ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Understanding Estonia's Cyber Support for Ukraine: Building Resilience, Not Status

Matthew Crandall | School of Governance, Law, and Society, Tallinn University, Tallinn, Estonia | ORCID: 0009-0000-2588-009X

Abstract

This article explores Estonia's cyber support for Ukraine following Russia's invasion in February 2022. Despite its small size, Estonia has significant cyber expertise and has played a pivotal role in safeguarding Ukrainian digital infrastructure and providing cybersecurity support. While Estonian cyber contributions to Ukraine are significant, it initially did not seek or receive international attention. Estonia is typically vocal in promoting its cybersecurity and e-governance expertise. This article aims to first explore the impact of Estonia's cyber support for Ukraine. Second, it aims to understand why Estonia did not try to use this support to bolster its status as a cyber authority. To do this, Estonia's cyber support is analysed and put into the proper geopolitical context. Interviews with high-ranking Estonian officials were conducted and an analysis of policy output was performed. This article finds that the importance of cybersecurity assistance is not as critical as military assistance, which is one reason why Estonia has not (yet) used its cyber assistance as a status opportunity. Although cybersecurity support may be considered secondary to military support, the significance of Estonia's cybersecurity assistance should not be overlooked. Although Estonia did not pursue status initially, there are some signs that this is beginning to change and Estonia is recognised for its cyber expertise.

Received: 03.01.2024

Accepted: 30.05.2024

Published: 05.07.2024

Cite this article as:
M. Crandall, "Understanding Estonia's cyber support for Ukraine: Building resilience, not status," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190396

Corresponding author:
Matthew Crandall, School of Governance, Law, and Society, Tallinn University, Tallinn, Estonia; E-mail: crandall@tlu.ee
0009-0000-2588-009X

Keywords
cybersecurity, Ukraine, resilience, status

1. Introduction

Russia's invasion of Ukraine on 24 February 2022 is seen in Estonia as an existential threat. Ukraine's importance to Estonia started long before the invasion in 2022 or the illegal annexation of Crimea in 2014. Estonia has long prioritised Eastern partnership countries, Ukraine, Moldova, and Georgia in particular, in development cooperation and foreign policy priorities [1]. In the lead-up to the 2022 invasion, Estonia's support for Ukraine was significant. Military assistance was the most attention-getting aspect of assistance. For example, Estonia provided Javelin anti-tank missile systems and decided to provide 122 mm artillery systems before the invasion began [2]. After the start of invasion, Estonia has been among the most vocal in its support for Ukraine. This was particularly evident when looking at military aid as a percentage of GDP; Estonia was among the top donor countries. In addition to military support, Estonia has been active in providing both military and civilian cyber support. Estonia's cyber support has not received noteworthy attention within Estonia or internationally. This is a stark contrast to the attention Estonia has received for the level of military and political support for Ukraine. For example, in April 2023, President Volodymyr Zelensky in a meeting with Estonian Prime Minister Kaja Kallas said: 'If every leader and every state were equally conscientious about protecting our common freedom on the continent, Russia's aggression would have already been defeated without question' [3]. What makes this development striking is Estonia's past promotion of its cyber expertise [4]. Given Estonia's internationally recognised cyber expertise and its promotion of itself as a cyber authority, it is surprising that it would not have brought more attention to its cyber support for Ukraine. This article explores the cyber assistance Estonia has provided to Ukraine and why Estonia has not yet tried to leverage this support to bolster its status as a cyber expert.

Estonia's cyber support for Ukraine merits a closer analysis for several reasons. First is the nature of the war in Ukraine. This is the first large-scale, long-term war involving a developed country dependent on the Internet [5]. The implications of this are significant. This changes both nature and importance of cybersecurity. Second, what impact can a small state with limited resources have on cybersecurity assistance? It is one thing for a small state to emphasise cyber support as part of a development cooperation

strategy during a time of peace, and it is another to react in a crisis.

Smaller states typically have limited material resources and thus cannot influence international affairs with military and economic might. Although there are exceptions like Israel or Norway, those are not reflective of the position of most small states. A majority of small states tend to pursue normative change and influence international affairs through avenues that do not require excessive resources [6]. One typical way is to be a standard bearer. Modelling ideal behaviour can be used as an example for other states. This is, perhaps why status-seeking is an appropriate conceptual framework to understand small state behaviour. Estonia, like many small states, has pursued a strategy of status-seeking. In particular, Estonia has modelled itself as an expert in cybersecurity and e-governance, adopting the nickname e-Estonia [4]. Given Estonia's significant cyber support for Ukraine, it is peculiar that Estonia has not publicly tried to boost its status as part of its strategy of cyber assistance. For example, the Ministry of Foreign Affairs page on support for Ukraine details a long list of different ways Estonia has supported Ukraine and Ukrainians. There is virtually no mention of any cyber support, aside from a list of donated goods that mentions IT equipment [2].

To better understand this paradox, this article first maps out Estonia's cyber support for Ukraine and place it in a larger geopolitical context. It then explores the reasons, why Estonia has not used this support to boost its own status. To do this, government documents and publications were analysed. In addition, expert interviews were conducted. This article then proceeded with a discussion on methods and a conceptual framework of status-seeking. This follows with two analytical sections, one mapping out Estonia's support for Ukraine, and another discussing the impact of the strategy and how the strategy was influenced by geopolitical considerations. The article concludes with implications of what this all means for small states with high cyber aspirations.

2. Literature Review: Small State Status in Cyberspace

Status in international relations is an emerging concept that is used to understand the foreign policy of aspiring great powers as well as small states. Status has its theoretical origins in a theory from psychology, the Social Identity Theory developed by Tajfel and Turner [7]. In this theory, the key to understanding individuals

is the relationship between groups and group membership. There is a need for positive self-esteem, which happens from inter-group comparisons. Status is then a social hierarchy that can be best understood when group interactions are taken into consideration [8]. There are many authors who applied this concept of psychology to international relations. Paul et al. discussed in their 2014 edited volume status in international relations [9]. The influential volume focused on emerging states and rising powers. The pursuit of status is not just for large states. As Neumann and Carvalho note, small states do not have the luxury of pursuing the power game or investing in tools of coercion due to limited resources [10]. Small states then must rely on moral authority for their pursuit of status [10]. In many ways, status as a theoretical concept is even more applicable for small states as most small states face status uncertainty [10]. This concern is also evident in the small state literature on ontological security. It has been argued that states suffering trauma are more prone to status uncertainty [11]. Estonia and other states occupied by the Soviet Union would fit this profile. There have been quite a few authors that have looked at small states seeking status in recent years. Most authors looked at single-state case studies, such as Cyprus [12], Lithuania [13], and Estonia [1], as well as others.

Status can be sought out for multiple reasons. For some, status can be the means to justify an end, thus a state would seek status to have a better chance at pursuing its foreign policy interests [14]. For others, the pursuit of status is the end goal due to the above-mentioned status uncertainty that small states often face. No matter the goal, looking at inner and outer group dynamics is key to understanding any status-seeking behaviour. Small states usually seek status from great powers by proving their usefulness [10]. There are also opportunities for small states to seek status from those outside their own status group [15]. The relationships of status-seeking can vary. In addition to states, international organisations are also an important avenue to seek status. The nature of status-seeking means that most status-seeking endeavours are highly visible campaigns and developments. Depending on the circumstances, status-seeking could be more targeted and remain outside the public eye. Small states and the United Nations (UN) Security Council can demonstrate this process [16]. For example, Estonia's selection to the UN Security Council from 2020–2021 was a visible act of status-seeking that included a global campaign and a successful vote in the UN General Assembly. Estonia's work on the UN Security Council was not as visible to the public but also resulted in an increase in status and improved reputation from other states who were serving with Estonia on the UN Security Council [17].

Despite the increasing literature on small-state status-seeking behaviour, there is no clear picture of the conditions that shape small-state status-seeking strategies. Why would a state choose a certain relationship or campaign to improve its status? The focus of this article is on Estonia and its cybersecurity assistance to Ukraine, from 24 February 2022 to the end of 2023. Looking at this relationship, it sheds light on the conditions needed for a state to seek out status.

At first glance, Estonia has not been as vocal in drawing attention to its cyber support for Ukraine, instead it focused on its military contributions. This seems at odds with the long-standing strategy of status-seeking via cybersecurity and e-governance. To better understand this development, the article uses a mixed methods approach utilising desk research and document analysis. Primary sources were gathered from government documents and strategies mostly produced by the Estonian Ministry of Foreign Affairs specific to Estonia's support for Ukraine. Estonia, like many other states, includes NGOs in the implementation of policies, especially in development cooperation. Regarding cyber assistance and Ukraine, a key institution is and has been the e-Governance Academy. Project information and documents related to Estonia's cyber assistance to Ukraine were analysed. In addition, two expert interviews were conducted in Tallinn, one in the late summer of 2023 and another in December 2023. Both high-ranking officials had intimate experience and knowledge of Estonia's cyber assistance to Ukraine and Estonia's strategy regarding cyber diplomacy foreign policy priorities. Due to the sensitive nature of the interviews, the officials desired to remain anonymous. This also ensured responses that are more direct. The officials were from different government institutions and complemented each other with their experiences. The identity of the officials, the transcripts of the interviews, and confirmation that the interviews took place, were shared with the editorial board to ensure that the rigours of academic research were met. The thoughts and takeaways from this article are heavily influenced by these interviews and the officials' perspectives.

The article analyses the data in two sections: first, a section outlining Estonia's cyber support to Ukraine, and second, the implications of Estonia's support and a discussion of its impact (or lack thereof) on Estonia's status-seeking strategy.

3. Estonian Support for Ukraine

One of the key elements of Estonia's foreign policy has been to increase its status within key international frameworks,

such as North Atlantic Treaty Organisation (NATO) and the European Union (EU) [18]. Estonia has tried to be a model ally, a producer of security, not only a consumer of security [19]. Although Estonia has done much to enhance its status in many aspects, it is the most visible in terms of cybersecurity and e-governance [20]. Estonian leaders share a consensus about the importance of developing and maintaining cyber and e-governance competencies. Estonia has developed innovative e-governance services that are international attention-getters, such as online voting and an e-residence program [21]. Perhaps, the most effective framework Estonia has used to increase its status has been NATO. Tallinn is the location of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). The CCDCOE facilitated the Tallinn Manual I and II, describing how international law can apply to cyberspace. The Tallinn Manual I and II bear the name of Tallinn, which put Tallinn in 'the mental world map of international law with a purposefully accomplished project' [22].

Russia's war in Ukraine brought large-scale World War II-style military conflict back to the heart of Europe. However, Ukraine is an advanced society with many digital services and dependencies on connectivity [23]. This created a significant challenge for Ukraine and for those assisting Ukraine to help keep Ukraine online. Russia's invasion of Ukraine changed the nature and scope of Estonia's cyber support for Ukraine. The following information is based on the expert interviews unless cited otherwise. The opinions of both expert interviews have been combined to allow this section to have a thematic flow.

Estonia's cyber support to Ukraine goes back well before the 2022 invasion. Cooperation in improving information and communication technologies (ICT) and e-governance solutions has been the backbone of Estonia's development cooperation strategy for some time now [18]. The e-Governance Academy has been the primary organisation to implement development cooperation projects. Projects carried out in Ukraine currently listed on their website go back to 2014 and cover several topics such as boosting e-governance solutions, improving cybersecurity readiness in Ukrainian public officials, and building cyber defence capabilities. The cost of the projects ranged from €44,000 to more than €17 million [24]. The funding often comes through EU funding mechanisms.

Having connections with Ukraine before the war broke out made it easier for Estonia to provide support after the war began. A few days before the war broke out, a team of Estonian cybersecurity

officials travelled to Ukraine to meet their counterparts to establish person-to-person contact. At that time, it was not completely sure as to what would happen, but things were pointing towards a war. These contacts were beneficial in helping to coordinate support after the breakout of the war.

Estonia's cyber support to Ukraine can be divided into two aspects: practical support and diplomatic support. Practical support can be largely described as bilateral cooperation. One key area of practical assistance Estonia provided was help safeguarding Ukrainian digital infrastructure. Ukraine needed to evacuate a significant amount of its public digital infrastructure, which was not an easy task. For many services, this meant relocating to the cloud, but due to the specific hardware of some systems, not everything could be deployed in the cloud. Some systems were exported to NATO territories to be maintained as an operational service. Estonia's attitude towards cyber assistance was to help in any way that Estonia could. As one official put it, 'Any assistance Ukraine wanted, if we were able to provide it we did, without hesitation'. Most of the support Estonia provided was intangible support, such as putting data in safekeeping and getting servers up and running.

Both officials interviewed stressed the important role of coordination in the support that Estonia gave. The outbreak of the war was described as a nightmare, a mess, and there was a lack of consolidation on Ukraine's part. Ukraine was understandably focused on the military aspect of defence and the intensity of the cyberattacks were at their highest before the invasion began. Requests for assistance were going from multiple channels to multiple actors and the result was confusion. Western partners had to know what Ukraine needed to avoid duplication and ensure that Ukraine could absorb the assistance. Estonia's prior contacts with Ukraine enabled Estonia to play a key role in helping to streamline the coordination efforts.

The key to shoring up and enabling Ukrainian cyber defence was the implementation of Western tech, usually from the private sector. One obstacle Ukraine faced with this was export controls and getting a licence for the product or service. In this situation, Estonia was able to relay requests to the US State Department, validate requests made by Ukraine, and play a constructive role in helping to get information to the proper actors promptly.

Perhaps, the most significant and certainly visible outcome of Estonia's cyber support for Ukraine is the Tallinn Mechanism, which was launched on 20 December 2023. This mechanism systematises

support from various countries and companies for civilian cyber assistance to Ukraine [25]. Estonia has assigned a diplomat to Kyiv to support the mechanism and has earmarked Euros 500,000 from its development cooperation fund to support the Tallinn Mechanism and Ukrainian civilian cybersecurity assistance. The participating countries, in addition to Estonia, are Canada, Denmark, France, Germany, The Netherlands, Poland, Sweden, the United Kingdom, and the United States. Given the long-term attacks and threats Ukraine is and will be facing from Russia, the Tallinn Mechanism aims to replace the ad hoc nature of cyber assistance with a systematised and more coherent manner. Estonia hopes that this format could be a model for future conflicts. The Tallinn Mechanism works in tandem with the IT coalition, which coordinates cyber assistance for military means.

Estonia is also a founding member of the IT coalition along with Ukraine and Luxembourg [26]. This is a good example of Estonia taking the initiative and making a difference. At a meeting of IT Coalition, Ukrainian minister of Defence Rustem Umerov stated that 'Technology will win the war … our advantage will be provided by asymmetric responses and they are possible, thanks to innovations that are already working' [27].

The second aspect of Estonian cyber support to Ukraine is diplomatic support. Diplomatic support happened in both open- and closed-door settings. Estonia has often supported Ukraine in the UN's open-ended working group on the use of ICT. Estonia promotes the application of international law in cyberspace and responsible behaviour in cyberspace [28]. Russia's actions in Ukraine go against both of these principles. Estonia has also consulted Ukraine on boosting its cyber diplomacy capabilities to improve its influence in the UN and globally.

Estonian diplomatic support also took place behind closed doors. Two instances are worth noting that were highlighted by the experts. In the early stages of the war, Estonia offered one platform so that Ukraine could exchange information securely. Some EU partners were vocal in their concern for this move because they also used the same platform. There was concern about the potential risk to them. Estonian officials spent a significant amount of time discussing and alleviating those concerns. In another format with multiple countries, the topic was raised to donate dual-use software. It was designed to detect vulnerabilities to improve cyber defence, but it could also be used to find vulnerabilities in Russia's systems and be used as an offensive capability. Estonia has for

years argued against the myth of offensive cyber capabilities. As one official noted, self-defence in cyberspace includes the use of offensive cyber capabilities. Estonian officials advocated for Ukraine and were a voice of reason: if bombs and guns were already being provided, then a piece of dual-use software would not change the risk factor for EU countries. The process was slow and Ukraine's request was eventually filled.

Although Estonia is a small state with limited resources and a country that does not have big technology companies, the contributions to helping Ukraine with cyber support were significant and noteworthy. When one official was asked if they were satisfied with Estonia's cyber support to Ukraine, the answer was yes. This still begs the question, if Estonia's contribution was significant, then why would Estonia not use this to improve its status as an expert in cybersecurity and e-governance? Why would Estonia not promote itself as a standard bearer for others to follow suit? The next section tackles these questions and discusses the implications and limitations of Estonia's cyber support.

4. Building Resilience Now, Status Later

Estonia's support for Ukraine should not be trivialised. One of the most sobering points raised by an official was how often Estonia was attacked by a distributed denial-of-service (DDoS) attack after Estonian state leaders made any public comment critical of Russia. This works like clockwork. Why then, despite the effort, the cost, and the risk is Estonia's cybersecurity support not talked about more? There are several reasons noted by the officials interviewed. As one official noted, 'Ukraine will not win the war with their e-solutions. Russians can be beaten right now by brutal force'. In this conflict we are not seeing cyberattacks against hospitals, we are seeing bombs hitting hospitals. What Ukraine needs the most is military support. This explains why Estonia has emphasised so heavily the need to do more to militarily support for Ukraine and why Estonia has emphasised itself as a standard bearer of military support to Ukraine as opposed to cybersecurity assistance.

A secondary concern is also related to risk management involved. Estonia needs to be cautious with what is supplied to not draw undue attention and increase its odds of being a target. The nature of Estonian cyber support was different from military support. Where military support was delivering material products to Ukraine, cyber support meant hosting Ukrainian data and servers in Estonia and facilitating Ukrainian communication with Estonian tools.

This invites a larger discussion about the nature of cyber capabilities in conflict. Some reflections on this topic have been already drawn [29]. As noted in the publication, cyber operations did not yield strategic results. One of the Estonian officials speculated that it also was related to Russia's miscalculations about how it would be a short war. This meant that after the initial cyberattacks before the war began, they took a back seat to the military invasion. Yet, we should be weary of treating these as separate. Cyber is linked to military capabilities, especially with intelligence. Cyber operations have played a significant role in disinformation campaigns and promoting narratives and messaging.

Many works on small states tend to overestimate the impact that a small state causes. It is important to mention the limitations of Estonia's support to Ukraine. The real hero in Ukraine's cyber defensive resilience is the Western technologies that Ukraine is using. The question was once asked how big is a small state in cyberspace (personal communication with peer reviewer on a draft version of an article, 2015)? It turns out that in a time of war the small state still has limitations due to a lack of resources. However, this does not mean that a small state cannot make a difference. Indeed, Estonia is hopeful that the collective response to provide cyber assistance to Ukraine can be a model for future conflicts.

What might all this mean for Estonia's status as a cybersecurity expert and an expert in e-governance? As one official stated, 'We will probably hear more about this in the future'. The official continued that the war is an existential threat to Estonia. Thus, we can see that status does not serve a primary function. When the existential threat has been subdued, then we can assume that Estonia will return to a more typical foreign policy of status-seeking. Some level of status-seeking has already taken place. The Tallinn Mechanism bears the name of Tallinn, similar to the Tallinn manuals, which is a good first step to ensuring that Estonia is internationally recognised for its effective cyber assistance to Ukraine.

5. Conclusions

This article observed Estonia's cyber support to Ukraine. Estonia, as a small state and a recognised cybersecurity expert, presented an interesting subject. Typical small-state behaviour would suggest that small states would seek status, something Estonia has consistently done by promoting itself as a cybersecurity expert. This article explored why Estonia's cyber support to Ukraine has not been used to build status. It found that for Estonia,

the aftermath of the invasion was not the time or place to pursue a status-seeking policy. Risk factors and more important priorities left cyber assistance out of the public eye. As the chaos of the invasion eased, Estonia eventually began to pursue a more typical status-seeking policy. This was most evident with the creation of the Tallinn Mechanism. Estonia's cyber support to Ukraine is significant in terms of both practical support and diplomatic support. The creation of IT Coalition and Tallinn Mechanism are significant and tangible accomplishments for Estonia. Owing to long-standing cooperation before the conflict, Estonia was more effective in playing the role of a facilitator. Although this might not seem like something significant, Estonia helped to solve the largest problem at the beginning of the war, that is, bringing structured coordination to a scene of chaos.

The nature of the conflict is such that military capabilities determine the outcome of the war. Accordingly, Estonia has focussed its messaging efforts on its military support for Ukraine and drawing attention to the importance of continued allied military support for Ukraine. If there is room for status-seeking, then it is not be at the expense of military support for Ukraine. While cyber operations have not been the defining feature of this war, it has still caused more questions to be asked.

While the focus of this paper is on a small state supporting Ukraine, there were other questions raised in the interviews, such as the role of big tech in conflicts. For a small state, this creates more questions and potential vulnerabilities when a CEO can make decisions that influence a conflict. Since cyber operations did not have a determining impact in this conflict, will this lead to a lack of attention for cyber defence capabilities and best practices? Perhaps the biggest takeaway for Estonia is that this has not been a one-way relationship. Estonia has been in close dialogue and learning from Ukraine's experiences as well. During this time of crisis, we can see that Estonia's key strategy is to help Ukraine win the war and also to help Ukraine and Estonia develop cyber resiliencies to be ready for future crises.

References

[1] V. Made, "Shining in Brussels? The Eastern partnership in Estonia's foreign policy," *New Perspectives,* vol. 19, no. 2, pp. 67–80, 2011.

[2] Estonian Ministry of Foreign Affairs. (May 31, 2023). *Estonia's aid to Ukraine*. [Online]. Available: https://vm.ee/en/estonias-aid-ukraine [Accessed: Aug. 20, 2023].

[3] The Kyiv Independent. (Apr. 24, 2023). *Zelensky meets with Estonian prime minister in Zhytomyr Oblast*. [Online]. Available: https://kyivindependent.com/zelensky-meets-with-estonian-prime-minister-in-zhytomyr-oblast/. [Accessed: Mar. 30, 2024].

[4] A. Papp-Váry, "A successful example of complex country branding: The 'e-Estonia' positioning concept and its relation to the presidency of the council of the EU," *Acta Universitatis Sapientiae, European and Regional Studies*, vol. 14, pp. 87–115, 2018, doi: 10.2478/auseur-2018-0013.

[5] M. Crandall, Anonymous high-ranking Estonian official, personal communication, Tallinn, Dec 28, 2023.

[6] G. Magnúsdóttir, B. Þórhallsson, "The Nordic States and agenda-setting in the European Union: How do small states score?," *Icelandic Review of Politics and Administration*, vol. 7, no. 1, pp. 205–225, 2011, doi: 10.13177/irpa.a.2011.7.1.11

[7] H. Tajfel, J.C. Turner, "An integrative theory of intergroup conflict,"in *Monterey*, W.G. Austin, S. Worchel, Eds., Pacific Grove, CA: Brooks/Cole, 1979, pp. 33–37.

[8] J.C. Turner, "Towards a cognitive redefinition of the social group," in *Social identity and intergroup relations*, H. Tajfel, Ed., Cambridge: Cambridge University Press, 1982, pp. 15–40.

[9] T.V. Paul, W.D. Larson, W.C. Wohlforth, *Status in world politics*. New York, NY: Cambridge University Press, 2014.

[10] I.B. Neumann, B. de Carvalho, Eds. "Introduction: Small states and status," in *Small state status seeking: Norway's quest for international standing*. London: Routledge, 2014, pp. 1–15.

[11] P. Charoenvattananukul, *Ontological security and status-seeking: Thailand's proactive behaviours during the Second World War*. New York, NY: Routledge, 2020.

[12] R. Pedi, K. Chainoglou, "The Republic of Cyprus in international and regional organizations: Towards a mature small state status seeking strategy?" in *The foreign policy of the Republic of Cyprus: Local, regional and international dimensions*, Z. Tziarras, Ed. Cham: Springer, 2022, pp. 287–309.

[13] A. Park, G. Jakstaite-Confortola, "Small state status-seeking: Lithuania's foreign policy status aspirations," *Europe-Asia Studies*, vol. 73, no. 7, pp. 1279–1302, 2021, doi: 10.1080/09668136.2021.1919291.

[14] R. Pedi, I. Kouskouvelis, "Cyprus in the Eastern Mediterranean: A small state seeking for status," in *The new eastern Mediterranean*, L. Spyridon, A.Tziampiris, Eds., New York, NY: Springer, 2019, pp. 151–167.

[15] M. Crandall, M.L. Sulg, "Small states and new status opportunities: Estonia's foreign policy towards Africa," *European Politics and Society*, vol. 24, no. 2, pp. 250–264, 2021, doi: 10.1080/23745118.2021.1990662.

[16] B. Thorhallsson, A.M. Eggertsdóttir, "Small states in the UN security council: Austria's quest to maintain status," *The Hague Journal of Diplomacy*, vol. 16, no. 1, pp. 53–81, 2020, doi: 10.1163/1871191X-BJA10017.

[17] R. Nodapera, *Small states in the UN security council: Case of Estonia through two presidencies in May 2020 and June 2021*. Master's thesis, School of Governance, Law and Society, Tallinn University, Tallinn, 2021.

[18] M. Crandall, I. Varov, "Developing status as a small state: Estonia's foreign aid strategy," *East European Politics*, vol. 32, no. 4, pp. 405–425, 2016, doi: 10.1080/21599165.2016.1221817.

[19] T.H. Ilves. (Dec. 5, 1996). *Address by foreign minister Toomas Hendrik Ilves to the Riigikogu*. [Online]. Available: https://vm.ee/en/news/address-foreign-minister-toomas-hendrik-ilves-riigikogu [Accessed: Aug. 20, 2023].

[20] M. Crandall, C. Allan, "Small states and big ideas: Estonia's battle for cybersecurity norms," *Contemporary Security Policy*, vol. 36, no. 2, pp. 346–368, 2015, doi: 10.1080/13523260.2015.1061765.

[21] M. Kimmo, I. Pappel, D. Draheim, "E-residency as a nation branding case," in *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, A. Kankanhalli, A. Ojo, D. Soares, Eds., New York, New York, USA, 2018, pp. 419–428.

[22] L. Mälksoo. (Aug. 8, 2013). *The Tallinn manual as an international event*. [Online]. Available: https://icds.ee/en/the-tallinn-manual-as-an-international-event. [Accessed: Dec. 30, 2023].

[23] F. Plantera. (2021). *The path towards e-Governance in Ukraine*. [Online]. Available: https://ega.ee/success_story/path-towards-egovernance-ukraine. [Accessed: Dec. 30, 2023].

[24] e-Governance Academy. (2023). *Digital transformation for Ukraine (DT4UA) projects*. [Online]. Available: https://ega.ee/projects/?country=ukraine. [Accessed: Dec. 30, 2023].

[25] Estonian Ministry of Foreign Affairs. (Dec.12, 2023). *Tallinn Mechanism*. [Online]. Available: https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism [Accessed: Dec. 22, 2023].

[26] Estonian Ministry of Defence. (Sep. 19, 2023). *Estonia, Luxembourg and Ukraine launched an IT coalition to support Ukraine*. [Online]. Available: https://www.kaitseministeerium.ee/en/news/estonia-luxembourg-and-ukraine-launched-it-coalition-support-ukraine. [Accessed: Dec. 30, 2023].

[27] Interfax Ukraine. (Nov. 29, 2023). *Umerov to participants of IT coalition: Technology to win war*. [Online]. Available: https://en.interfax.com.ua/news/general/950946.html. [Accessed: Dec. 30, 2023].

[28] Estonian Ministry of Foreign Affairs. (2021). *Estonian contribution on the subject of how international law applies to the use of information and communication technologies by states, to be annexed to the group of government experts on advancing responsible state behavior in cyberspace (2019–2021)*. [Online]. Available: https://www.vm.ee/media/799/download on 30.12.2023. [Accessed: Dec. 30, 2023].

[29] M. Schulze, M. Kerttunen, "Cyber operations in Russia's war against Ukraine," *SWP Comment*, no. 23, p. 8, Apr 17, 2023, doi: 10.18449/2023C23.