's participation in civilian missions | Välisministeerium*. Republic of Estonia. Available at: https://www.vm.ee/en/estonias-participation-civilian-missions (Accessed: February 12, 2023).
Miró, J. (2022) "Responding to the global disorder: The EU's quest for open strategic autonomy," *Global Society*, pp. 1–21. Available at: https://doi.org/10.1080/13600826.2022.2110042.
Michalopoulos, S. (2020) "Athens smarting after exclusion from German-hosted Libya conference," Euractiv, 16 January. Available at: https://www.euractiv.com/section/global-europe/news/athens-smarting-after-exclusion-from-german-hosted-libya-conference/ (Accessed: February 12, 2023).
Myatt, M. (2021). "Small, Smart, Powerful?," *Competition in World Politics*, pp.233–260. Available at: https://doi.org/10.1515/9783839457474-010.
Nedos, V. (2022) "Greece enters fight against hybrid threats," *ekathimerini.com*, 18 February. Available at: https://www.ekathimerini.com/news/1177658/greece-enters-fight-against-hybrid-threats/ (Accessed: February 12, 2023).
Ntousas, V. (2021) *Greece in the Eastern Mediterranean: Turning engagement into influence*, *ECFR*. Available at: https://ecfr.eu/article/greece-in-the-eastern-mediterranean-turning-engagement-into-influence/ (Accessed: February 12, 2023).
Paganini, P. (2021) European Commission and other institutions were hit by a major cyber-attack, Security Affairs. Security Affairs. Available at: https://securityaffairs.co/116441/hacking/european-commission-institutions-cyberattack.html (Accessed: February 12, 2023).
Papadimitriou, J. (2018) "Hackers trade attacks amid worsened Greek-Turkish ties," *Deutsche Welle*, 5 June. Available at:https://www.dw.com/en/greek-turkish-hackers-trade-retaliatory-cyberattacks-amid-worsened-relations/a-43672264 (Accessed: February 12, 2023).
Papadopoulos, A.G. and Fratsea, L.- M. (2019) "Migration and Refugee Flows in Greece in the Post-Crisis Period: Exploring Different Claims for Socio-Spatial Justice," *Il Mulino - Rivisteweb*, (3), pp. 401–423. Available at: https://doi.org/https://doi.org/10.1447/96701 .
Papadopoulos, Y. (2022) "Cyberattacks well-planned, aim at ransom," ekathimerini.com, 26 March. Available at: https://www.ekathimerini.com/news/1180540/cyberattacks-well-planned-aim-at-ransom/ (Accessed: February 12, 2023).
Papakonstantinou, G. (2020) "Turkish hackers: We hit Greek government websites," *ETHNOS*, 5 February. Available at: https://www.ethnos.gr/Politics/article/83330/toyrkoixakersxtyphsameellhnikeskybernhtikesistoselides (Accessed: February 12, 2023).
Pedi, R. (2016) *Theory of international relations: small states in the international system.* PhD thesis. University of Macedonia. Available at: https://www.didaktorika.gr/eadd/handle/10442/38599?locale=en (Accessed: February 12, 2023).
Pedi, R. (2017) "Greece in the Aftermath of the Economic Crisis Needs to Change Its Strategy in the International System: Choosing Between Melians and David.," in Marangos, J. (eds) , *The internal impact and external influence of the Greek financial crisis*. New York,: Palgrave Macmillan, Cham, pp. 143–160. Available at: https://link.springer.com/chapter/10.1007/978-3-319-60201-1_9 (Accessed: February 12, 2023).
Pedi, R. and Sarri, K. (2021) "Resilience through entrepreneurship: Enriching european external action service's resilience toolbox*," Entrepreneurship, Institutional Framework and Support Mechanisms in the EU, pp. 149–164. Available at: https://doi.org/10.1108/978-1-83909-982-320211014.
PESCO (n.d.) *Permanent structured cooperation (PESCO)*, *PESCO*. European Union. Available at: https://www.pesco.europa.eu/#projects (Accessed: February 12, 2023).
RFC2350 - National CERT operation - nis.gr (n.d.) *National Intelligence Service (EYP)*. Available at: https://www.nis.gr/downloads/national-cert/RFC2350-EN.pdf (Accessed: February 12, 2023).
Samsoerizal, A.D., Hidayat, E.R. and Sukendro, A. (2022) "Analytical Study of Indonesian Cybersecurity: Lesson Learned From Estonian Cyberattacks In 2007 ," *International Journal of Arts and Social Science*, 5(2), pp. 32–33.
Sant, S.van and Goujard, C. (2022) "European Parliament website hit by cyberattack after Russian terrorism vote," *Politico*, 23 November. Available at: https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/ (Accessed: February 12, 2023).
SIPRI (n.d.) *SIPRI Military Expenditure Database, SIPRI MILEX. SIPRI*. Available at: https://milex.sipri.org/sipri (Accessed: February 12, 2023).
Sabbagh, D. (2021) *Experts say China's low-level cyberwar is becoming severe threat*, *The Guardian*. Guardian News and Media. Available at: https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat (Accessed: February 12, 2023).
Souliotis, Y. (2020) "The Turkish hackers 'strike again'.," *Kathimerini*, 26 August. Available at:

https://www.kathimerini.gr/society/1093398/xanachtypisan-oi-toyrkoi-chaker/ (Accessed: February 12, 2023).

Stamouli, N. (2022) "Greece's spyware scandal expands further," *Politico Europe*, 5 November. Available at: https://www.politico.eu/article/greece-spyware-scandal-cybersecurity/ (Accessed: February 12, 2023).

Statistics Estonia, 2022. *Life expectancy and disability-free life expectancy have decreased*, *Statistikaamet*. Statistics Estonia. Available at:https://www.stat.ee/en/find-statistics/statistics-theme/population (Accessed: February12, 2023).

Strategic Communications (2022) *A Strategic Compass for Security and Defence. rep. European External Action Service*. Available at: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (Accessed: February 12, 2023).

Tallinn Digital Summit. n.d. *Concept*, *Tallinn Digital Summit*. Available at: https://www.digitalsummit.ee/ (Accessed: February 12, 2023).

Thorhallsson, B. (2000) *The Role of Small States in the European Union*. 1st ed. London: Ashgate Publishing Limited, pp.4-7.

Thorhallsson, B. and Wivel, A. (2006) "Small states in the European Union: What do we know and what would we like to know?," *Cambridge Review of International Affairs*, 19(4), pp. 651–668. Available at: https://doi.org/10.1080/09557570601003502 .

Thorhallsson, B. (2018) "Studying small states: A review," Islands and Small States Institute, 1(1), pp. 26–27.

Tidy, J. (2021) "European Banking Authority hit by Microsoft Exchange hack," *BBC News*, 8 March. Available at: https://www.bbc.com/news/technology-56321567 (Accessed: February 12, 2023).

Tiirmaa-Klaar, H. (2010) *Rahvusvaheline Koostöö Küberjulgeoleku Tagamisel*, *Diplomaatia*. International Centre for Defence Studies. Available at: https://diplomaatia.ee/rahvusvaheline-koostoo-kuberjulgeoleku-tagamisel/ (Accessed: February 12, 2023).

Toome, E. (2022) *Cyber Security Education in Estonia: From kindergarten to NATO cyber defence centre*, *Education Estonia*. Available at: https://www.educationestonia.org/cyber-security-education-in-estonia/ (Accessed: February 12, 2023).

Toulas, B. (2022) *Greek natural gas operator suffers ransomware-related data breach*, *BleepingComputer*. BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/greek-natural-gas-operator-suffers-ransomware-related-data-breach/ (Accessed: February 12, 2023).

ToVima Team (2022) "Greek Parliament: Authorities probe hacking of 60 email accounts.," *To vima International*, 21 January. Available at: https://www.tovima.gr/2022/01/21/international/greek-parliament-authorities-probe-hacking-of-60-email-accounts/ (Accessed: February 12, 2023).

Veebel , V. and Ploom, I. (2022) "Through the Estonian Looking Glass: Can NATO's Credible Deterrence and EU Strategic Autonomy Succeed Simultaneously?," in Česnakas, G., and Juozaitis, J. (eds),*European Strategic Autonomy and Small States' Security:In the Shadow of Power.* London, UK: Routledge, pp. 94–108. Available at: https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003324867/european-strategic-autonomy-small-states-security-giedrius-%C4%8Desnakas-justinas-juozaitis.

Whyte, A. (2022) "DDoS attacks on Estonian state sites continued over weekend," *ERR, ERR News*, 25 April. Available at: https://news.err.ee/1608575371/ddos-attacks-on-estonian-state-sites-continued-over-weekend (Accessed: February 12, 2023).

Whyte, A. and Wright, H. (2021) "Hacker downloads close to 300,000 personal ID photos," *ERR, ERR News*, 29 July. Available at: https://news.err.ee/1608291072/hacker-downloads-close-to-300-000-personal-id-photos (Accessed: February 12, 2023).

Wivel, A. and Crandall, M. (2019) "Punching above their weight, but why? explaining Denmark and Estonia in the transatlantic relationship," *Journal of Transatlantic Studies*, 17(3), pp. 405–412. Available at: https://doi.org/10.1057/s42738-019-00020-2 .

Worldpopulationreview.com (n.d.) *2023 world population by country (live), 2023 World Population by Country (Live)*. Available at: https://worldpopulationreview.com/ (Accessed: February 12, 2023).

Wrange, J. and Bengtsson, R. (2019) "Internal and external perceptions of small state security: The case of Estonia," *European Security*, 28(4), pp. 449–472. Available at: https://doi.org/10.1080/09662839.2019.1665517 .

Wright, H. (2022a) "DDoS cyberattacks temporarily disrupt Estonian foreign ministry website," *ERR News*, 9 May. Available at: https://news.err.ee/1608591475/ddos-cyberattacks-temporarily-disrupt-estonian-foreign-ministry-website (Accessed: February 12, 2023).

Wright, H. (2022b) "Estonia subjected to 'extensive' cyberattacks after moving Soviet monuments," *ERR news*, 18 August. Available at: https://news.err.ee/1608688201/estonia-subjected-to-extensive-cyberattacks-after-moving-soviet-monuments (Accessed: February 12, 2023).