DOCTORAL THESIS

Knowledge Transfer for Public Administrations: The Case of Elections and Cybersecurity

Radu-Antonio Serrano-Iova

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2024

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
39/2024

Knowledge Transfer for Public Administrations: The Case of Elections and Cybersecurity

RADU-ANTONIO SERRANO-IOVA

TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Ragnar Nurkse Department of Innovation and Governance
This dissertation was accepted for the defence of the degree 25/05/2024

Supervisor: Dr. David Dueñas-Cid
Public Sector Data-Driven
Technologies Research Center
Kozminski University
Warsaw, Poland

[Formerly] Ragnar Nurkse Dep. of
Innovation and Governance
Tallinn University of Technology
Tallinn, Estonia

Co-supervisors: Dr. Veiko Lember
Ragnar Nurkse Dep. of Innovation and Governance
Tallinn University of Technology
Tallinn, Estonia

Dr. Dr. Robert Krimmer
Dr. Krimmer Consulting OÜ
Tallinn, Estonia

Opponents: Dr. Uwe Serdült
Centre for Democracy Studies Aarau (ZDA)
University of Zurich
Zurich, Switzerland

Dr. Noella Edelmann
Center for E-Governance
Department for E-Governance and Administration
Danube University Krems
Krems an der Donau, Austria

Defence of the thesis: 26/08/2024, Tallinn

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for doctoral or equivalent academic degree.

Radu-Antonio Serrano-Iova

----
signature

ISSN 2585-6898 (publication)
ISBN 978-9916-80-172-7 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-173-4 (PDF)
DOI https://doi.org/10.23658/taltech.39/2024
Printed by Koopia Niini & Rauam

Serrano-Iova, R.-A. (2024). *Knowledge Transfer for Public Administrations: The Case of Elections and Cybersecurity* [TalTech Press]. https://doi.org/10.23658/taltech.39/2024

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
39/2024

Haldusasutuste teadmussiire: valimiste ja küberturvalisuse juhtum

RADU-ANTONIO SERRANO-IOVA

TALTECH
KIRJASTUS

Contents

List of publications

The thesis is based on the following publications by the author:

I **Serrano-Iova, R.A.** (2024) [Forthcoming]. National Cybersecurity: Global and Regional Descriptive Snapshots through the Analysis of 161 Countries. *Halduskultuur - The Estonian Journal of Administrative Culture and Digital Governance*. ETIS 1.1.

II Krivonosova, I. & **Serrano-Iova, R.A.** (2021). From the Parliament to a Polling Station: How to Make Electoral Laws More Comprehensible to Election Administrators. In: *Election Law Journal*, Vol 20(4), pp. 364–381. Meredith, M. (Ed.). Mary Ann Liebert, Inc.: U.S. doi:10.1089/elj.2020.0670. ETIS 1.1.

III **Serrano-Iova, R.A.** & Watashiba, T. (2023). NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation. In: *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023*, Vol. 22(1), pp. 420–428. Andreatos, A. & Douligeris, C. (Eds.). ACI: UK. doi:10.34190/eccws.22.1.1168. ETIS 3.1.

IV Dueñas-Cid, D., Krivonosova, I., **Serrano, R.**, Freire, M., & Krimmer, R. (2020). Tripped at the Finishing Line: The Åland Islands Internet Voting Project. In: *Electronic Voting. E-Vote-ID 2020. Lecture Notes in Computer Science, Vol. 12455*, pp. 36–49. Krimmer, R., et al. (Eds.). Springer: Cham. doi:10.1007/978-3-030-60347-2_3. ETIS 3.1.

Additional articles:

V **Serrano-Iova, R.A.** (2023) [Forthcoming]. Pitfalls at the Starting Line: Moldova's IVS Pilot. In: *Electronic Voting. E-Vote-ID 2023. Lecture Notes in Computer Science.* ETIS 3.1

Author’s contribution to the publications

The author’s contribution to the papers in this thesis is outlined below:

I First author. The author of the doctoral thesis was the lead author of this paper, responsible for writing up all the content of the paper, including the literature review, the overall framework, and the writing up of the article.

II Second author. The author of the doctoral thesis is not the lead author of this paper yet was still heavily involved in writing up part of the content of the paper, including the literature review, and methodology, and designing the diagrams that were the focus of the paper.

III First author. The author of the doctoral thesis was the lead author of this paper, responsible for writing up most of the content of the paper, including the literature review, the overall framework, and the writing up of the article. The author also presented the work and was the corresponding author with the conference outlet.

IV Third author. The author of the doctoral thesis is not the lead author of this paper yet was still heavily involved in field work, data collection (travelling twice on-site to collect the information) and data analysis. The author also contributed significantly to writing up most of the content of the paper, including the research design, literature review, data collection, and the results.

V First author. The author of the doctoral thesis was the lead author of this paper, responsible for writing up all the content of the paper, including the literature review, the overall framework, and the writing up of the article. The author also presented the work and was the corresponding author with the conference outlet.

Introduction

Elections are a main component of the democratic way of life, "…among the most ubiquitous of contemporary political institutions, and voting is the single act of political participation undertaken by a majority of adults in a majority of the nations in the world today…" (Rose & Mossawir, 1967, p. 173). Quite similarly, cybersecurity is a main component of the ICT-focused and globalised way of life, covering "…all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents…" (ENISA, 2017, p. 6). This thesis deals with both topics, and while there might be some overlap between them, e.g., the cybersecurity of electronic voting tools, it does not combine, merge, or otherwise attempt to study them together. Nevertheless, as central public administration technological systems, they have common core components without which it would be impossible to administrate governmental affairs in the digital era. Knowledge transference is one of those core organisational building blocks (Goh, 1998), which also determine the effectiveness of any technological system. Understanding how to better transfer knowledge in two critical public administration systems – e-elections and cyber security – is the focus of this thesis.

The following thesis is the result of an industrial doctoral programme. The industrial doctoral programme has inherent differences from a regular one, the biggest being the opportunity to work in a company or an organisation and complete the studies related to the field of the profession (TalTech, n.d.). During the duration of his studies, the author of this thesis was appointed to projects in both cybersecurity and e-democracy, the latter focusing on elections. Therefore, the publications that provide the backbone of this thesis concern these seemingly compartmentalised topics. While the publications themselves provide novel knowledge, ideas, and concepts in their respective fields, and followed exploratory methods that have been put into practice, the development of this thesis provides the perfect environment for an overarching discussion embracing both fields of research and resulting in insights that can be of benefit and value for public administrations.

Knowledge comes heavily into play in elections. There are different domains of knowledge (e.g., law, public administration, ICT, logistics, etc.) and stakeholders with various institutionalised practices and interests (e.g., central government, private vendors, citizens, etc.) that are oftentimes in conflict with each other and need to be aligned and orchestrated. As a result, for example, private sector knowledge and insistence might lead to successfully lobby public administrations into purchasing electoral technologies in a non-sustainable way (Licht et al., 2021). Similarly, relative to internet voting, only a handful of people understand the entirety of such a system, with most of the electorate commonly knowing and focusing only on the threats and risks to such voting method (ibid.). On the other hand, knowledge is essential in cybersecurity. Cyber-attack vectors are predominantly targeted at people, not systems, which can be prepared by transferring the corresponding knowledge, awareness, and training (Banciu et al., 2020). The previously mentioned issue is compounded in public administrations, since policy and regulations might focus on rapid and effective delivery of services to the citizens, trumping cybersecurity concerns (Bertollini et al., 2022). Alas, all "[t]echnological systems are defined in terms of knowledge…" (Carlsson & Stankiewicz, 1991, p. 111), and actions based on a lack of understanding and knowledge will result in ineffective and arbitrary results (Wiig, 2002). Thus, knowledge management is nowadays an imperative for governments, enhancing government competence, improving their services' quality and their healthy development (Alvarenga et al., 2020). The transfer of knowledge, as a component of its management, can assist in the aforementioned goals, especially from the perspective of cybersecurity and elections. Bad knowledge management/transfer, i.e., the lack of knowledge, can result in the failure of electronic and internet voting, as was the case in the Netherlands (Dueñas-Cid, 2024) and Åland Islands (Article IV), respectively, or delays in the resolution of cyber-attacks and crisis, like Costa Rica's 2022 ransomware attack (Kosevich, 2024).

Knowledge transfer (KT) literature regarding elections is seemingly non-existent[1]; while on the other hand, knowledge transfer literature regarding cybersecurity is vast and even specialised (e.g., Rhee et al., 2009; Feledi et al., 2013; Ben-Asher & Gonzalez, 2015; Safa et al., 2016; Gupta & Wolf, 2018; Pala & Zhuang, 2019), however, not from the national or public administration perspective[2]. With all this in mind, this dissertation answers the following research question: how can knowledge transfer be conducted regarding elections and cybersecurity, and what are their benefits for public administrations? To answer this question, the insights presented in the individual articles will be analysed through the lens of the Dynamic Knowledge Transfer Capacity (DKTC) model, a KT framework "…particularly well-suited to analyze complex systems with multiple stakeholders…" (Parent et al., 2007, p. 90). According to the aforementioned authors, the DKTC allows the user to view KT from the process itself and the existing capacities (i.e. assets) for successful KT. The DKTC will be used to classify the insights of the articles and clarify their role in knowledge transfer.

While the overarching discussion focuses on KT, each article also adds to their individual fields. Article I examines the state of national cybersecurity throughout the world, presenting regional trends and differences, while introducing a plethora of countries that can be considered as role models for various best practices. Article III delves more specifically into national cybersecurity strategies and attempts to uncover any trends in them related to international cooperation, neutrality, and warfare/conflicts. On the side of elections, Article II demonstrates the use of Business Process Model and Notation to simplify electoral laws to make them more comprehensible to various stakeholders, while Article IV explores a failure of implementation of an internet voting system, while creating a theoretical framework that could explain the relationship between all the elements and stakeholders in the given context. Article V goes one step further and tries to apply the framework of Article IV in a practical manner in order to assist in the future implementation of an internet voting system. Articles III, IV and V have been presented at international conferences, the first and the last of them by the author of the dissertation.

Next to this introduction, the dissertation is structured into five distinct chapters. Chapter 1 focuses on the theoretical background of knowledge transfer, elections, and cybersecurity. It delves deeper into the topics and explores past literature, specifically within the context of public administration. Chapter 2 presents a methodological summary of the Articles being used for this dissertation. It discusses the research designs, the data collection and analysis procedures and the limitations that the individual Articles have. Chapters 3 and 4 deal with the results and answer the research question. And finally, Chapter 5 brings together everything for a formal conclusion.

[1] As at the writing of this dissertation in early 2024. For more information, please view the subsection of 'KT in elections' starting on page 19.

[2] As at the writing of this dissertation in early 2024. For more information, please view the subsection of 'KT in cybersecurity' starting on page 23.

Abbreviations

BPMN	Business Process Model and Notation
DKTC	Dynamic Knowledge Transfer Capacity
EMB	Electoral Management Body
IVS	Internet Voting System(s)
KM	Knowledge management
KS	Knowledge sharing
KT	Knowledge transfer
NCSI	National Cyber Security Index
NCSS	National Cyber Security Strategy

1 Background

> *"There are people who only want to know for the sake of knowing: it is a base curiosity. Others seek to know in order to be known themselves: it is a shameful vanity, and these do not escape the taunts of the satirical poet who said for the benefit of their peers: "For you, knowledge is nothing, if another does not know that you know." There are still people who acquire science to resell it and, for example, to make money or honours from it: their motive is ugly. But some want to know in order to edify: that is charity. Others to be edified: that is wisdom. Only men in these last two categories do not abuse science, since they only apply themselves to understanding in order to do good."* (Bernard of Clairvaux, 1953, p. 429–430)

This chapter is subdivided into three main sections and deals with the background information necessary to better understand this dissertation and the corresponding articles. The first section introduces knowledge transfer as part of knowledge management, before delving into the literature review of knowledge transfer in public administration, the Dynamic Knowledge Transfer Capacity (DKTC) model and a selection of knowledge management/transfer tools. The second section introduces elections, electoral management, internet voting and ends with a subsection on knowledge transfer in elections. The final section deals with national cybersecurity, the corresponding national strategies, and finishes once more with a brief review of knowledge transfer literature in cybersecurity.

1.1 Knowledge Management and Transfer

Knowledge management (KM) is defined as the way an institution captures, transfers, creates, and leverages its intellectual assets to become more efficient, effective, profitable, and to solve problems of international context (Yao et al., 2007). In the context of public administration, KM must be fully aligned with the administration's objectives and provide effective services and functions to implement the existing public agenda and a stable, just, orderly, secure, and prosperous society with an acceptable level of quality of life and with continuous development of its citizens for competitiveness in the regional and global economies (Wiig, 2000).

Previous research in the field of KM in the last three decades has been primarily centred around the general field itself (24% of the 1016 written articles) and around 5% on knowledge transfer and knowledge sharing (combined); the use of these last two terms as keywords is also quite extensive (Farooq, 2024). In regard to the public sector, KM understandably presents less publications and the most recent literature review from 2015 established that out of the 180 published articles, knowledge innovation was discussed in 11% of the articles, while personal and organisational learning were discussed in another 10% of the articles (Massaro et al., 2015).

Argote & Ingram (2000) define knowledge transfer (KT) as the process through which one unit (e.g., an individual, a group, a section, etc.) is affected by the experience of another within the context of an organisation. Outside of one, in between organisations, the units are replaced by firms, entities, institutions, or other larger organisational units (Easterby-Smith et al., 2008). In any case, KT can take place in both directions, and more importantly, "*… the recipient needs to be motivated to gain knowledge, and the donor* *must have something worthwhile to offer*." (ibid., p. 679) Transferring knowledge, or its attempts, can create new knowledge (Argote et al., 2003).

Knowledge sharing (KS) references the transfer of technology, skills, and wisdom between an organisation's units (Tsai, 2002; Wang et al., 2009). Depending on the different dimensions and contexts, the definition might be tweaked, and even include the wording of the previous term, e.g., KS is the process where two or more parties transfer knowledge (Farooq, 2020). Cummings (2003) presents a possible clarifier between these terms in a footnote: "*In most knowledge-sharing situations, reciprocal knowledge exchanges, rather than one-way knowledge transfers, are either sought or occur…*" (p. 7). However, he explains that even if the exchange is reciprocal, each participant is either a donor or recipient of knowledge, at a time (Cummings, 2003).

Knowledge innovation is a term that has no concrete definition. In their literature review, Massaro et al. (2015) use the term to refer to articles discussing innovation within the parameters of their study on KM. Traditionally, in KM literature 'innovation' is seen as the outcome, and knowledge has a role in the process (Quintane et al., 2011). Quintane et al. (2011) posit a new definition: innovation is new knowledge that is duplicable, new in the context it is introduced to and with demonstrated usefulness.

For the purpose of this dissertation, the author will not debate the minute nuances between KT and KS, since this is outside the scope, but will use them as synonyms, with KT being the primary term used. Knowledge innovation has been included since it has appeared in public administration literature reviews, the term is related to the previous two, and because it can be the result of new knowledge created through KT. The following subsection delves deeper into past studies of these concepts in public administration literature.

KT in Public Administration

Since as early as the 1970s, KT was being studied empirically for the field of public administration. Bowman (1978) analysed the importance of sources of administration knowledge, barriers to the use of that knowledge, and how to transfer research findings into the practical world. He found that both theoreticians and practitioners saw their own group as the "*… most significant source of information…*" (p. 569), although some considered that members of the opposite group would also be relevant sources of information. More importantly, a general belief was unearthed: *"… the practicality of research and its applicability to specific situations should be the objective…"* (p. 569). Some barriers to KT include communication and status issues, resistance to change, and lack of incentives to implement new ideas. And finally, KT would be best accomplished through courses, training programmes and seminars. (Bowman, 1978) In the end, this article wished to illustrate that the chasm between theoreticians and practitioners was not as deep as was thought.

Burch V. & Strawderman (2014) discuss another barrier to KT in public administration, namely generational differences. They posit that the digital natives and later generations are creative, desire to solve problems and pursue factual data, which leads them to be aware of the need, and therefore conduct, constant skill development and technological updates. Thus, *"… work-related material and information must come quickly in small bits…"* (p. 72), tasks should have end goals, and search – discover – rewards capabilities should be prevalent within responsibilities. In short, adopting gamification characteristics would increase KT and employee retention in public administration (Burch V. & Strawderman, 2014), not to mention the impact it would have on productivity and efficiency.

Past research in public administration KT has also involved case studies, ranging from local to national levels. Rashman and Hartley (2002) investigated the facilitators and barriers to interorganisational KT at a local-level scheme in the UK. The enablers included curiosity to find out new ways of doing things, improving performance, and the desire to support the institution. The barriers included, but were not limited to, lack of resources, initiative fatigue, their constraints, and deficiencies. Similarly, Yao et al. (2007) studied knowledge sharing within the context of Hong Kong public administration. Their findings indicated that KM and KS were welcome, however, the biggest barrier was the culture and smaller barriers included budget deficits (i.e., lack of resources, low morale, and fear of increased workload).

More specifically, in the field of political science (in the subfield of policy studies), a specialised term appears – policy transfer. The most cited, Dolowitz and Marsh (2000), define it as the *"…process in which knowledge about policies, administrative arrangements, institutions and ideas in one political setting (past or present) is used in the development of policies, administrative arrangements, institutions and ideas in another political setting."* (p. 5) This term has appeared in public administration literature due to its inherent and applicable nature. However, it is important to remember that "[k]*nowledge transfer is more extensive than policy transfer."* (Stone, 2012, p. 483) Policy transfer might occur due to the necessity for solutions, the wish to improve in international reputation and/or national political support, the desire to persuade others of the necessity of the said policy, among other reasons (Savi & Randma-Liiv, 2013). It may be 'forced' upon as a condition of international aid, membership requirements, or just be the result of best practices and international harmonisation. Thus, it would be important to select the appropriate role model(s) from which to 'receive' such policy transfer. Country likeness (in terms of geography, culture, linguistic and historical ties, etc.) and success have influenced such decisions. (Savi & Randma-Liiv, 2013) And while globalisation brought with it openness and availability of information and solutions to policy issues, all this information is tailored to the location that implemented it in the first place. Therefore, not everyone does (or should) copy-paste when policy transfer is involved. Some copy the desired items, and during implementation, tweak them to suit the existing context and conditions (Zhang & Yu, 2019), while others look for policies in countries experiencing similar situations and problems (Savi & Randma-Liiv, 2013).

Dynamic Knowledge Transfer Capacity (DKTC) model

Parent et al. (2007) proposed a model to explain organisational knowledge transfer (Figure 1). Their Dynamic Knowledge Transfer Capacity (DKTC) model is a framework that identifies *"… the components required for social systems to generate, disseminate and use new knowledge to meet their needs."* (p. 85) It allows the user to view KT from the process itself and from the existing capacities (i.e., assets) for successful KT. The referenced social system is defined as a group of individuals in either loose or tight relationship that is formed to respond to specific needs, e.g., an organisation, company, state, region, country, etc. The model (Figure 1) includes two pre-existing conditions (need and prior knowledge) and four capacities, which influence each other. The 'need' refers to the purpose or problem that involves multiple stakeholders and allows identifying what new knowledge is required, who are the stakeholders, and what is the current state of the knowledge (i.e., prior knowledge), both tacit and explicit. (Parent et al., 2007)

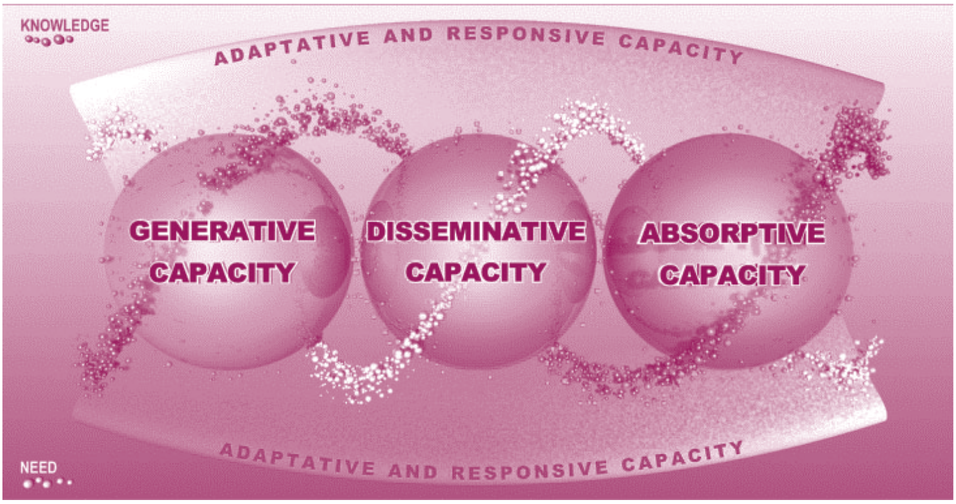


Figure 1. The Dynamic Knowledge Transfer Capacity model (Parent et al., 2007, p. 86)[3]

The four capacities of the model (Figure 1) are:

- Generative: involved in discovering or improving knowledge, and the derived processes, technologies, products, and services.
- Disseminative: involved in contextualising, formatting, adapting, translating, and/or diffusing knowledge.
- Absorptive: involved in recognising valuable new knowledge, assimilating it, and applying it.
- Adaptive and Responsive: involved in continuous learning and renewing the elements of KT for improvement.

According to the authors, all these capacities are needed in varying degrees for successful KT. The DKTC model focuses on the 'assets' necessary to improve KT, and if any are missing, these need to be cultivated or obtained. Finally, this model is suited to analyse complex systems with multiple stakeholders, which comes in handy when discussing public administration.

The DKTC model has been applied in a couple of past studies. Ekirapa-Kiracho et al. (2014) used it in combination with another framework to explore the capacity of research producers and users in Africa to generate, disseminate and use findings, and examine their strengths and weaknesses. In the same year, Rezania & Ouedraogo used the model within the business field, focusing on identifying the capacities for KT in an enterprise resource planning implementation project that ran from 2008 to 2011. Other authors have used the DKTC model as a stepping stone to elaborate their own KT models tailored to specific subfields. Vizecky (2011) applied it for the topic of business intelligence while, most recently, Zackarias et al. (2022) used it as the basis for their conceptual model to improve KT between junior and senior employees in engineering projects.

[3] Reproduced as originally introduced, with the written permission of Dr. Mario J. Roy, co-author of the original source.

KM/KT tools

Knowledge is part of three basic elements of any organisation – members, tasks and tools/assets – and the interactions between them (McGrath & Argote, 2001). KT can occur by moving the members, task, tools, and/or interactions from one social unit to another (Argote & Fahrenkopf, 2016). Argote & Fahrenkopf (2016) have gathered that tools themselves have had a positive effect in KT, with a myriad of them available in literature and practice.

Massingham's (2014) case study of an organisation examined the effectiveness of such tools in that setting. The effectiveness was measured as the impact on performance improvements inside the institutions. In the context of the case study, the most successful tools were future capability requirements, sourcing decisions, and knowledge valuation (Massingham, 2014). Basically, knowing current individual gaps, thinking objectively about future needs, and making appropriate decisions to fill and/or resolve them. Mazorodze & Buckley (2020) also studied various KT tools within the context of knowledge intensive institutions in Namibia. Their study concluded that the three most effective tools within their studied context were communities of practice, mentoring, and storytelling (Mazorodze & Buckley, 2020). Table 1 presents a selected list of the KM/KT tools used in both articles.

Table 1. List of selected KM/KT Tools presented by Massingham (2014) and by Mazorodze & Buckley (2020)

Tool	Description
Coaching[4]	Transference of knowledge focusing on immediate problems and opportunities.
Communities of practice	Transference of knowledge through formal or informal groups.
Competency mapping	As-is competency levels were compared against management expectations to identify the needs and produce a gap analysis.
Double-loop learning	Challenges pre-existing assumptions by modifying them based on experience.
Future capability requirements	Needed capabilities are identified and categorised into different groups.
Interviews	Transference of knowledge from the interviewee to the interviewer.
Knowledge repositories	Transference of knowledge via digital warehouses of documentation and expertise.
Knowledge valuation	Allocation of a score to gauge the knowledge of individuals and allow for a gap analysis.
Mentoring	Transference of knowledge from an experienced individual to one that is not.
Mind maps	Transference of knowledge through the expression of an individual's intuition and judgement toward the resolution of new problems.
Parallel thinking	Brainstorming method that makes participants focus on one perspective at a time.

[4] According to Mazorodze & Buckley (2020), coaching and mentoring are not synonyms, and are in fact different KT tools.

Tool	Description
Sourcing decision	Responsibilities are assigned to specific stakeholders, in or outside the organisation, who would own a resource.
Storytelling	Transference of knowledge through narratives which can build a shared understanding.
Succession planning	Development of plans to transfer knowledge before an individual leaves the organisation.
Video taping	Transference of knowledge from the interviewee to the interviewer, but with the possibility of being reused.

Information technologies have also become KT tools. As a prime example, knowledge repositories are *"…online storehouses of expertise and documentation about a specific domain and discipline…"* (Mazorodze & Buckley, 2020, p. 5). The issue is that these databases are considered to be private, and from an organisational perspective, they allow people to find relevant information and knowledge easily, help connect people knowledgeable on the topic, reduce learning and training times, and allow for the potential discovery of new knowledge (Mazorodze & Buckley, 2020). Hypertext itself has been touted as a KT tool by Swift (1991). Hypertext allows for the creation of knowledge repositories but can be used in conjunction with other ways of representing knowledge. It allows users non-linear paths to access information, i.e., it lets the user make their own choices of what knowledge to access based on their needs. The only requirement is that the links must be organised in a pattern or structure which is meaningful and understandable for the user. (Swift, 1991)

Discovering knowledge in a database is not new. In fact, since 1991, it has been a field of its own, knowledge discovery in databases (KDD), which researches how to uncover useful and/or interesting knowledge from these sources (MIT, 1991). KDD is a subfield of machine learning and focuses on large amounts of uncertain data. However, as seen from Article **I**, the data in the discussed database is already information and is no longer uncertain. Thus, in this case, knowledge discovery (and its subsequent transfer) can also be conducted by non-machines. This point is further explored by Dougherty (1999) who posits that despite the dominating IT-led perspective in KM and KT, databases are just tools, and in the end, KT depends on the choices made by individuals. This is all to say that the existence of KT tools does not guarantee KT by itself, but it may simplify, aid, enable it.

1.2 Elections

This subsection explores elections, specifically dealing with electoral management and internet voting. These last two concepts were the overarching themes for Article **II**, and Articles **IV** and **V**, respectively. Article **II** presented a way to simplify the information relative to electoral management as a desire for easier understanding and teaching. Article **IV** analysed a unique case study involving a failure of implementation of internet voting. Through this analysis, a theoretical artefact was created to attempt to explain it. This artefact was further used in Article **V** to try to understand the current efforts related to the implementation of internet voting in a different environment, and to help identify pitfalls and issues that might arise during its inception. The following section is devoted to explaining the topics of electoral management, internet voting, and knowledge transfer in elections.

Electoral management

Managing or administering an election in a country is an enormous task, and sometimes it is the largest activity that has been organised in that country (International IDEA, 2014). With the increasing globalisation, electoral administration and management has become more scrutinised. As new technologies appear, some have been introduced as solutions for greater efficiency in these endeavours. The term 'election administration' refers to how the register of electors is compiled, how they vote, and how those votes are counted (James, n.d.). Electoral management, on the other hand, alludes to the entity governing the elections, and the different tools, roles, and functions that it might have to pull such an incredible endeavour off (ACE, n.d.).

The term electoral management body (EMB) refers to the body or bodies responsible for the management of an election, regardless of the size of the existing institutional framework. It can be responsible for some or all elements necessary[5] for an election and might take on other tasks[6] relevant to the process. EMBs should be guided by multiple principles, but for the purpose of this dissertation, the author presents three of them: transparency, efficiency, and professionalism. Transparency is necessary since the electoral process is highly scrutinised and such lack might bring about suspicion. Efficiency is required so that all allocated funds are properly spent, and services are fully delivered on time and correctly. Professionalism is essential since the whole process needs its procedures to be implemented accurately and correctly by competent staff. This translates to the need to transfer the correct knowledge and skills to electoral administrators. (International IDEA, 2014)

The EMBs' work is cyclical because the nature of the electoral process itself. Throughout the so called 'electoral cycle', EMBs might have varied powers and responsibilities relative to the activities of the process. The electoral cycle (illustrated by Figure 2) is defined as being:

> "[t]*he full series of steps involved in the preparation, implementation and evaluation of an election or direct democracy instrument, which is viewed as one electoral event in a continuing series. In addition to the steps involved in a particular electoral process, it includes preelectoral activities such as the review of relevant legal and procedural provisions and electoral registration, as well as post-electoral evaluation and/or audit, the maintenance of institutional memory, the process of consultation and the planning of the forthcoming electoral process.*" (International IDEA, 2014, p. 400)

Resources, human and otherwise, are also dependent on the cycle and might fluctuate as a result of the current phase the cycle. Poll workers, for example, are temporary stipended volunteers that are necessary for delivering the election. Their responsibilities (which might be subject to change depending on each country) include setting up polling stations, greeting voters, ensuring that only those that are allowed and can vote do so, handing out the ballots, ensuring the secrecy of the vote and order at the polling station. (Clark & James, 2023)

[5] These necessary elements include the determination of who can and is allowed to vote, the receipt and validation of the electoral nominations, the administration of the poll, and the count and tabulation of the votes (International IDEA, 2014).

[6] These refer to registering voters, delimiting boundaries, educating and informing voters, monitoring media, and resolving electoral disputes (International IDEA, 2014).

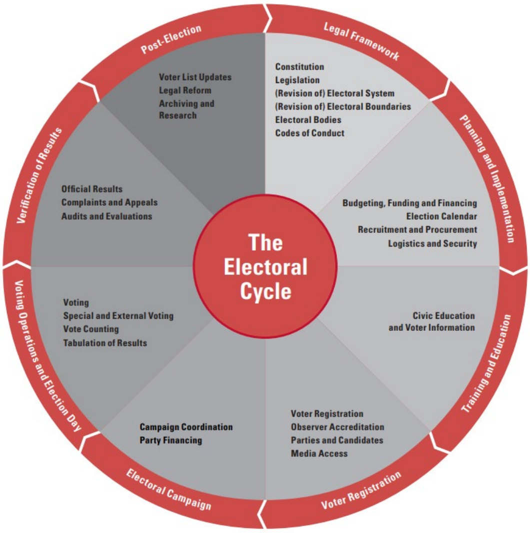


Figure 2. The Electoral Cycle (International IDEA, 2014, p. 16).

Voting is held in the 'Voting Operations and Election Day' phase of the electoral cycle. Balloting can happen during election day in a specified official location, or outside these parameters. When the latter happens, it is called convenience voting, a term which refers to any type of voting that allows voters to cast their ballot at a place and time other than those on election day (Gronke et al., 2008). The idea is to make it easier and/or cheaper for the voter to vote and this can be done by mail, phone, secure website, or the web, or physically earlier at satellite locations or voting centres. While the benefits of increasing turnout seem positive, other concerns related to costs, fraud and coercion always appear when discussing convenience voting. (Gronke et al., 2008) Another issue that has been analysed involved a case study in the US where withdrawn candidates performed better through mandated voting by mail, because citizens were not exposed to information that was revealed in the final weeks and days leading to the election day (Meredith & Malhotra, 2011).

One final consideration regarding convenience voting is that electors prefer to do things the way they have done in the past (Alvarez et al., 2018). This is tied to the adoption of technology where *"…prospective users are often uncertain about the advantages and disadvantages of new technologies."* (p. 95) Therefore, if this uncertainty is reduced or removed, and the advantages are verified, the individual might proceed with the adoption. However, if these technologies are framed negatively, for example by focusing on election fraud as in the case study from the US, less citizens will think about using convenience voting methods and would prefer to keep on using paper ballots during election day. (Alvarez et al., 2018) The next subsection delves a little deeper into one specific type of convenience voting, i.e., Internet voting or i-voting, exploring its characteristics and dimensions, in addition to other subjects.

I-voting

Internet voting, or i-voting is a type of convenience, remote and electronic voting. Convenience, as previously stated, because it allows the elector more flexibility of where to and when (within the established legal timeline) to vote. Remote, because the voter does not have to be physically located near or in a designated location to vote and because it *"…depends on an underlying communication network to function properly."* (Gibson et al., 2016, p. 279) And finally electronic, because it depends on electronic technology in order to work properly. Therefore, Internet voting is a type of remote electronic voting that allows the voter to cast their vote through an electronic device connected to the Internet, without having to be present in a supervised environment. (Gibson et al., 2016) A system that allows Internet voting is therefore referred to as an IVS, i.e., an Internet voting system.

At the time of writing this dissertation, in March 2024, International IDEA's (2024) database indicated that a total of 15 countries out of 174 in the world were currently using IVS. Closer inspection of this database revealed that the evidence for this claim related to the approval for the use of IVS by the corresponding legislation (i.e., electoral law) and/or instructions on how to vote online. Figure 3 showcases the countries that fulfil the preceding parameters and were identified by International IDEA.

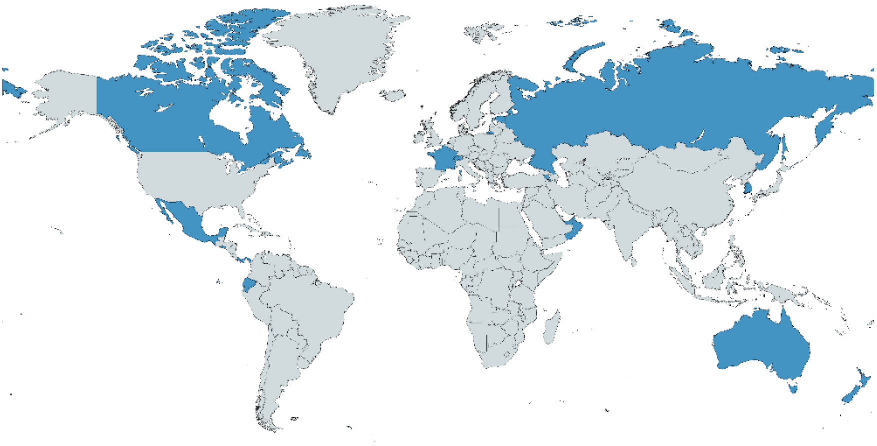


Figure 3. World map indicating countries that have approved the use of IVS in their legislation (data sourced from International IDEA, 2024)

Internet voting, as any other activity, may exhibit drivers and barriers when attempting to implement it. Licht et al. (2021) summarised these into two lists of fifteen elements each. Some of the drivers include, but are not limited to, universal access, the reduction of costs, improvement of processes, increasing turnout or at least preventing its further decline, being a form of convenience voting and the socioeconomic status of the voter. On the other hand, barriers are not limited to changes in the legal requirements, security concerns, theoretical-technical vulnerabilities, lack of a framework, lack of verifiability, general mistrust in technology, in government and in EMBs.

There is a specific driver that characterises Internet voting – the reduction of costs. In essence, Internet voting is the most cost-effective and cheapest way of doing so (Krimmer et al., 2021). Cost accounting was used to analyse multi-channel local elections in Estonia. This was also the first instance that BPMN was used in order to model electoral activities, which in turn allowed the detection of potential expenses connected to such processes. In the end, Internet voting was around 75% cheaper than election day voting in ordinary polling stations, making it extremely cost efficient. It also concluded that by introducing Internet voting as an additional channel unused capacities can appear, and other voting channels are affected with a reduction in cost effectiveness, because they are not being used as much as they would have been. (Krimmer et al., 2021)

Having considered the information above, there were still some locations that wished to implement Internet voting, like the Åland Islands. Unfortunately, as described in Article **IV**, their attempt did not succeed. And even if such failures do not detract other countries, like Moldova, to try it on their own, they can still be used to learn lessons and to attempt to facilitate the implementation.

KT in elections

KT in elections is a topic that has seen very limited research[7]. A systematic search in Web of Science and Scopus of the terms 'knowledge transfer' or 'knowledge sharing' and 'elections' resulted in a very small sample, of which few articles, if any, could be relevant to this dissertation. Using the first combination leads to Maurer's (2009) paper discussing knowledge transfer during election campaigns and focusing on how media and politicians present the parties' programmes to the citizens. The rest of the papers (forty-five other results) focus on either term of the combination, without any linkages between them.

The second combination, this time using 'knowledge sharing', yields a higher number of results (a hundred eighty-six results), but similarly, most of the results are focused on either term separately, without bringing them together, or dealing with 'sharing' and 'elections'. The more relevant articles investigated sharing information or knowledge online for political purposes or prior to an election (Beam et al, 2016; de León et al, 2023). The author also swapped 'elections' for 'electoral administration' or just 'electoral', with considerably fewer than a dozen results and similarly lacking combined research.

An additional attempt was made with the terms 'knowledge tool' and 'elections'. The most relevant result is a chapter in the proceedings of a KM conference, a case study about the US investigating the use of Twitter as a tool that affects the voters' opinions (Alfarhoud, 2018). The rest of the one hundred fifty results once more balanced results for 'knowledge' and 'tool' or 'tool' and 'elections', with less relevancy to our topic. A final attempt was made with the terms 'knowledge transfer tool' and 'elections', but no relevant results were found. Similar investigations were conducted using Google Scholar, but no new insights were uncovered, even though the number of possible results inflated into thousands and millions.

1.3 Cybersecurity

This subsection explores the concept of cybersecurity and its related terms, national cybersecurity and national cybersecurity strategy. These last two concepts were the overarching themes for Articles **I** and **III**, respectively. Article **I** explored national cybersecurity from a global perspective, having analysed 161 countries. It presented similarities and differences in the national approaches, and pinpointed countries that could be used as role models based on practical endeavours. Article **III** explored all national cybersecurity strategies publicly available at the date of the study from a perspective of conflict/warfare, neutrality, and international cooperation. It outlined their recurrence and drew inferences regarding national positions with regard to these topics. The following subsection is devoted to explaining the topics and exploring past research related to knowledge transfer.

[7] At the time of writing this dissertation in early 2024.

A nation's cybersecurity

Cybersecurity is one of those elusive terms that have no fully accepted definition, starting from the fact that it can be written as a single word, or as 'cyber security', and even their capitalisation is in question. ENISA (2015) posited that it is an umbrella term which is impossible to define because it would not be able to *"…cover the extent of things cybersecurity covers…"* (p. 7) and that relevant contextual definitions are recommended. A few years later in 2017, ENISA defined cybersecurity on the basis of cyberspace, as presented in Article **I**. Nevertheless, it is not the only definition in academia and the rest of the world follows the recommendation of selecting the definition that is most relevant and fits their corresponding context. The term's definition undergoes further modifications depending on the language, and in some cases, it is replaced by other terminology (e.g., information security [Korea], cyber defence [Israel], digital security, etc.) based on the national environments and situations. Table 2 presents some definitions of the term cybersecurity. These were mostly gathered from authorities in charge of the topic, whenever possible, or the legal acts that cover it. The definitions that were in other languages than English (e.g., French and Italian) have been translated by the author of this dissertation). The definitions have been presented in the alphabetical order of their countries/institution.

Table 2. Various definitions of cybersecurity

Original Language(s) / Country	Definition	Source
French / France	State of an information system that is resistant to cyberattacks and accidental failures occurring in cyberspace. Cybersecurity is ensured by cyberprotection as well as, in case of the State, by cyberdefense.	ANSSI, 2023
Italian / Italy	Set of measures – physical, logical and procedural – aimed at guaranteeing confidentiality, integrity, and availability of information processed via IT systems.	ACN CSIRT, (n.d.)
English / None - ITU	The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: • Availability • Integrity, which may include authenticity and non-repudiation • Confidentiality	ITU, 2008

Original Language(s) / Country	Definition	Source
English / UK	The protection of devices, services, and networks – and the information on them – from unauthorised access, theft, or damage.	NCSC, (n.d)
English / USA	1. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. 2. The process of protecting information by preventing, detecting, and responding to attacks. 3. The ability to protect or defend the use of cyberspace from cyber attacks.	NIST, (n.d)

Considering the various definitions and interpretations given to it based on the different contexts, 'national cybersecurity' goes one step further and adds to it. Once more, we find ourselves with a term that has no universally accepted definition, although it is widely used throughout the world (NATO CCDCOE, 2012). The NATO CCDCOE (2012) defined it as *"…the focused application of specific governmental levers (which includes both incentives and regulation) and information assurance principles to public, private, and relevant international ICT systems, and their associated content, where these systems directly pertain to national security"* (p. 42–43), while the author of this dissertation, in Article **I**, applies ENISA's definition of cybersecurity to the national level, to be achieved by the government in charge and the relevant stakeholders.

Given that cybersecurity has been identified as an umbrella term, and the addition of the word 'national' has extended this 'umbrella' to encompass a whole nation, it has not been established what the term 'national cybersecurity' covers. The NATO CCDCOE (2012) posits that national cybersecurity in turn has five mandates, sub-topics so to say, that are part of it: cyber military, countering cybercrime, intelligence and counter-intelligence, critical infrastructure protection and national crisis management, and cyber diplomacy and internet governance. Article **I** applies the methodology of the NCSI, and in addition to including almost all previous mandates[8], it expanded the list of mandates to include the development of cybersecurity policy, cybersecurity education and awareness, protection of digital services (both public and private), protection of personal data, the development of electronic identification and trust services. This 'table of contents' related to national cybersecurity while theoretically constructed from best practices by experts and practitioners, might not yet be complete. However, it does provide a first glance into national cybersecurity and what is necessary in practice to maintain it. The next paragraphs present national cyber security strategies (NCSS). As a subtopic of national cybersecurity, these official documents are most of the time publicly available to present a nation's approach to the topic.

[8] The NCSI presented 46 indicators grouped into 12 capacities. Of the NATO CCDCOE (2012) mandates, the NCSI methodology did not include the 'intelligence' responsibility and renamed 'counter-intelligence' as 'cyber threat analysis', and the 'cyber diplomacy and internet governance' as 'contribution to global cybersecurity'.

National cyber security strategy

Article **III** explores the concept of a national cyber security strategy (NCSS) and defines it as *"…a document that identifies interests and ambitions related to national cybersecurity and communicates the use of resources to reach those goals."* (p. 421) Their structure and contents may vary depending on the national postures, however, being high-level strategic documents, common elements can be found in them, including, but not limited to, presenting the national values and the strategic vision, assessing the current situation and future challenges, and defining goals, actions, activities and/or timelines to address them (Article **III**).

Given the aforementioned characteristics, it is common to find that academic literature in the field of cybersecurity includes multiple articles either analysing individual NCSSs or comparing the NCSSs of different countries. Luijif et al. (2013) studied the NCSSs (published between 2009 and 2011) of ten countries from an inductive standpoint in order to discover similarities and differences. Differences included the presence or lack of a definition for cyber security, their focus on the national approach, and the scope of the document. Similarities accentuated the need for a whole-of-society approach, the existence of global threats, and the protection of critical infrastructure. (Luijif et al., 2013) Newmeyer (2015) analysed various existing NCSSs in addition to best practices published by cybersecurity related international organisations to offer recommendations on what the NCSSs of developing countries should contain. Some of the recommended items include: reference to political will, the establishment of public-private and/or interagency multi-stakeholder groups, the existence of a legal framework, protection of critical infrastructure, emphasis on education, the creation and administration of incident and crisis response entities, and the protection of civil liberties. (Newmeyer, 2015)

Most recently, Oruj (2023) evaluated the cybersecurity strategies of twelve nations in an attempt to improve the understanding of the term 'cybersecurity' from a global perspective. Nevertheless, the conclusion makes it clear that *"*[c]*ountries have different views on cybersecurity…"* (p. 114), and even if countries understand the need for international cooperation, the absence of a common terminology makes it harder for them (Oruj, 2023). Odebade & Benkhelifa (2023), ten years after Luijif et al. (2013), once more compared ten NCSSs to identify strengths and weaknesses. Some of the latter include the lack of an implementation or constant evaluation plan, the lack of budgetary transparency, and missing overarching principles (e.g. scope, timelines, roles, resource allocation, etc.). At the end of their paper, they posit some recommendations for the improvement of NCSS.

KT in cybersecurity

Unlike elections, knowledge transfer/sharing and cybersecurity has seen more research. Sharing previous relevant experiences and knowledge is considered an indispensable resource for cybersecurity awareness (Rhee et al., 2009). It is also reduces, mitigates and thwarts security incidents risks (Arachchilage & Love, 2014; Tamjidyamcholo et al., 2014; Ben-Asher & Gonzalez, 2015). For the private sector, sharing cybersecurity knowledge can reduce the tendency of stakeholders to underinvest in cybersecurity (Gordon et al., 2015).

Regarding the internal workings of an organisation, knowledge sharing positively affects an employee's attitude to comply with cybersecurity policies, in addition to furthering cybersecurity knowledge (Safa et al., 2016). On a larger scale, Feledi et al. (2013) present a web-portal through which cybersecurity knowledge can be shared among different organisations. Some of the identified barriers to the adoption of this tool included (ibid.):

- unwillingness and lack of justification to contribute, unless clear benefits were presented;
- trust between the users, since sharing knowledge might lead to competitive disadvantages;
- unclear definition of the target group of users, since sharing knowledge might take away competitive advantages;
- attraction and maintenance of a critical mass of users to guarantee the usefulness and sustainability of the web-portal;
- maintaining and assuring the quality of the knowledge, which could be either left to the user community or moderators.

As in the previous case, Tamjidyamcholo et al. (2014), identified a similar barrier in a virtual community, which showed low willingness for members to share knowledge. This stemmed from the idea that sharing knowledge might also increase cybersecurity risks, since malicious actors could also have access to this knowledge and use it for their own purposes. Nevertheless, their findings indicated that knowledge sharing decreases cybersecurity risks.

Since cybersecurity and its subtopics permeate all sectors, other research has focused on more pointed questions. From an educational perspective, Gupta & Wolf (2018) attempt to answer whether knowledge from teaching and researching cybersecurity is transferable into practice, focusing on a university's IT department and its website. Their research suggests that this was the case in relation to research excellence[9] but not teaching excellence, institutional size, nor tuition costs (Gupta & Wolf, 2018). With a similar perspective, Waddell (2024) presents a human-centred[10] cybersecurity education programme developed for healthcare and using lessons learned from commercial aviation in Canada.

On a final, more technical point, there is a body of literature dedicated to cybersecurity information[11] sharing. Pala & Zhuang's (2019) literature review categorises the existing articles into 1) technical/conceptual (that discuss frameworks, and decision-supporting tools); 2) policy making (studying public-private partnerships, their lawfulness and information sharing agreements); 3) game theory (researching the balance between investing in cybersecurity, risks and privacy, in addition to mechanisms to improve information sharing); and 4) other analytics (focusing on alternative analytical models to game theory). The existing literature's position on information sharing and collective knowledge is that they are beneficial for strengthening mitigation and response capabilities and reducing the cost of cybersecurity investments. (Pala & Zhuang, 2019). These benefits are more than likely retained once information becomes knowledge.

[9] Cybersecurity research excellence is presented as having *"…papers accepted at prestigious cybersecurity conferences."* (Gupta & Wolf, 2018)

[10] Focusing primarily on the human risk factor (Waddell, 2024).

[11] Information is data (i.e., representations of facts that are unprocessed or unrelated) organised to produce meaning. Knowledge is one step higher in the hierarchy and is considered to be the product of information in combination with the person's experiences, intuition and expertise. (Zins, 2007)

2 Methodology

The research conducted for this dissertation followed a qualitative research design, and all articles, with the exception of Article **IV**, follow pragmatism as the research paradigm. The remaining article follows an interpretivist approach. While Article **II** does not investigate information systems or information and communications technologies, the findings can be applied to legislation applicable to these topics. In information systems, pragmatism has been presented as an alternative to interpretivism and positivism (Goldkuhl, 2012). According to Goldkuhl (2012), *"*[p]*ragmatism is concerned with action and change and the interplay between knowledge and action…*" (p. 136) and "[t]*o perform changes in desired ways, action must be guided by purpose and knowledge…"* (p. 139). Therefore, the purpose of an inquiry into a part of reality is to create knowledge to affect change in said part of reality. On the other hand, interpretivism looks to discover, acknowledge, reconstruct, understand, and use the subjective meanings existing in the world as the foundation for theories. (Goldkuhl, 2012)

Thus, Articles **I** and **III** are inquiries into the real world looking to construct more knowledge that is useful for action (in the fields of cybersecurity) through data assessment and intervention. Article **II** constructs knowledge by demonstrating a way to simplify information that is useful for the administration of elections. Article **IV** attempts to understand a case study and creates a theoretical framework that attempts to explain the study, while Article **V** works with this construct to provide constructive knowledge and engage change in another real-world case.

2.1 Research design of the articles in the dissertation

Articles **II**, **IV**, and **V** deal with single case studies. Case studies are known for being used for exploratory or descriptive purposes, but they can also serve for explanatory reasons (Yin, 2018). Yin (2018) justifies using single cases when these are critical, unusual, common, revelatory, or longitudinal. The cases in Articles **II** and **IV** are unusual (with Estonia's implementation of multiple ways of convenience voting and the Åland Islands' attempt to introduce internet voting, respectively), while that of Article **V** is unique (since it attempts to apply the framework of Article **IV** to the practical situation of Moldova's internet voting pilot).

The NCSI methodology was used in Article **I**. As described in that article, it was created by the e-Governance Academy as the foundation for the National Cyber Security Index (NCSI)[12], a live global index, and as a cybersecurity reference, assessment and capacity building tool. The methodology is based on literature review, with the additional step of a 'peer review' verification of said literature by two or more cybersecurity experts. The literature review part refers to the search and identification of publicly available official information that might fulfil the criteria of 49 different cybersecurity indicators[13]. The 'peer review' part of the process refers to the checks and verification of said information to make sure that it complies with the individual criteria of each indicator.

[12] The author of this dissertation has been assigned to the NCSI since 2018, assisting in the data collection and analysis of most, if not all, of the 177 economies that were present and had been published by September 2023 in the NCSI.

[13] The NCSI methodology was updated in September 2023 (NCSI, 2023). Article **I** was written at the start of 2023 when the previous methodology was applicable. The previous methodology had 46 indicators, while the current one has 49 indicators.

Information that fulfils the criteria is approved and published as part of that specific country's dataset. Filling the indicators with correct evidence will directly impact the country's score, which in turn will affect the country's overall rank in the NCSI. For more information, please refer to the methodological section of Article **I**. Article **III** also uses literature review. In this case, its application was much more direct since the research questions clearly indicated the literature to review, namely the NCSS. As Snyder (2019) posits, literature review as a methodology permits to identify all the evidence fitting a specific criterion to answer specific questions or hypotheses, thus summarising findings to discover areas where research and/or improvements are needed. In the case of Article **III**, since the hypotheses were specific and directly related to the NCSS, literature review was the best methodology to verify them.

Article **II** also made use of design science, which has been defined as the study and creation of artefacts being developed and used for solving practical problems of general interest (Johannesson & Perjons, 2014). In it, the steps designed by Peffers et al. (2007) for design science in information systems research were followed: identification and motivation of the problem, definition of the solution objectives, design and development, demonstration, evaluation, and communication. The demonstration of Article **II** was conducted on a single case study. Under this definition, this dissertation can also be categorised under this paradigm since it is attempting to improve upon knowledge transfer and information governance in public administrations through the introduction of useful artefacts.

2.2 Data collection and analysis

Considering the documentary nature of public administration, the attempts to find opportunities and deficiencies (i.e., trends) and/or to solve issues, data collection heavily relied on document analysis and secondary data analysis. Given the sheer number of countries included in Articles I and III (161 and 113, respectively), document analysis formed the basis of these publications. Article **I**'s data had been collected for three consecutive years and collated into the NCSI. While the NCSI itself contained 46 indicators (grouped into 12 capacities), not every country presented documentary evidence for each indicator. Still, given the constant update of the live NCSI, and the revision of data that might not have matched the criteria for the NCSI, more than 7,000 documents were analysed using the NCSI's methodology and summarised into 161 cases for Article **I**. Article **III** was smaller in scope, and only those countries that presented publicly available national cyber security strategies were selected for the study. This amounted to 113 documents analysed for the three main topics of the study.

Article **II** also used document analysis, because the Electoral Law was the main focus and its simplification into a BPMN diagram was the result. Since diving into documents was not sufficient for Articles **IV** and **V**, further information was collected through semi-structured interviews. In total, twenty-one interviews with electoral stakeholders were held in the Åland Islands by the writing team. The interviews prior to the Election Day in the Åland Islands were tailored toward a different topic. Nevertheless, once the failure of internet voting happened, the information obtained served as the background for our new focus. The rest of the interviews focused on trying to understand the reason(s) behind such failure. A dozen semi-structured interviews with stakeholders involved with elections, for Article **V**, served as background information for the practical application of the framework created by Article **IV**. Table 3 presents an overview of the articles and their research and data collection methodologies.

Table 3. Overview of the research designs of the Articles

Article	Main methodology	Data Collection			
		Document analysis	Interviews	Secondary data analysis	Literature review
I	NCSI	x		x	x
II	Design science and a single case study	x	x	x	x
III	Literature review	x		x	x
IV	Single case study	x	x	x	x
V	Single case study	x	x	x	x

The collected data was analysed using different approaches, which were either inductive or deductive, depending on the article being used. Articles **I**, **II**, **III**, and **IV** used a deductive approach, while Article **IV** applied an inductive one. Article **I** made use of the NCSI methodology, which presented 46 individual cybersecurity topics grouped around a set core (labelled as capacities) of 12 themes. Article **II** built on the idea that electoral laws could be made easier to understand and used the Business Process Model and Notation (BPMN) to demonstrate the hypothesis. Article **III** was similarly based around hypotheses which were constructed around the themes of warfare, neutrality, and international cooperation in national cybersecurity strategies, from which the corresponding coding ensued. The inductive approach was used in Article **IV**, categorising the data into core themes identified by using the NVIVO qualitative data analysis software. Finally, Article **V** employed a deductive approach by using the artifact created in Article **IV** as the theoretical starting point of the case study.

2.3 Limitations

A couple of limitations could be mentioned regarding this dissertation and the included articles. The first would be the application of non-governmental approaches to public administration research, as is the case with Articles **I** and **II**. In the former case, the NCSI was created and is currently managed by a nonprofit organisation (although there are records of countries using the Index to improve their own national situation), and in the latter case, the use of the BPMN comes directly from the private sector (although there have been instances of BPMN use in public sector research, see Article **II** for references).

The second more important limitation is the reliance on the availability and completeness of official information. In Article **I**, the NCSI, as-is, is completely based upon publicly available official information. Information that is not shared cannot be added to the record and appears as an absence rather than registering any attempts toward completion. Article **II** also depends on the accessibility of the electoral law and any other internal processes during the electoral cycle to map the activities correctly. Article **III** studied 113 countries out of 194 UN member states because these were the only ones that had a publicly available NCSS. Similarly, as in Article **I**, the lack of publicly available NCSSs does not mean that the country is not attempting to draft one or does not have some other process/artefact that replaces such a document. Article **IV** mentioned thatthe lack of information in a couple of instances due to secrecy and confidentiality, which might have brought further clarification to the creative theoretical framework.

Article **V** uses this theoretical framework in an ever-evolving situation that the author is not able to fully monitor from all possible perspectives, in addition to some information being withheld under the same reasons as in Article **IV**.

The third limitation, only applicable to this dissertation, concerns the DKTC. Its limitation is that the model does not take into account that useful knowledge can be created before a need is uncovered (Dooba & Downe, 2011). To put it into the perspective of this work, it would be the case of Article **IV**, a theoretical framework which was created as an explanation to a failure in implementation. The nature of the framework was such that it might have only served to explain this particular failure until a similar case appeared in the future, if at all. This was useful knowledge that could not be transferred outside the specific parameters of the failure of implementation. However, with the appearance of a new need, such as that of this dissertation or of Article **V**, this knowledge could now be transferred to fulfil the new need(s). While this limitation is part of the DKTC, it has not impacted this work in a meaningful way.

Given the compartmentalisation of the topics, the final group of limitations refers to those applicable to each and every one of the articles in this dissertation. The author kindly refers the readers to the corresponding articles to read more about them.

3 Results

This chapter presents the results of the individual articles in the context of KT. The first section will deal with KT and elections, while the last section will do the same for KT and cybersecurity. Given that the publications themselves provide novel knowledge, ideas, and concepts in their corresponding fields, not a lot of focus will be put on their corresponding findings (readers are kindly referred to the publications themselves for more information), but on their added value to knowledge transfer literature and concepts, as discussed in the background chapter.

3.1 KT regarding elections

Knowledge transfer regarding elections can be undertaken through the translation of the electoral law and processes into BPMN, as presented in Article **II**, in addition to creating theoretical frameworks to be applied in practice, as elaborated upon in Articles **IV** and **V**. The benefits of such approaches will be made clearer in the following paragraphs.

BPMN translation

Article **II** presents the idea of using BPMN to make electoral laws more comprehensible to multiple stakeholders. When applying the DKTC model, the author can identify that the existing knowledge involves the electoral code and all corresponding legislative instruments that regulate the elections. The discussed need can either be the one framed in the research question of this dissertation (i.e., how to transfer knowledge) or in the research question of the article (i.e., how to make electoral laws more comprehensible). The stakeholders involved can be classified as those part of the EMB and/or administering the elections, or as those not part of these bodies, i.e., the majority of the citizens/voters.

The use of BPMN would be a type of disseminative capacity when applying the DKTC model. The primary focus of this type of capacity is knowledge diffusion, and among the activities generally associated with this capacity, one of them matches the use of BPMN, adapting/translating knowledge to end-users' reality (see Parent et al., 2007). As mentioned in Article **II**, the instructions for poll workers are mainly derived from the electoral laws, and the more difficult they are to understand, the more difficult it becomes to deliver elections properly. Given that poll workers may yield specific powers during voting days, it means that if the implementation of the proceedings differs, the quality and integrity of elections may be affected. Other stakeholders that are also interested in this kind of information are the voters. As seen in the electoral cycle, there is a training and education phase during which voters can expect information to be shared with them. If the system presents multiple ways of convenience voting, this need for information and knowledge on how to proceed, compounds. Lack of transparency may have a direct consequence to the conduct of the voters, and thus directly impact the elections.

The translation of an electoral law into a BPMN diagram would clearly illustrate the regulations and outline the responsibilities of information-related behaviours across the different stakeholders involved in electoral management. It would also serve as a reminder to them about their specific rights and responsibilities they should follow in the corresponding steps. Additionally, it maximises the use of human, logistical and financial resources, and allows them to be more easily audited, as in the literature about the cost of elections. Finally, it would safeguard against issues caused by human error before, during, and at the end of elections. Such diagrams would also increase the transparency and openness of public administration toward citizens, which might positively affect their trust in the institution and the process. Organisationally speaking, it would harmonise and make trainings easier and make organisational shifts and changes in work practices faster to adapt to. In case of issues in the elections, audits would be easier to conduct since the processes and responsibilities are well and clearly documented. Figure 4 illustrates an example of a BPMN diagram created to represent the responsibility of a Voting District Committee for the process of advance voting, using the electoral law in force for Estonia’s 2019 Parliamentary elections.

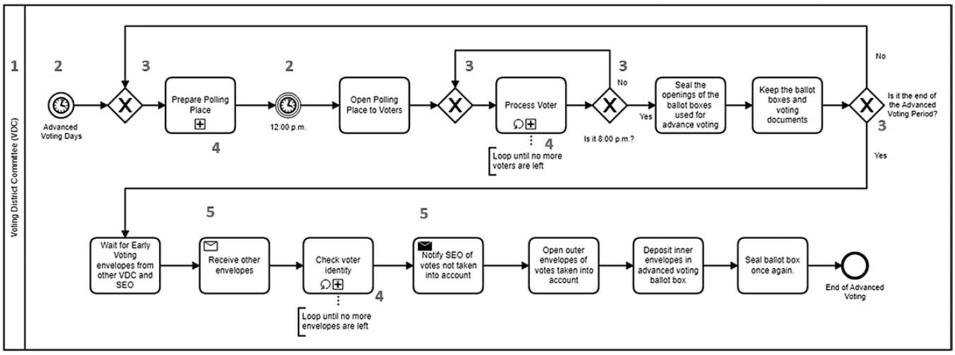

1
Voting District Committee (VDC)
2
Advanced Voting Days
3
Prepare Polling Place
4
2
12:00 p.m.
Open Polling Place to Voters
3
Process Voter
4
Loop until no more voters are left
3
No
Yes
Is it 8:00 p.m.?
Seal the openings of the ballot boxes used for advance voting
Keep the ballot boxes and voting documents
No
Is it the end of the Advanced Voting Period?
3
Yes
5
5
Wait for Early Voting envelopes from other VDC and SEO
Receive other envelopes
Check voter identity
4
Loop until no more envelopes are left
Notify SEO of votes not taken into account
Open outer envelopes of votes taken into account
Deposit inner envelopes in advanced voting ballot box
Seal ballot box once again.
End of Advanced Voting

*Figure 4. BPMN of the advanced voting delivery in the 2019 Parliamentary elections in Estonia (Article **II**)*

The BPMN diagram also serves as the way to transfer knowledge from one practitioner to another. It also segments a long process into its constituent activities, thus presenting the information in small understandable bits that reach out to an end goal. The creation of a diagram should not considerably impact the resources of public administration and they would only be updated if there are any changes in the corresponding law. On the other hand, it should have no impact regarding policy transfer; this should only happen at the level of the electoral law. If this does happen, then updating the diagram to reflect the new environment would be much easier, given that all activities have been separated and the process simplified.

The diagrams themselves combine a couple of KM/KT tools. Given that they would be specifically used within the context of elections, this means that a very specific group of people would be using it. Therefore, there are communities of practice and the transference of knowledge via mentoring is done through this formal group. Specific actors and stakeholders are identified, which means that sourcing decisions are easier to handle as every activity is assigned to a specific individual or entity. During the elections themselves, the diagrams can be used for coaching and supporting the decisions of the EMBs. Finally, given that some of the staff is not permanent, succession planning is made easier since the knowledge to be transferred is already illustrated in such a diagram.

The diagram itself can be drawn by hand or using IT. Since it is an illustration of an electoral law, it becomes a knowledge repository. The information contained in it can be hypertexted to provide additional information about the specific stakeholder, term or activity. Since it presents an as-is picture of the current electoral law, it makes it easier to see where improvements can be made and errors exist, so as to further improve the corresponding legislation.

Applicable theoretical frameworks

Articles **IV** and **V** are more specific in nature, dealing with the implementation of an IVS. The research team had headed to the Åland Islands to better study the costs of Internet voting and other voting channels during their elections. However, at the last minute their government decided not to implement Internet voting, thus making the researchers refocus their efforts into understanding why the implementation of the IVS had failed. As a result, Figure 5 was repurposed from a more general e-Participation system failure (Toots, 2019) into one that could theoretically explain the case of the Åland Islands.

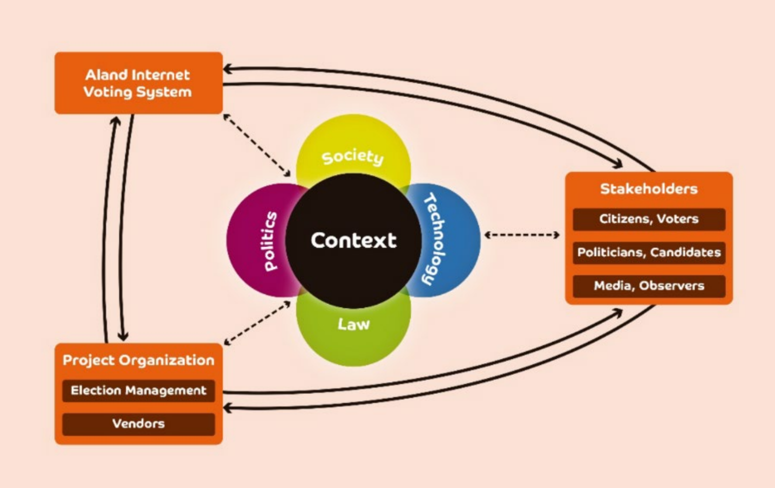


*Figure 5. Mirabilis of IVS failure (Article **IV**, p. 42)*

While the creation of theoretical frameworks is not new in public administration studies, the innovative approach is attempting to use one of them for practical purposes. In this case it refers to Article **V**, where the author attempts to apply this framework to analyse the current situation of IVS implementation in Moldova to identify potential pitfalls and to ultimately prevent a failure like in the Åland Islands. As we have previously seen, there are not many countries that have implemented IVS, so for this specific case, information about IVS implementation should be effectively used and maximised whenever possible.

When applying the DKTC model, the author can identify that the existing knowledge involves the electoral code, the stakeholders and all corresponding legislative instruments and contextual elements relative to elections. Similarly, as in the previous case, the discussed need can either be framed in the research question of this dissertation (i.e., how to transfer knowledge) or in the research question of the article (i.e., how to identify potential pitfalls). The stakeholders involved can be classified as those part of the IVS implementation, or as those not part of it.

The Mirabilis of IVS failure (Figure 5) serves as both a generative and a disseminative capacity. As the former, its primary focus is on knowledge discovery, and as the latter, on knowledge diffusion (see Parent et al., 2007). It allows the identification of contextual elements and classification of stakeholders involved in IVS implementation. It also permits the discovery and diffusion of the relationships between the different stakeholders, themselves, and takes into account the context as well. Once this is done, further analysis can yield opportunities and risks to be handled by the implementors of the IVS.

Having a diagram that explains the failure of implementation and using it to avoid it, is a non-standard way of seeing things, which might also be classified as new and effectively as double-loop learning. As a KM/KT tool, it combines storytelling (i.e., the failure of the Åland Islands), with competency mapping and knowledge valuation to identify the needs and produce a gap analysis. It also services the identification of future capability requirements and effectively becomes a knowledge repository where the necessary elements start to be added one by one. While the implementation of IVS is still underway in Moldova, the practicality of this theoretical framework for this specific case is unmatched.

3.2 KT regarding cybersecurity

KT regarding cybersecurity can be handled by the creation of a publicly available database of documentation and sources, which can also double as an index, as presented in Article **I**, in addition to massively multi-country studies to find commonalities and best practices, as elaborated upon in Articles **I** and **III**. The benefits of such approaches will be made clearer in the following paragraphs.

Database/Index

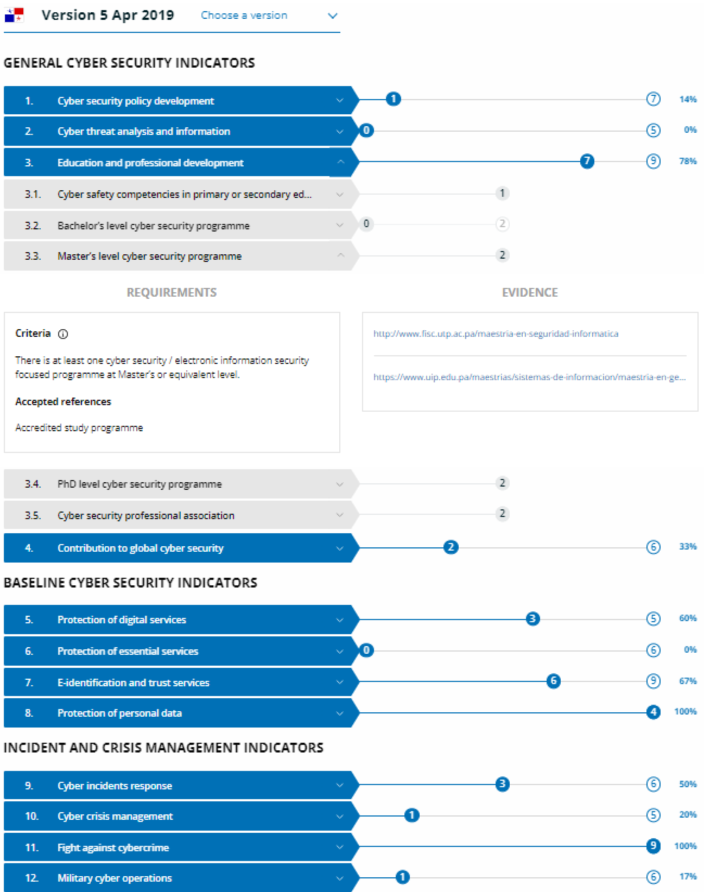
Article **I** presents a novel idea for KT with regards to national cybersecurity. Databases (i.e., knowledge repositories) are not in fact novel. But making a global index sufficiently transparent to become a publicly available database/knowledge repository is innovative. The approach of basing the scoring of the index only on publicly available information, while it brings bias to the index[14], creates a database of factual and practical information that can serve public administrations around the world. The NCSI, discussed in Article **I**, is organised into three categories, twelve capacities, and forty-six indicators. It is solely based on publicly available official information, disclosing everything from the criteria for each indicator and methodology to the scoring and transparency of the accepted evidence, allowing stakeholders to understand the components of national cybersecurity. All evidence is available as hyperlinks to the original sources for easy viewing. Figure 6 presents a partially expanded screenshot of a country page from the NCSI (taken from Article **I**).

When applying the DKTC model, the author can identify that the existing knowledge involves everything relative to cybersecurity in a country. The discussed need can either be framed in the research question of this dissertation (i.e., how to transfer knowledge) or in the research question of the article (i.e., how national cybersecurity is undertaken throughout the world). The stakeholders involved are those in charge of cybersecurity in the country. The index/database (i.e., the NCSI) serves as a generative, disseminative and absorptive capacity, focusing on knowledge discovery, diffusion, and application, respectively (see Parent et al., 2007).

Unlike with the database of Feledi et al. (2013), basing the NCSI on publicly available official information maintains and ensures the quality of knowledge, which in turn results in trust from its users, who are able to view (and verify, if needed) the evidence. The issue of competitive disadvantages is a non-starter since the knowledge and information are publicly available. On the other hand, similarly to Feledi et al. (2013), the target group of

[14] Referring to the NCSI of Article **I**, countries that are more transparent and/or more digitised regarding their national cybersecurity have more chances to fulfill the Index criteria and thus receive a higher score.

users is not explicitly defined by the NCSI. However, this does not detract from the usefulness or sustainability of the web-portal. While the NCSI is maintained by the creators and country volunteers, there is a clear benefit to keeping the knowledge up to date for countries as it leads to a better position in the ranking, which in turn might translate into a better international standing for the corresponding nation.



Version 5 Apr 2019 Choose a version

GENERAL CYBER SECURITY INDICATORS

1.	Cyber security policy development	1	7	14%
2.	Cyber threat analysis and information	0	5	0%
3.	Education and professional development	7	9	78%
3.1.	Cyber safety competencies in primary or secondary ed...	1		
3.2.	Bachelor's level cyber security programme	0	2	
3.3.	Master's level cyber security programme	2		

REQUIREMENTS

Criteria

There is at least one cyber security / electronic information security focused programme at Master's or equivalent level.

Accepted references

Accredited study programme

EVIDENCE

http://www.fisc.utp.ac.pa/maestria-en-seguridad-informatica

https://www.uip.edu.pa/maestrias/sistemas-de-informacion/maestria-en-ge...

3.4.	PhD level cyber security programme	2		
3.5.	Cyber security professional association	2		
4.	Contribution to global cyber security	2	6	33%

BASELINE CYBER SECURITY INDICATORS

5.	Protection of digital services	3	5	60%
6.	Protection of essential services	0	6	0%
7.	E-identification and trust services	6	9	67%
8.	Protection of personal data	4		100%

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9.	Cyber incidents response	3	6	50%
10.	Cyber crisis management	1	5	20%
11.	Fight against cybercrime	9		100%
12.	Military cyber operations	1	6	17%

*Figure 6. Partially extended screenshot of a Country Page (Panama) from the NCSI (from Article **I**)*

If countries were to create and/or manage their own database it would present a compendium of information, categorised into different subtopics, which would allow stakeholders to remember their rights and responsibilities in terms of cybersecurity. The availability of the information also assists stakeholders when they need it for tasks and procedures. Managed by public administrations, they would be able to regulate the quality of the information in it and update it as soon as anything changes. It would serve as a freedom of information measure by allowing official information to be publicly available and easy to access and would improve the openness of public administration. Finally, it would create a clear record of past documentation every time something is updated.

The NCSI mentioned in Article I deals with Bowman's (1978) conundrum of how to transfer research findings into the practical world. The knowledge presented in the article is wholly practical but arranged from a theoretician's perspective to simply it.

Its applicability to specific situations is enormous, since the methodology of the Index subdivides national cybersecurity into capacities, and further into indicators. Next, the generational differences discussed by Burch V. & Strawderman (2014) are also covered. As knowledge is subdivided into 46 indicators, it can be said that the information has been presented in small bits. The fact that not all nations are able to present evidence for all the criteria in the Index also highlights the search – discover – rewards capabilities, since if they are missing, a country would want to fulfil those as soon as possible to receive a better ranking and standing in the international arena. The barriers related to knowledge transfer do not disappear, but having access to different, practical examples of what other nations are doing in terms of national cybersecurity allows those facing obstacles to find proven solutions and/or ideas that might work if they are slightly modified to fit their contexts.

Policy transfer is also possible, and importantly, countries can now select from where to transfer knowledge, given that Article **I** presents a more varied number of role models. For example, Figure 7 outlines the countries that were the top scorers in the African region for the twelve different capacities being monitored in the Index. Countries across the world can look at these role models and have a greater choice to work with in terms of country likeness. This is also true for the Americas, Asia, Europe, and Oceania regions, thus presenting new opportunities for KT between countries in the world.

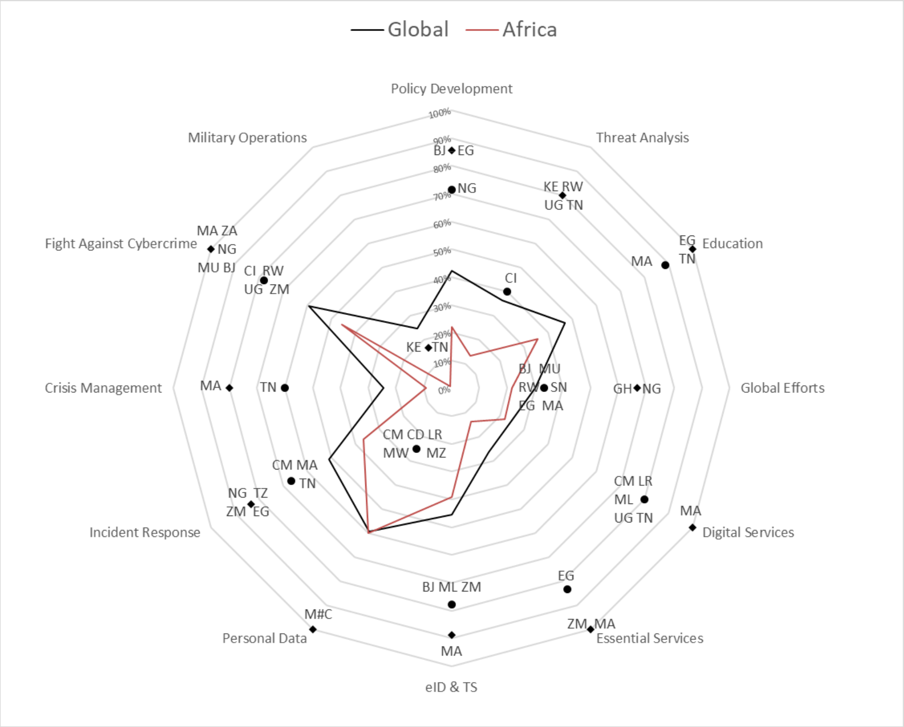


*Figure 7. Cybersecurity focus in Africa and top scorers for each capacity (Article **I**)*

Finally, as a KM/KT tool, the database combines multiple tools in itself, which is a knowledge repository. The database can be used for competency mapping, as described in Article **I**. Given the large amount of role models, double-loop learning can also happen, since newer sources for examples can challenge preexisting assumptions.

After the corresponding mapping is completed, future capability requirements are identified and public administration can work on it. If a score is given, like in the case of the NCSI, knowledge valuation is being implemented. And finally, sourcing decisions would be easier to make since stakeholders are easily identifiable.

Massively multi-country studies

Massively multi-country studies provide a trove of innovation in terms of practical knowledge, which from the point of IG, would make effective use and maximise the value of all existing information resources. This can be achieved by focusing on a general topic, like national cybersecurity in Article **I**, or a narrower one, like searching for international cooperation, neutrality, and warfare/conflict in the NCSS as detailed in Article **III**. Multi-country studies are not a new element, as presented in the previous subsection. However, massively multi-country studies are studies that involve almost all or all countries applicable. It would not be beneficial to set a lower limit to the number of countries to be involved, however, having explored 161 and 113 countries in Articles **I** and **III**, respectively, it is clear enough to see these as being classified as massively multi-country studies. The benefit of this approach is that it allows discovering new information that would otherwise not have been available if a lesser number of countries had been studied.

When applying the DKTC model, the author can identify that the existing knowledge involves anything relative to cybersecurity for a corresponding study. The discussed need can either be the one framed in the research question of this dissertation (i.e., how to transfer knowledge) or in the research question of the corresponding article (e.g., in our case, the one from Article **III**). The stakeholders involved are those relative to the cybersecurity research that is to be conducted. A massively multi-country study serves as a generative capacity, focusing on knowledge discovery (see Parent et al., 2007). The author has already discussed how such investigation in Article **I** allowed identifying other role models in addition to the traditional cybersecurity superpowers. Article **III,** on the other hand, with its narrower focus, made it possible to determine the national positions held in relation to the three national cybersecurity subtopics, which due to the current geopolitical situation in the world was necessary to identify the countries that would align themselves with each other. Massively multi-country studies combine communities of practice with competence mapping and the identification of future capability requirements. Aligned public administrations will, hopefully, be able to better interact and cooperate with each other, having better understood the existing resources and needs to be tackled.

4 Discussion

The following table compiles the results chapter in the first three rows and further focuses on their usability by specific stakeholders and their applicability to other topics, which will be the focus of this discussion chapter.

Table 4. Overview of the results

Knowledge transfer through	Corresponding DKTC capacity	KM/KT Tools combined within	Usable by	Applicable to other topics
BPMN translation	Disseminative	• Communities of practice • Mentoring • Decision sourcing • Coaching • Succession planning • Knowledge repository • Hypertext	• Public administrations • Civil society organisations • Academia* • Citizens*	Plausible
Theoretical Frameworks (Mirabilis of IVS failure)	Generative and Disseminative	• Double-loop learning • Storytelling • Competency mapping • Knowledge valuation • Capability requirements identification • Knowledge repository	• Public administrations • Private sector • Academia*	No
Databases / Index	Generative, Disseminative and Absorptive	• Knowledge repository • Competency mapping • Double-loop learning • Capability requirements identification • Knowledge valuation • Decision sourcing	• Public administration • Private sector • Civil society organisations • Academia* • Citizens*	Yes
Massively multi-country studies	Generative	• Communities of Practice • Competence mapping • Capability requirements identification	• Public administration • Private sector • Civil society organisations • Academia*	Yes

*While the DKTC is a model that explains organisational KT, the author of this dissertation recognises that 'Academia' and 'Citizens' cannot be considered as organisations (unless under some specific exceptions). Nevertheless, the DKTC model was created for social systems (see Page 13), which is what 'Academia' and 'Citizens' can be considered. 'Academia' and 'Citizens' have been included in the discussion to demonstrate the value and usability of the proposed KT instruments beyond the organisational setting.

4.1 BPMN translation

Relative to elections, the BPMN can be used by public administrations, especially EMBs, to translate any election-related documented procedure-filled activity into a clear and simplified diagram, which can be used to facilitate understanding, provide training, and update corresponding legislation, as well as used during elections and/or to offer greater transparency toward the population. Civil society organisations, especially electoral observers, would benefit from such a diagram (whether created by them or by the public administrations) to better understand (and follow the enactment of) the electoral processes in that specific country. Since the BPMN simplifies the process to the smallest unit corresponding to an action, civil society organisation can observe with detailed granularity the electoral process and identify possible discrepancies more easily that might otherwise not be identified. The academia can also use this tool, should it focus on studying the electoral cycle. Such studies are not only limited to the inherent actions and process chains but can be the intermediate step for more precise cost management studies. Additionally, since the diagram is constructed using open-source knowledge of the BPMN, which contains standardised notations and rules, it would make comparisons easier between different types of voting within the same electoral process or between the electoral processes of different countries. Citizens would benefit from such a diagram but might not be the ones that expend time or effort into the creation of such a diagram. For them, it would be another tool that can bring additional transparency before and during elections. Therefore, public administrations and civil society organisation may consider using BPMN to increase the electoral awareness of citizens.

The translation into BPMN can be applicable to other topics and sectors, but only if those are similarly documented procedure-filled activities. As its name implies, BPMN is useful for illustrating business processes, and as such, its usefulness rests upon process-filled activities. Some examples could include legislated/documented procedures that involve heavy paperwork and multiple stakeholders (e.g., customs procedures, the backend of public administration services, the judicial process, etc.). One of the drawbacks of the BPMN translation is the need to study and understand the rules of how to draw a BPMN. Nevertheless, since this is open-source knowledge, it is not restrictive for anyone that wishes to learn about it. Reading a BPMN might be as easy as following a flowchart, but there might be some symbols and illustrations that are not known by the reader. This could be resolved by adding the corresponding legend to the BPMN for the reader to interpret.

4.2 Theoretical frameworks (Mirabilis of IVS failure)

In the electoral cycle, the Mirabilis of IVS failure would allow public administrations to pre-emptively understand the different stakeholders that come into play for the implementation of internet voting and the relations between them. It would then allow to draw out possible flaws and shortcomings, from the perspective of different context, that might affect the overall progression of the implementation. Having knowledge of these risks may allow them to evade, mitigate, and/or, in the worst case, prepare to tackle them head on. While the private sector might have apprehensions in using a theoretical framework, it can provide them with an expanded understanding and knowledge of the implementor's context and characteristics to better tailor the IVS to their needs. It can also provide advance notice of obstacles that may hinder the completion of their contractual responsibilities. From the perspective of the private sector, it is always beneficial to know your client. Finally, given that academia is the birthplace of this particular theoretical framework, its usability is only limited by the specificity of the topic, namely internet voting systems. While the context was related to the failure of implementation, Article **V** presents the proof of concept that the mirabilis can be repurposed for analysing the phases before and during implementation.

The applicability of theoretical frameworks in other sectors exists. However, since the author is specifically focusing on the Mirabilis of IVS failure, this would not be transferrable to any other topic. Additionally, since it was created to explain a case study of the failure in the adoption of an IVS, this inherent bias does not allow the framework to be used in any other electoral context without major modifications. For any other electoral topic, it would suit users best to return to the parent framework (i.e., Toot's (2019) e-Participation system failure) of the Mirabilis and adapt it to their corresponding needs. In addition to this bias that is a limiting factor relative to its usability, its use is predicated heavily upon the user's knowledge of internet voting, the electoral process, stakeholders, among other related topics, and the user's own predisposition of using a theoretical framework, which in addition to coming from academia, might uncover failures and problems where they would not want them.

4.3 Databases/Index

For cybersecurity, a database/index with publicly available evidence is a treasure trove for public administrations. The main benefit comes from the use of the data in order to make better informed decisions on the topic, while considering their strengths and weaknesses. Knowledge from different official and publicly available sources provides a more varied perspective than that of just the usual suspects, i.e. countries considered superpowers in the cybersecurity arena. Additionally, a database/index can help public administrations develop and maintain their commitment to transparency, while also increasing their standing in the international sphere. The private sector also benefits directly from such bountiful data. It can be the starting point for market research and other business proposals and plans, which might bring about new opportunities. On the other hand, participation of the private sector in this type of index is highly unlikely, since the core characteristic is transparency. This might not bring about competitive advantage and might even be a risk for companies. In the case of the NCSI, the focus is on national cybersecurity and only few of the indicators could theoretically accept evidence from the private sector, as long as it is publicly available. In this specific case, the participation of the private sector provides a competitive advantage, since it technically serves as another source of free advertisement. Civil society organisations would also find such a database/index usable. Similarly to the private sector, understanding the current strengths and weaknesses at a national level provides with a bird's eye perspective that would allow them to capitalise on the knowledge through old and new alliances with both the public and private sector. Their participation in the endeavour would similarly serve as free advertisement. The main consideration is that since the database/index might be focused on a specific overarching topic (like cybersecurity), only organisations dedicated to that topic and relevant subtopics might benefit and use it. With regard to academia, it can become the starting point of desk research. Being publicly available information, the evidence is linked directly to the source and the research process can expand exponentially from there. Given that all the information is neatly organised and categorised, it opens the doors for comparative and massively multi-country studies. When it comes to citizens, as previously mentioned, it might be useful for public administrations' transparency efforts, as the citizens can use this database to better understand what their country has implemented in the corresponding field. Linking the evidence to the official sources also allows citizens to navigate their country's pages and be better informed of the current situation.

Introducing this method to other sectors has a high level of applicability. Complex topics, similar in scope and breadth to cybersecurity, can be divided into their different concepts for better understanding and categorisation. Following the practice of making the database/index and its methodology transparent would bring additional knowledge transfer value. However, one of the major drawbacks is primarily the creation of the specific metrics or the internal organisation to order, categorise and archive the different subtopics relative to a specific topic. Extensive knowledge of the corresponding topic is needed for this initial endeavour. The next obstacle brings to light the necessity of having resources, human and technological specifically, in order to implement and maintain such an open data database. However, depending on the existence and the level of implementation and sophistication of existing open data clusters, the quantity of resources might be alleviated. Should the data and the methodology be publicly available, visitors or users of such a database/index should not have any issue browsing and/or using it for different purposes. Finally, the creators, administrators and users alike might do well to remember that any creation has inherent biases, which in turn might affect the ranking nature of an index. For example, any transparent index based on publicly available evidence will have a bias towards transparency. A ranking based on the existence of such evidence will favour those that are more open and likely to share existing information. Therefore, the creators and administrators have the extended responsibility to make sure they communicate correctly the benefits of such an index and they do not mischaracterize it under penalty of losing the trust of the visitors and users. Similarly, the users must always consider this and other inherent biases to maximise the value of the knowledge contained therein.

4.4 Massively multi-country studies

Public administrations would find such studies quite beneficial. As with the database/index, they would be able to see what is essentially as close as possible a global perspective and which in turn results in the discovery of new opportunities for partnerships and alliances. This benefit also extends to the private sector and civil society organisations. The former could also use these studies as the basis for market research and expansion opportunities. The latter might use the information to reach out across borders and coalesce efforts among multiple similarly focused organisations. The usability by academia is twofold. Firstly, it would allow for new studies and new focus on even the oldest of topics that had been based on a limited sample in the past. Secondly, it would introduce countries that are not usually present in mainstream research lines. From this variety, new knowledge would emerge to increase the permutations of possible solutions available to everyone else.

Similarly to a database/index, transposing this method to another topic is highly possible and usable. Unlike the former, however, this can be applicable for individual subtopics and even concepts to get an almost global perspective. The main obstacle stems from the immense research that must be done in order to make sure that all possible countries for whom a specific topic corresponds are included, and that the information remains valid by the time the study is conducted and completed. This in turn opens other potential cans of worms relative to the availability of the information, the language barriers, translation bias, among many others. These studies also translate into a major endeavour that might take a long time, depending on the level of granularity of the study. However, the advantages for readers and users of such studies outweigh the issues, since they might present new concepts, overwrite preconceptions, and provide the fuel for new ideas and opportunities.

5 Conclusion

Elections and cybersecurity are important components of life as we know it today. This dissertation deals with both topics, without overlapping, merging or combining their study. This is due to the variety of the author's responsibilities during the industrial doctoral programme. The publications that provide the backbone of this dissertation are focused on these topics. While the corresponding knowledge fields have been advanced with these publications, the author believed that they would also serve to enrich knowledge transfer literature, since it is non-existent with regard to elections and not focused from the perspective of public administrations, in regard to cybersecurity. This was achieved by applying the DKTC model to the publications in order to answer the following research question: how can knowledge transfer be conducted regarding elections and cybersecurity, and what are their benefits for public administrations?

The dissertation proposes to tackle KT in elections through the use of BPMN diagrams to illustrate processes of the electoral law and electoral cycle, and more specifically in the implementation of IVS, the use of the IVS failure framework as the tool to analyse and foresee pitfalls in any implementation attempts. There are multiple benefits to these approaches, but summarizing the most important ones, they serve as great tools for using and maximising the value of existing information in addition to being low resource instruments for knowledge transfer within the organisation and with other external stakeholders. The use of BPMN would be a type of disseminative capacity, thus focusing on knowledge diffusion, while the use of the Mirabilis of IVS failure serves as both a generative and a disseminative capacity, focusing on both knowledge discovery and diffusion.

Regarding cybersecurity, this work proposes the use of a publicly available database/index in conjunction with massively multi-country studies. The dissertation foresees either the use of the current NCSI, or the creation of a new database by any public administration. The benefit of such a tool is that in addition to being a knowledge repository available for any stakeholder, it can be a living record of the changes happening in-country. In combination with massively multi-country studies, it allows the discovery of new opportunities and challenges, which is definitely transferable knowledge for the benefit of a government. The use of the NCSI or any other similar database/index would be a type of generative, disseminative and absorptive capacity, focusing on knowledge discovery, diffusion and application. While the application of massively multi-country studies primarily serves as a generative capacity, focusing on knowledge discovery.

With the exception of the theoretical framework for IVS implementation, all other approaches are applicable, without many modifications and to a certain extent, to other topics in public administration. BPMN diagrams could be used to illustrate laws that describe processes in them. The database/index and massively multi-country studies can similarly be applied to any topic that a government deals with. Future research could focus on demonstrating the applicability of these tools in the field for other topics and/or on improving their effectiveness.

List of figures

List of tables

References

ACE - ACE Electoral Knowledge Network. (n.d.) Electoral Management. Retrieved from https://aceproject.org/ace-en/topics/em/explore_topic_new Last accessed: 04.03.204

ACN CSIRT - Agenzia per la Cybersicurezza Nazionale Computer Security Incident Response Team. (n.d.) Glossario: cybersecurity. Retrieved from https://www.csirt.gov.it/glossario/33 Last accessed: 03.03.204

Alvarenga, A., Matos, F., Godina, R., & C. O. Matias, J. (2020). Digital Transformation and Knowledge Management in the Public Sector. *Sustainability*, Vol. 12(14). doi:10.3390/su12145824

Alvarez, R.M., Levin, I., & Li, Y. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. *Journal of Information Technology & Politics*, Vol. (15)2, pp. 94–105. doi:10.1080/19331681.2018.1460288

ANSSI - Agence nationale de la sécurité des systèmes d'information. (2023). Glossaire. Retrieved from https://cyber.gouv.fr/glossaire Last accessed: 03.03.204

Alfarhoud, Y. T. (2018). The Use of Twitter as a Tool to Predict Opinion Leaders that Influence Public Opinion: Case Study of the 2016 United State Presidential Election. In: Knowledge Discovery and Data Design Innovation, Vol. 14. Alemneh, D. G., Allen, J. & Hawamdeh, S. (Eds). pp. 191–206. doi:10.1142/9789813234482_0010

Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Computers in Human Behavior*, Vol. 38 (0), pp. 304–312. doi:10.1016/j.chb.2014.05.046

Argote, L., & Fahrenkopf, E. (2016). Knowledge transfer in organizations: The roles of members, tasks, tools, and networks. *Organizational Behavior and Human Decision Processes*, Vol. 136, pp. 146–159. doi:10.1016/j.obhdp.2016.08.003.

Argote, L., & Ingram, P. (2000). Knowledge Transfer: A Basis for Competitive Advantage in Firms. *Organizational Behavior and Human Decision Processes*, Vol. 82(1), pp. 150–169. doi:10.1006/obhd.2000.2893

Argote, L., McEvily, B., & Reagans, R. (2003). Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes. *Management Science*, Vol. 49(4), pp. 571–582. doi:10.1287/mnsc.49.4.571.14424

Banciu, D., Rădoi, M., & Belloiu, S. (2020). Information Security Awareness in Romanian Public Administration: An Exploratory Case Study. *Studies in Informatics and Control*, Vol. 29(1), pp. 121–129. doi:10.24846/v29i1y202012

Beam, M. A., Hutchens, M. J., & Hmielowski, J. D. (2016). Clicking vs. sharing: The relationship between online news behaviors and political knowledge. *Computers in Human Behavior*, Vol. 59, pp. 215–220. doi:10.1016/j.chb.2016.02.013

Ben-Asher, N. & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, Vol. 48, pp. 51–61. doi:10.1016/j.chb.2015.01.039

Bernard of Clairvaux. (1953). Sermon XXXVIème sur le Cantique des Cantiques (Sermon XXXVI on the Song of Songs). *Œuvres mystiques de Saint Bernard*. pp. 429–430. Editions du Seuil

Bertollinni, A., Ferrarelli, M., Parente, O., Ferilli, C., Poultsidis, T., Andriessen, J., Schaberreiter, T., & Papanikolaou, A. (2022). Cybersecurity Awareness in Rome and Larissa: Before, During and After CS-AWARE. *Cybersecurity Awareness*. Andriessen, J., Schaberreiter, T., Papanikolaou, A., & Röning, J. (Eds.). Springer: Cham. doi:10.1007/978-3-031-04227-0_5

Bowman, J.S. (1978). Managerial Theory and Practice: The Transfer of Knowledge in Public Administration. *Public Administration Review*, Vol. 38(6), pp. 563. doi:10.2307/976039

Burch V., R.F., & Strawderman, L. (2014). Leveraging Generational Differences to Reduce Knowledge Transfer and Retention Issues in Public Administration. *Public Administration Research*, Vol. 3(2). doi:10.5539/par.v3n2p61

Clark, A., & James, T.S. (2023). Electoral administration and the problem of poll worker recruitment: Who volunteers, and why? *Public Policy and Administration*, Vol. 38(2), pp. 188–208. doi:10.1177/09520767211021203

Carlsson, B., & Stankiewicz, R. (1991). On the nature, function and composition of technological systems. *Journal of Evolutionary Economics*, Vol. 1(2), 93–118. doi:10.1007/bf01224915

Cummings, J. (2003). Knowledge Sharing: A Review of the Literature. *The World Bank Operations Evaluation Department 29385*. Retrieved from https://documents1.worldbank.org/curated/pt/547921468780624297/pdf/293850Knowledge0sharing.pdf Last accessed: 03.03.204

de León, E., Vermeer, S., & Trilling, D. (2023). Electoral news sharing: a study of changes in news coverage and Facebook sharing behaviour during the 2018 Mexican elections. *Information, Communication & Society*, Vol. 26(6), pp. 1193–1209. doi: 10.1080/1369118X.2021.1994629

Dolowitz, D.P., & Marsh, D. (2000). Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making. *Governance*, Vol. 13(1), pp. 5–23. doi:10.1111/0952-1895.00121

Dooba, I.M., & Downe, A.G. (2011). Extraction and translation of safety knowledge in organizations using incident reports. African Journal of Business Management, Vol. 5 (23), pp. 9794–9799. doi:10.5897/AJBM11.969

Dougherty, V. (1999). Knowledge is about people, not databases. *Industrial and Commercial Training*, Vol. 31 (7), pp. 262–266. doi:10.1108/00197859910301962

Dueñas-Cid, D. (2024) [Forthcoming]. Trust and distrust in electoral technologies: what can we learn from the failure of electronic voting in the Netherlands (2006/07). *Proceedings of the Digital Government Research 2024 International Conference.*

Easterby-Smith, M., Lyles, M.A., & Tsang, E.W.K. (2008). Inter-organizational knowledge transfer: current themes and future prospects. *Journal of Management Studies*, Vol. 45(4), pp. 677–690. doi:10.1111/j.1467-6486.2008.00773.x

Ekirapa-Kiracho, E., Walugembe, D.R., Tetui, M., Kisakye, A.N., Rutebemberwa, E., Sengooba, F., Kananura, R.M., Wensing, M. & Kiwanuka, S. (2014). Evaluation of a health systems knowledge translation network for Africa (KTNET): a study protocol. *Implementation Science*, Vol. 9. doi:10.1186/s13012-014-0170-4

ENISA. (2015). Definition of Cybersecurity: Gaps and overlaps in standardization. Retrieved from https://www.enisa.europa.eu/publications/definition-of-cybersecurity Last accessed: 03.03.204

ENISA. (2017). ENISA overview of cybersecurity and related terminology. Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
Last accessed: 05.04.2024

Farooq, R. (2020). A conceptual model of knowledge sharing. *International Journal of Innovation Science*, Vol. 10(2), pp. 238–260. doi:10.1108/IJIS-09-2017-0087

Farooq, R. (2024). A review of knowledge management research in the past three decades: a bibliometric analysis. *VINE Journal of Information and Knowledge Management Systems*, Vol. 54(2), pp. 339–378. doi:10.1108/VJIKMS-08-2021-0169

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, Vol. 17(4), pp.199–209. doi:10.1016/j.istr.2013.03.004

Gibson, J.P., Krimmer, R., Teague, V. & Pomares, J. (2016). A review of E-voting: the past, present and future. *Annals of Telecommunications*, Vol. 71, pp. 279–286. doi:10.1007/s12243-016-0525-8

Goh, S.C. (1998). Toward a Learning Organization: The Strategic Building Blocks. *SAM Advanced Management Journal*, Vol. 63, pp. 15–22.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, Vol. 21, pp. 135–146.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, Vol. 34(5), pp. 509–519. doi:10.1016/j.jaccpubpol.2015.05.001

Gronke, P., Galanes-Rosenbaum, E., Miller, P.A., & Toffey, D. (2008). Convenience Voting. *Annual Review of Political Science*, Vol. 11(1), pp. 437–455. doi:10.1146/annurev.polisci.11.053006.190912

Gupta, A. and Wolf, J. R. (2018). An Examination of Cybersecurity Knowledge Transfer: Teaching, Research, and Website Security at U.S. Colleges and Universities. *Journal of Cybersecurity Education, Research and Practice*, Vol. 2018(2).

International IDEA – International Institute for Democracy and Electoral Assistance. (2014). *Electoral Management Design*. Catt, H., Ellis, A., Maley, M., Wall, A., Wolf, P. (Eds.)

International IDEA – International Institute for Democracy and Electoral Assistance. (2024). ICTs in Elections Database. Retrieved from https://www.idea.int/data-tools/data/question?question_id=9349&database_theme=327 Last accessed: 09.03.2024

ITU – International Telecommunication Union. (2008). Series X: Data Networks, Open System Communications And Security - Telecommunication security - Overview of cybersecurity - Recommendation ITU-T X.1205

James, T.S. (n.d.). Election Administration. Retrieved from https://tobysjames.com/election-administration/ Last accessed: 04.03.204

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. Springer: Switzerland. doi:10.1007/978-3-319-10632-8

Kosevich, E. (2024). Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: a Latin America typology and review. *Area Development and Policy*, Vol. 9(1), pp. 86–107. doi: 10.1080/23792949.2023.2259972

Krimmer, R., Dueñas-Cid, D., & Krivonosova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? *Public Money & Management*, Vol. 41(1), pp. 17–26. doi:10.1080/09540962.2020.1732027

Licht, N., Dueñas-Cid, D., Krivonosova, I., & Krimmer, R. (2021). To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. *Electronic Voting. E-Vote-ID 2021. Lecture Notes in Computer Science*, Vol. 12900. Krimmer, R., et al. (Eds.). Springer: Cham. doi:10.1007/978-3-030-86942-7_7

Luiijf, H.A.M., Besseling, K., Spoelstra, M., de Graaf, P. (2013). Ten National Cyber Security Strategies: A Comparison. *Critical Information Infrastructure Security. CRITIS 2011. Lecture Notes in Computer Science*, Vol. 6983. Bologna, S., Hämmerli, B., Gritzalis, D., Wolthusen, S. (Eds.) Springer: Berlin, Heidelberg. doi:10.1007/978-3-642-41476-3_1

NATO CCDCOE. (2012). National Cyber Security Framework Manual. Klimburg, A. (Ed.). Retrieved from https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf Last accessed: 05.04.2024

NCSC - National Cyber Security Centre (n.d.) Glossary. Retrieved from https://www.ncsc.gov.uk/section/advice-guidance/glossary Last accessed: 03.03.204

NCSI - National Cyber Security Index. (2023). Update to the NCSI 3.0 Methodology. Retrieved from https://ncsi.ega.ee/97/update-to-the-ncsi-30-methodology/ Last accessed: 05.04.2024

Newmeyer, K.P. (2015). Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal*, Vol. 1(3), pp. 9–19.

NIST - National Institute of Standards and Technology. (n.d.) Glossary: cybersecurity Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity Last accessed: 03.03.204

Massaro, M., Dumay, J., & Garlatti, A. (2015). Public sector knowledge management: a structured literature review. *Journal of Knowledge Management*, Vol. 19(3), pp. 530–558. doi:10.1108/jkm-11-2014-0466

Massingham, P. (2014). An evaluation of knowledge management tools: Part 1 – managing knowledge resources. *Journal of Knowledge Management*, Vol. 18(6), pp. 1075–1100. doi:10.1108/jkm-11-2013-0449

Maurer, M. (2009). Wissensvermittlung in der Mediendemokratie. Wie Medien und politische Akteure die Inhalte von Wahlprogrammen kommunizieren (Knowledge transfer in media democracy. How media and political actors communicate the content of election manifestos). In: *Politik in der Mediendemokratie.* Marcinkowski, F., & Pfetsch, B. (Eds). pp. 151–173. doi:10.1007/978-3-531-91728-3_7

Mazorodze, A.H., & Buckley, S. (2020). A review of knowledge transfer tools in knowledge-intensive organisations. *SA Journal of Information Management*, Vol. 22(1). doi:10.4102/sajim.v22i1.1135

McGrath, J.E., & Argote, L. (2001). Group processes in organizational contexts. In: *Blackwell handbook of social psychology: Group processes*. Hogg A., & Tindale R. (Eds.). pp. 603–627.

Meredith, M., & Malhotra, N. (2011). Convenience Voting Can Affect Election Outcomes. *Election Law Journal: Rules, Politics, and Policy*, Vol 10(3). doi:10.1089/elj.2010.0088

MIT – Massachusetts Institute of Technology. (1991). *Knowledge Discovery in Databases*. Piatetsky-Shapiro G., Frawley W. (Eds). MIT Press.

Odebade, A.T., & Benkhelifa, E. (2023) A Comparative Study of National Cyber Security Strategies of ten nations. *Computers and Society*. doi:10.48550/arXiv.2303.13938

Oruj, Z. (2023). Cyber Security: Contemporary Cyber Threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*, Vol. 1(2), pp. 100–116. doi:10.18372/2786-5495.1.17309

Parent, R., Roy, M., & St-Jacques, D. (2007). A systems-based dynamic knowledge transfer capacity model. Journal of Knowledge Management, 11(6), 81–93. doi:10.1108/13673270710832181

Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. *Decision Analysis*, pp. 1 – 25. doi:10.1287/deca.2018.0387

Peffers, K., Tuunanen, T., Rothenberger, M.A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, Vol. 24(3), pp.45–77. doi:10.2753/mis0742-1222240302

Quintane, E., Casselman, R.M., Reiche, B.S., & Nylund, P.A. (2011). Innovation as a knowledge-based outcome. *Journal of Knowledge Management*, Vol. 15(6), pp. 928–947. doi:10.1108/13673271111179299

Rashman, L., & Hartley, J. (2002). Leading and learning? Knowledge transfer in the Beacon Council Scheme. *Public Administration*, Vol. 80(3), pp. 523–542. doi:10.1111/1467-9299.00316

Rezania, D. & Ouedraogo, N. (2014). Organization development through ad hoc problem solving: A case of knowledge transfer capacity development in an ERP implementation project. *International Journal of Managing Projects in Business*, Vol. 7 (1), pp. 23–42. doi:10.1108/IJMPB-11-2012-0067

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: its influence on end users' information security practice behavior. *Computers & Security*, Vol. 28 (8), pp. 816–826. doi:10.1016/j.cose.2009.05.008

Rose, R., & Mossawir, H. (1967). Voting and Elections: A Functional Analysis. *Political Studies*, Vol. 15(2), pp. 173–201. doi:10.1111/j.1467-9248.1967.tb01843.x

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, Vol. 56, pp. 70–82. doi:10.1016/j.cose.2015.10.006

Savi, R., Randma-Liiv, T. (2013). Policy transfer in new democracies: challenges for public administration. In Policy Transfer and Learning in Public Policy and Management. Eds. Common, R., Carroll, P. (pp. 77–89). Routledge.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, Vol. 104, pp. 333–339. doi:10.1016/j.jbusres.2019.07.039

Stone, D. (2012). Transfer and translation of policy. *Policy Studies*, Vol. 33(6), pp. 483–499. doi:10.1080/01442872.2012.695933

Swift, M. K. (1991). Hypertext: A Tool for Knowledge Transfer. *Journal of Systems Management*, Vol. 42(6).

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. Computers & Security, Vol. 43, pp. 19–34. doi:10.1016/j.cose.2014.02.010

TalTech – Tallinn University of Technology. (n.d.). Admission to doctoral Studies at Taltech. Retrieved from: https://taltech.ee/en/phd-admission Last accessed: 02.04.2024

Toots, M. (2019). Why E-participation systems fail: The case of Estonia's Osale.ee. Government Information Quarterly, Vol. 36(3), pp. 546–559. doi:10.1016/J.GIQ.2019.02.002

Tsai, W. (2002). Social structure of 'coopetition' within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization Science*, Vol. 13(2), pp. 179–190. doi: 10.1287/orsc.13.2.179.536

Vizecky, K. (2011). A Design Theory for Knowledge Transfer in Business Intelligence. *AMCIS 2011 Proceedings - All Submissions*. Available at: https://aisel.aisnet.org/amcis2011_submissions/51

Waddell M. (2024). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. *Healthcare Management Forum*, Vol. 37(1), pp. 13–16. doi:10.1177/08404704231196137

Wang, C.L., Hult, G.T.M., Ketchen, D.J., & Ahmed, P.K. (2009). Knowledge management orientation, market orientation, and firm performance: an integration and empirical examination. *Journal of Strategic Marketing*, Vol. 17(2), pp. 99–122. doi:10.1080/09652540902879326

Wiig, K. M. (2000). *Application of Knowledge Management in Public Administration*.

Wiig, K. M. (2002). Knowledge management in public administration. *Journal of Knowledge Management*, Vol. 6 (3), pp. 224–239. doi:10.1108/13673270210434331

Yao, L.J., Kam, T.H.Y., Chan, S.H. (2007). Knowledge sharing in Asian public administration sector: the case of Hong Kong. *Journal of Enterprise Information Management*, Vol. 20(1), pp. 51–60. doi:10.1108/17410390710717138

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*, 6th Edition. SAGE Publications, Inc.: London

Zackarias, A.J., Bond-Barnard, T.J., & van Waveren, C.C. (2022). Improving Knowledge Transfer Processes to Address Skills and Knowledge Gaps between Senior and Junior Staff in Engineering Projects. South African Journal of Industrial Engineering, Vol. 33(4), pp. 147–164. doi:10.7166/33-4-2672

Zhang, Y., & Yu, X. (2019). Policy transfer: the case of European Union–China cooperation in public administration reform. *International Review of Administrative Sciences*. doi:10.1177/0020852319841427

Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American Society for Information Science and Technology*, Vol. 58(4), pp. 479–493. doi:10.1002/asi.20508

Acknowledgements

În primul rând, cel mai important, aș dori să-i mulțumesc Dumnezeului Atotputernic pentru că mi-a oferit credință, putere, perseverență, cunoaștere și înțelepciune pentru a îndeplini cu succes acest studiu, pe care El mi l-a pus în fața.

A mi familia, especialmente a mi madre, Veronica de Serrano, y a mi padre, Juventino Serrano, les estaré eternamente agradecido por sus inagotables sacrificios, apoyo, enseñanzas y formación a lo largo de los años, que me han permitido convertirme en la persona que soy hoy. ¡Gracias por todo, siempre!

This dissertation would have not been possible without the understanding, support, and continuous advice of my supervisors, past and present, Dr. Dr. Robert Krimmer, Dr. Liia Hänni, Dr. David Dueñas-Cid, and Dr. Veiko Lember. Although your time guiding me was short, I have always attempted to apply your wisdom and insight into this work and my daily life. Thank you for your teachings!

Un grand merci à Dr. Mario J. Roy, pour m'avoir permis de reproduire l'illustration du modèle DKTC, et sans le travail duquel cette thèse n'aurait pas été possible.

To the co-authors of the articles used in this dissertation, it was an immense pleasure working with you and I appreciate you being my colleagues in the search for knowledge. Gràcies! Спасибо! Obrigado! Danke! ありがとう!

Tahaksin tänada oma E-riigi Akadeemia perekonda nende aja ja toetuse eest läbi aastate, eriti pr Annela Kiiratsit ja pr Marit Lani, kes tutvustasid mulle NCSI-d ning organisatsiooni juba 2018. aastal. Avaldan tänu ja tunnustust ka kolleegidele küberturvalisuse pädevuskeskuses ning kõigile riikide panustajatele, kes aitavad NCSI-d ajakohasena hoida.

Mein besonderer Dank gilt Frau Dr. Katharina Friedlinde Heil, die mir in den dunkelsten Stunden den Weg gewiesen hat.

To Ms. Kiyumbu Wilkister Ludenyi, I thank her for the long-distance support and guidance, stemming from our talks and from her insightful writings.

As the place that allowed me to embark on this journey, the Ragnar Nurkse Department of Innovation and Governance, I would like to express my appreciation to their staff for the provided support and unique experiences I encountered over the past years. The journey has been filled with learning opportunities, that have culminated in this dissertation, and which will continue to serve me well in my future endeavours.

Finally, I thank all my colleagues and friends, from both the academic and professional sectors, who have assisted and cheered me on throughout these years. May their futures be full of blessings and success!

Abstract

Knowledge Transfer for Public Administrations: The Case of Elections and Cybersecurity

Elections and cybersecurity are important components in today's democratic and globalised way of life. This thesis deals with both topics, but it does not combine, merge or otherwise attempt to study them together. The focus of this dissertation is on understanding how to better transfer knowledge in two critical public administration systems – e-elections and cyber security. This thesis is a result of an industrial doctoral programme where the author has been appointed to projects in both cybersecurity and e-democracy, the latter focusing on elections. As a result, the backbone publications are on these topics and provide novel knowledge, ideas, and concepts in their corresponding fields. This thesis is the perfect environment for conducting an overarching discussion embracing both fields of research and resulting in insights that can be of benefit and value for public administrations.

Knowledge comes heavily into play in the aforementioned topics. Bad knowledge management/transfer, and the corresponding lack of knowledge can result in the failure of electronic and internet voting, and/or delays in the resolution of cyber-attacks and crisis. Knowledge transfer literature regarding elections is seemingly non-existent while on the other hand, knowledge transfer literature regarding cybersecurity is vast and even specialised, however, not from a national or public administration perspective. This dissertation answers the following research question: how can knowledge transfer be conducted regarding elections and cybersecurity, and what are their benefits for public administrations?

To answer this question, the insights presented in the articles of the thesis will be analysed through the lens of the Dynamic Knowledge Transfer Capacity (DKTC) model, co-authored by Drs. Parent, R., Roy, M., and St-Jacques, D. in 2007. The DKTC will be used to classify the insights of these publications and clarify their role in knowledge transfer. The individual articles and their research were conducted using different methodologies, i.e., case study, literature review, design science, and the NCSI methodology; while data collection primarily involved document and data analysis, interviews, and literature review.

The findings reveal that KT regarding elections can be undertaken through the translation of the electoral law and processes into BPMN, while KT regarding cybersecurity can be handled by the creation of a publicly available database of documentation and sources, which can also double as an index, in addition to massively multi-country studies to find commonalities and best practices.

This doctoral thesis contributes to KT literature in public administration by proposing ways to transfer knowledge in the context of e-elections and cybersecurity. Multiple stakeholders can benefit from their use and their applicability without many modifications to other topics is great. BPMN diagrams could be used to illustrate laws that describe processes in them. The database/index and massively multi-country studies can similarly be applied to any field of public administrations. Future research could focus on demonstrating the practical applicability of these tools in other topics and/or improving their effectiveness.

Lühikokkuvõte

Haldusasutuste teadmussiire: valimiste ja küberturvalisuse juhtum

Valimised ja küberturvalisus on tänapäeva demokraatliku ja globaliseerunud eluviisi olulised komponendid. See lõputöö käsitleb mõlemat teemat, kuid see ei ühenda ega seo neid ega püüa neid muul viisil koos uurida. Doktoritöö fookuses on mõista, kuidas paremini edastada teadmisi kahes üliolulises avaliku halduse süsteemis – e-valimised ja küberturvalisus. See uurimistöö on tööstusdoktorantuuriõppe tulemus, kus autor tegeleb nii küberturvalisuse kui ka e-demokraatia projektidega, millest viimane keskendub valimistele. Selle tulemusena on põhiväljaanded kõnealustel teemadel ja pakuvad uudseid teadmisi, ideid ning kontseptsioone vastavates valdkondades. See doktoritöö on ideaalne võimalus kõikehõlmava arutelu läbiviimiseks, mis puudutab mõlemat uurimisvaldkonda ja annab teadmisi, mis võivad olla kasulikud ning väärtuslikud avalikule haldusele.

Teadmised mängivad eelmainitud teemadel olulist rolli. Kehv teadmiste haldamine/edasiandmine ja sellest tulenev teadmiste puudumine võib põhjustada elektroonilise ning internetihääletuse ebaõnnestumise ja/või viivitusi küberrünnakute ja kriiside lahendamisel. Valimistega seotud teadmussiirde kirjandus on pealtnäha olematu, samas kui teisalt on küberturvalisust käsitlev teadmussiirde kirjandus tohutu ja isegi spetsialiseerunud, kuigi mitte riikliku või avaliku halduse seisukohast. See doktoritöö vastab järgmisele uurimisküsimusele: kuidas saab läbi viia valimiste ja küberturvalisuse teadmussiiret ning milline on nende kasu avalikule haldusele?

Sellele küsimusele vastamiseks analüüsitakse selle teadustöö artiklites esitatud teadmisi dünaamilise teadmussiirde võimekuse (DKTC) mudeli kaudu, mille kaasautorid on Drs. Parent, R., Roy, M., ja St-Jacques, D. (2007). DKTC-d kasutatakse nende väljaannete teabe klassifitseerimiseks ja rolli selgitamiseks teadmussiirdes. Üksikud artiklid koostati ja nende uuringud viidi läbi, kasutades erinevaid metoodikaid, st juhtumiuuringut, erialakirjanduse ülevaadet, disainiteadust ja NCSI (riiklik küberturvalisuse indeks) metoodikat; samas kui andmete kogumine hõlmas peamiselt dokumentide ja andmete analüüsi, intervjuusid ja erialakirjanduse ülevaadet.

Tulemused näitavad, et valimistega seotud teadmussiirde saab läbi viia valimisseaduse ja -protsesside üleviimise kaudu BPMN-i (äriprotsesside modelleerimise ja kirjapanemise viis), samas kui küberturvalisusega seotud teadmussiiret saab käsitleda avalikult kättesaadava dokumentatsiooni ja allikate andmebaasi loomisega, mis võib lisaks massiliselt mitut riiki hõlmavatele uuringutele ühiste joonte ning parimate tavade leidmiseks ka indeksina kahekordistuda.

Siinne doktoritöö panustab teadmussiirde kirjandusse avalikus halduses, pakkudes välja viise teadmiste edastamiseks e-valimiste ja küberturvalisuse kontekstis. Nende kasutamisest saavad kasu mitmed sidusrühmad ja nende rakendatavus (ilma paljude muudatusteta) teiste teemade puhul on suurepärane. BPMN-diagramme võiks kasutada neis toimuvaid protsesse kirjeldavate seaduste illustreerimiseks. Andmebaasi/indeksit ja massiliselt mitut riiki hõlmavaid uuringuid saab samamoodi rakendada mis tahes avaliku halduse valdkonnas. Tulevased uuringud võiksid keskenduda nende vahendite praktilise rakendatavuse näitamisele muudes valdkondades ja/või nende tõhususe parandamisele.

Appendix 1

Publication I

Serrano-Iova, R.A. (2024) [Forthcoming]. National Cybersecurity: Global and Regional Descriptive Snapshots through the Analysis of 161 Countries. *Halduskultuur - The Estonian Journal of Administrative Culture and Digital Governance*. ETIS 1.1.

National Cybersecurity: Global and Regional Descriptive Snapshots through the Analysis of 161 Countries

Radu Antonio Serrano Iova[1][0000-0003-2183-0313]

[1] Tallinn University of Technology, Ragnar Nurkse Department of Innovation and Governance
Akadeemia tee 3, 12618 Tallinn, Estonia
raduantonio.serranoiova@taltech.ee

Abstract

National cybersecurity includes so many topics and considerations that a global overview of trends is a quite complex endeavour. Previous studies either focus on individual countries or multiple ones while considering only a specific subtopic or point of interest of national cyber security. The purpose of this article is to present the regional cybersecurity trends of 161 nations, as of late January 2023, through the use of the National Cyber Security Index (NCSI). With the help of the NCSI, its methodology and publicly available database, we will provide both global and regional snapshots of what countries have been focusing on and doing in reference to their national cybersecurity. This will allow the discovery of similarities, best practices and more importantly underdeveloped topics that should be improved upon to guarantee a more robust approach to national cybersecurity. Globally the national approaches seem to be reactionary, with very little focus on proactive measures, but regionally some differences start to appear. Future research will be able to build upon this research by either individual case studies or comparative studies among multiple countries.

Keywords

Cybersecurity, global, cybercrime, cyberoperations

ICT and digital technologies have become so ubiquitous around all of us, that cyber security is no longer a topic that is undertaken by only handful of highly specialized individuals. Because of this, whole countries nowadays must endeavour to create complex strategies and policies to protect their cyber security, and mitigate, and recover from, attacks and threats. As Shackelford and Kastelic have posited in their opening statement "*nations bear increasing responsibility for enhancing cybersecurity.*" (2014, 1)

The definition of the term cybersecurity or cyber security it is still under discussion in multiple academic and non-academic circles (Bay 2016; Craigen et al. 2014; ENISA 2015). The debate turns even more complex when you consider the different languages throughout the world that are discussing this universal topic (Carlini 2016; Guranda 2021; K. Newmeyer et al. 2015; Pohlmann 2019), the multiple national interpretations that are given to the term(s) and the difference in approaches in academia and the non-academic worlds. For this article, we will refer to the definition of the European Union Agency for Cybersecurity (ENISA):

> "*Cybersecurity comprises all activities necessary to protect cyberspace[1], its users, and impacted persons from cyber threats… Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security).*" (ENISA 2017, 6)

National cybersecurity refers to all these efforts at the state level, by the government in charge and relevant stakeholders. Although national cybersecurity has been the focus of academic research before (K. P. Newmeyer 2015; Carlini 2016), this article attempts to answer the following questions:

[1] Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information. (ENISA 2017, 6)

- How is national cybersecurity undertaken throughout the world?
- What similarities and differences exist in national cybersecurity efforts, at the regional and global level?
- From which countries can future best practices be adopted for specific national cybersecurity efforts?

A comparative analysis of 161 national cybersecurity efforts, grouped into regions, allows to answer these questions. This comparison is constructed according to the national cyber security framework, which forms the basis of the similarly named National Cyber Security Index (NCSI). Given the almost global nature of the sample size, the M49 Standard of the Statistics Division of the United Nations Secretariat has been used.

The purpose of this article is both theoretical and practical. Theoretical, providing a holistic snapshot of national cybersecurity focus globally, and fostering further research through bilateral/multilateral regional comparative studies or individual case studies. Practical, so that countries can use this information as a benchmark and see what they are missing or can improve upon, and/or further endeavour to publicise their efforts so that other nations may benefit from the knowledge and best practices.

National cybersecurity research: from the sporadic to the specific

Previous research has been focused either on individual case studies or multiple country comparative studies, with the focus on a single theme (e.g., cybercrime, critical infrastructure protection, governance, etc.) or a single sector (e.g., health, defence, industry, etc.). For example, Berthelet (2020) analyses the topic of the fight against cybercrime within the context of the European Union as a whole, exploring how the different members states act together to fight this transnational phenomenon (Berthelet 2020). Bada et al. (2019) analyse national cybersecurity awareness in six African countries. Their paper presents recommendations for the implementation of national awareness campaigns and how to identify and prioritize relevant activities (Bada et al. 2019). Le Barreau & Longeon (2016) on the other hand, present a study case of Saudi Arabia. Their analysis centres on "*the integration of cybersecurity into national security*" and additional implications between the stakeholders (Le Barreau & Longeon 2016 155). Loiseau et al. (2013) study Canada and how its national cybersecurity has evolved throughout the years. Dewar et al. (2018) and Shackelford & Kastelic (2014) focus on national cyber security strategies and policies. The former also delve into cyber defence of France, Finland, Germany, and the United Kingdom. However, the latter present the analysis of multiple countries. On the other hand, there are also compilations of individual studies, such as Stevens (2018) and Romaniuk & Manjikian (2021). However, the former is a special edition of a journal, whose individual articles deal with specific cybersecurity themes, while the latter, a book, presents chapters and is "*the most comprehensive and up-to-date comparative overview of the cyber-security strategies and doctrines of the major states and actors in Europe, North America, South America, Africa, and Asia*" (page i). In this book, once again we see that each chapter is an individual study, and focus is on the 'major states and actors' (bypassing countries that might be worthy of study), without any regional or global analysis that might uncover similarities or differences between the chosen countries.

A singular, almost similar, global endeavour is the Global Cybersecurity Index (GCI). The GCI is compiled by ITU-D, the Telecommunication Development Sector of the International Telecommunication Union. In short, an Expert Group sends out a GCI Questionnaire to focal points in the Member States, who then respond and return such answers to the Expert Group for analysis (ITU-D n.d.). While the tools and methodology are publicly available, the responses and weighting process are not. Therefore, we posit that the GCI is not academic in nature, due to its replicability factor being affected by its partially obscure methodological process.

This article focuses on expanding the lack of academic studies on the overarching cybersecurity field with an almost global analysis, information extracted in late January 2023, and inductive regional similarities and differences.

Framework and Methodology

The National Cyber Security Index (NCSI) was created by the e-Governance Academy (eGA) as a live global index, and as a cybersecurity reference, assessment and capacity building tool (eGA 2022, 12). It does so through 46 indicators (presented in Annex 1). These indicators were developed through the national cyber security framework (eGA n.d.-b) which in turn alludes to the CIA (Confidentiality, Integrity and Availability) triad. The CIA triad refers to "*the fundamental elements of security controls in information systems*" (Samonas & Coss 2014, 22), which in turn has been "*a popular definition of cybersecurity*" (Ham 2021, 18:1). However, this has not been the case of the aforementioned framework, and as Ham (2021, 18:1) posits, more focus has been "*on the activity and associated risks for cybersecurity*". The national cyber security framework assessed the fundamental threats to the CIA triad of the national ICT systems and services. "*In order to manage these cyber threats, a country must have appropriate capacities for baseline cyber security, incident management, and general cyber security development.*" (eGA n.d.-b)

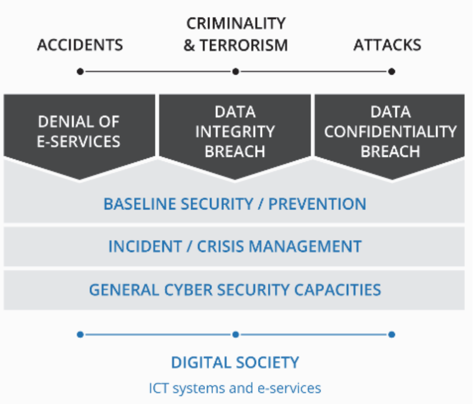
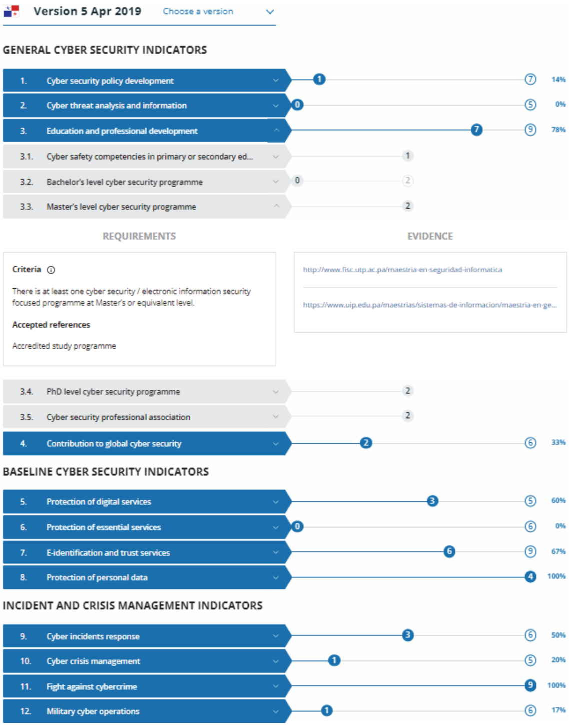

ACCIDENTS
CRIMINALITY & TERRORISM
ATTACKS
DENIAL OF E-SERVICES
DATA INTEGRITY BREACH
DATA CONFIDENTIALITY BREACH
BASELINE SECURITY / PREVENTION
INCIDENT / CRISIS MANAGEMENT
GENERAL CYBER SECURITY CAPACITIES
DIGITAL SOCIETY
ICT systems and e-services

Figure 1 National Cyber Security Framework (eGA n.d.-b)

Once the threats were identified, measures and capacities followed, with the selection of important and measurable aspects. This led to the development of the 46 indicators, which in turn are grouped into 12 capacities (seen in Figure 2):

1. Cyber security policy development
2. Cyber threat analysis and information
3. Education and professional development
4. Contribution to global cyber security
5. Protection of digital services
6. Protection of essential services
7. E-identification and trust services
8. Protection of personal data
9. Cyber incidents response
10. Cyber crisis management
11. Fight against cybercrime
12. Military cyber operations

(eGA n.d.-b, 2020)



Version 5 Apr 2019 Choose a version

GENERAL CYBER SECURITY INDICATORS

1.	Cyber security policy development	1	7	14%
2.	Cyber threat analysis and information	0	5	0%
3.	Education and professional development	7	9	78%
3.1.	Cyber safety competencies in primary or secondary ed...	1		
3.2.	Bachelor's level cyber security programme	0	2	
3.3.	Master's level cyber security programme	2		

REQUIREMENTS

Criteria

There is at least one cyber security / electronic information security focused programme at Master's or equivalent level.

Accepted references

Accredited study programme

EVIDENCE

http://www.fisc.utp.ac.pa/maestria-en-seguridad-informatica

https://www.uip.edu.pa/maestrias/sistemas-de-informacion/maestria-en-ge...

3.4.	PhD level cyber security programme	2		
3.5.	Cyber security professional association	2		
4.	Contribution to global cyber security	2	6	33%

BASELINE CYBER SECURITY INDICATORS

5.	Protection of digital services	3	5	60%
6.	Protection of essential services	0	6	0%
7.	E-identification and trust services	6	9	67%
8.	Protection of personal data	4		100%

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9.	Cyber incidents response	3	6	50%
10.	Cyber crisis management	1	5	20%
11.	Fight against cybercrime	9		100%
12.	Military cyber operations	1	6	17%

Figure 2 Partial screenshot of a Country Page (Panama) with the third capacity expanded and Indicator 3.3 expanded as well

Each measurable indicator is attributed either 0 points (for no evidence) or a specific number of predetermined points (for existing evidence). A country must publicly provide proof of fulfilment of a specific indicator's criteria in order to gain those points. Therefore, to fulfil a specific capacity, a country should provide proof of fulfilment of that capacity's indicators (see Annex 1 for a full overview of the capacities, the indicators and their respective weights). For example, capacity 1 (i.e., cyber security policy development) contains four indicators (i.e., 1.1, 1.2, 1.3, and 1.4). Each indicator in turn has been assigned a number of points and is subjected to the 'all-or-nothing' approach regarding evidence. Then, the points of indicators with evidence can be divided by the total of points possible in a capacity to indicate the completion rate of that capacity. Following the previous example, if Country A only has evidence for indicator 1.1, it presents a completion rate of 43% for capacity 1; if Country B has evidence for indicators 1.3 and 1.4, it presents a completion rate of 28% for capacity 1; if country C has evidence for all indicators, it presents a completion rate of 100% for capacity 1.

All evidence is collected by the NCSI team, or by country contributors,[2] and is submitted via the back-end platform and verified by experts[3], who either accept or reject it for the specific indicator that they have been presented. The verification process is not public, but if a piece of evidence is rejected, the experts can leave an explanation for the submitter. Accepted evidence is published in the corresponding country page and visible to any visitor of the website.

The NCSI has been utilised extensively across recent academic debates (Andrade et al. 2021; Calderaro & Craig 2020; Maglaras et al. 2020). Jazri & Jat (2017) mention the NCSI in their road toward "*proposing a simplified and quick framework of measuring cyber security risks profile for critical organizations*" (page 1). Yarovenko (2020) used the NCSI in her "*assessment of the level of threat to national information security*" (page 195). Farahbod et al. (2020) uses information from the NCSI and other international indices to "*explore the relationship between cyberattacks and the factors that can possibly be used to predict the impact of such attacks within supply chain domains*" (page 63). Kruhlov et al. (2020) make use of NCSI country data in their attempt to "*analyze the possibility of providing cybersecurity through the use of public-private partnership (PPP) mechanisms*" (page 1). And most recently, Urbanovics (2022) utilized NCSI country data for

[2] The NCSI core team has varied among the years, containing between two to five individuals, (eGA, n.d.-a) while the country contributors themselves have also fluctuated as well, stabilizing at around 60% of the number of countries in the index.

[3] As to ensure bias is as low as possible during the verification process, the evidence is checked by at least two different individuals who are considered cybersecurity experts and have previously collaborated in this area with eGA. To guarantee the impartiality of their decisions, their identifiable information is not made public by neither the system nor the NCSI team.

the quantitative analysis of an overarching "*comparative analysis of the strategy development processes in six Latin American countries including Argentina, Brazil, Chile, Colombia, Mexico and Peru*" (page 79).

The following analysis and discussion sections includes the data of all 161 countries that were available in the NCSI late January 2023 (NCSI 2022, 2023). The data was valid as of its extraction date; however, it was made up from country datasets last updated between 2020 and 2023.[4] Given the large number of the studied sample size, the national results are presented at the level of continents and regions, using the country groupings of the M49 Standard of the Statistics Division of the United Nations Secretariat. It categorizes countries purely by geography and has been used in papers touching upon global matters, albeit mostly in nature research (e.g., De la Fuente et al. (2020), Amon et al. (2022)). The M49 Standard was chosen since there exists no other alternative to group such a large sample of countries without running into inherent definition issues due to lack of consensus on the classification terminology (e.g., small, main, developing countries, etc.), there exist no similar papers dealing with such a large sample in the field and the NCSI presents information about U.N. members and allows to visualize them by said standard. Additionally, it is a classification system that helps "*to circumvent several concerns levied against national comparisons*" (Field et al. (2021), 1800).

Each country is presented in one region only, and these geographic regions are based on continental regions (United Nations 2021) (see Annex 2 for a full overview of the regions and the countries in them). For a better presentation of the results, the data has been arranged into radar charts (Figures 3 through 8), with each of the spokes (not illustrated for the purpose of simplicity) representing an NCSI capacity (as indicated in each of the vertices), with values corresponding to the completion rate (the centre point representing a 0% completion rate, and each vertex, 100% completion rate). The regional average completion rate values for all capacities have been connected to one another through the use of coloured lines, thus becoming the global and corresponding regional snapshots. While Figure 3 presents the global and regional snapshots,

[4] Being a live index, the countries are updated constantly and continuously as information is made available by the NCSI team or the different country contributors. As of late January 2023, there were only 161 countries in the NCSI and all of them were last updated between 2020 and 2023. All available countries in the NCSI were used for this publication (see Annex 2 for the comprehensive list), no countries in the NCSI were excluded.

Figures 4 through 8 also present the best performing countries for each capacity. This latter group of Figures, in addition to presenting the global and regional snapshots, includes the top two completion rate values for each specific capacity and any country that achieved such value. Said countries have been noted using the ISO 3166-1 alpha-2 country codes[5], and placed in a random order around the corresponding point that represents the value of the completion rate. If more than eight countries at a time scored the same completion rate, the placeholder 'M#C' (i.e., multiple number of countries) has been used in the figures to replace such a large group of countries that cannot be orderly presented in the figure.

Global and Regional Findings

Globally, personal data protection and fight against cybercrime capacities represent the top focus of countries. Africa, the Americas, Asia and Europe present more than 50% completion for the former capacity, while only America, Asia and Europe do so for the latter. Incident response is slightly above halfway its completion rate; however, this is due to Europe and Asia's completion rates balancing out the lower ones from the rest of the regions.

The protection of digital services and crisis management capacities have been underdeveloped globally. All regions, except for Europe, present less than 25% completion in relation to digital service protection. Crisis management is Europe's lowest completion rate (47%), which is still higher than the rest of the regions'. Throughout the world, the other lagging capacities are cyber military operations and the protection of essential services. The rest of the capacities have more mid-range completion values, however, variations among individual regions. Based on the collected data, the cyber security trends as of late January 2023 have been as shown in Figure 3.

[5] The ISO 3166 standard can be found at: https://www.iso.org/iso-3166-country-codes.html

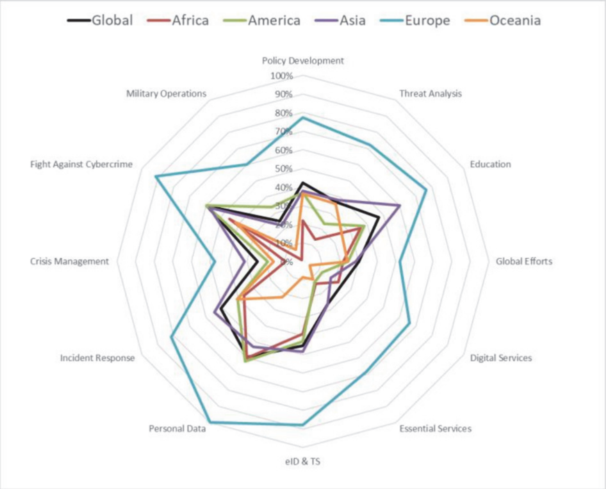


Figure 3 Global cybersecurity focus and in each of the individual regions

The next sub-sections will delve into the different regions, in alphabetical order, and their findings, followed by the Discussion and Recommendations section which will present inductive trends and patterns.

Africa

The African region excels at personal data protection (in relation to the rest of the capacities), with mid-range scores in the fight against cybercrime, incident response and electronic identification and trust services. They are underdeveloped in military operations and cyber crisis management, with more work needed regarding the protection of essential services and cyber threat analysis. Morocco and Tunisia score the highest, with high completion percentages in nine and seven of the capacities, respectively (Figure 4).

In this region, 46% of the countries have no policy development capacity at all. As of 2023, only Benin and Egypt lead the capacity, followed by Nigeria. Similarly, threat analysis is among the capacities that contain the lowest completion in Africa. Nevertheless, four countries present the highest (80%) completion rate. Egypt and Tunisia lead in the next capacity related to education and professional development, while Nigeria and Ghana lead with 67% completion rate in global efforts (Figure 4).

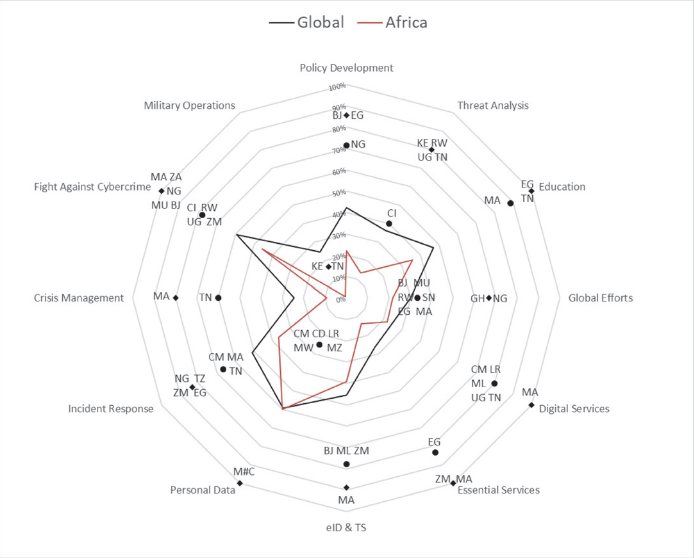


Figure 4 Cybersecurity focus in Africa and top scorers for each capacity

Morocco is at the forefront with a 100% completion rate in the protection of digital services capacity, closely followed by Cameroon, Liberia, Malawi, Tunisia, and Uganda. Zambia, Morocco and Egypt return with completion rates of 100%, 100%, and 83%, respectively, for the protection of essential services. Regarding electronic identification and trust services, Benin, Mali and Zambia have a 78% completion rate, following Morocco's 100% completion rate (Figure 4).

Data protection is the capacity in which 21 out of the 37 African countries in the NCSI have achieved 100% completion rate, with Cameroon, the Democratic Republic of Congo, Liberia, Malawi and Mozambique following with 25%. The incident response capacity has four leading countries (Egypt, Nigeria, Tanzania, and Zambia) all with 83% completion rate. However, cyber crisis management is underdeveloped in Africa (and led by Morocco and Tunisia with a 80% and 60% completion rate, respectively). In the fight against cybercrime, Benin, Mauritius, Morocco, Nigeria and South Africa lead with 100% completion rate. Finally, in the military operations capacity, Kenya and Tunisia lead with a 17% completion rate because of their participation in a international military exercises with cyber components (Figure 4).

Americas

The American region’s average overall trends are under the global average, except for the Military Cyber Operations, Fight Against Cybercrime and Personal Data Protection capacities. The countries should work hard to improve the protection of digital and essential services, crisis management and threat analysis. The Dominican Republic has eight capacities with high completion percentages, while Canada, Paraguay and the United States follow with high completion percentages in seven capacities. Nevertheless, other countries also score at the top of in individual capacities (Figure 5).

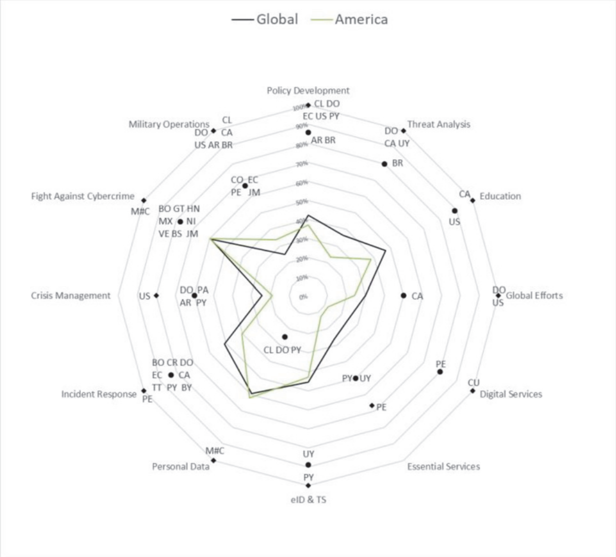


Figure 5 Cybersecurity focus in the Americas and top scorers for each capacity

Regarding policy development, a 100% completion rate exists in the United States, Ecuador, Paraguay, Dominican Republic, and Chile. However, threat analysis and global effort capacities are very underdeveloped in the region, with only a handful of countries leading them (Figure 5). The education capacity is headed by the Canada and the U.S., with 100% and 89% completion rates, respectively. Slightly more than one third of the region maintains some level of protection of digital services, with Cuba and Peru leading with 100% and 80% completion rates (Figure 5). Regarding the essential services protection capacity, Paraguay and Uruguay are both at 50%, and Peru at 67% completion rate, with almost half of the countries not having any protective elements whatsoever. Electronic ID and trust services in the region is spearheaded by Paraguay 100% and Uruguay 89%. In the region, almost 70% has passed some sort of data protection legislation, but evidence has found that only 21 of them have established a corresponding authority.

Cyber incident response is led by Peru 100%, followed by Bolivia, Costa Rica, the Dominican Republic, Ecuador, Trinidad and Tobago, Paraguay, Uruguay and Canada, with an 83% completion rate. Crisis management is the third most underdeveloped capacity of the region, spearheaded by the U.S. with 80% and Panama, Argentina, Paraguay and the Dominican Republic's 40% completion rates (Figure 5).

The fight against cybercrime capacity is the closest capacity to the global average, however, above it (Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Peru, Canada, the U.S., Argentina and Paraguay lead with a 100% completion rate, with followed by other countries' 78% rate). Finally, the region's military cyber operations capacity exceeds the global average, and is spearheaded by 4 Latin American countries, Canada, and the U.S. (Figure 5).

Asia

Asia's highest scoring capacity revolves around education, followed by the fight against cybercrime. Their lowest scores are evidenced in the protection of digital services, followed by cyber military operations and the protection of essential services. Saudi Arabia, Singapore and Malaysia score the highest, with high completion percentages in eight of the capacities, respectively, followed by South Korea and Cyprus, in six of them.

In Asia, the policy development capacity's average is below the global average. Only 17 nations (41% of the countries in the sample) have reached a completion rate of more than 50%. Out of these, Georgia, Japan, South Korea and Qatar have achieved 100% completion rate in the policy development capacity (Figure 6).

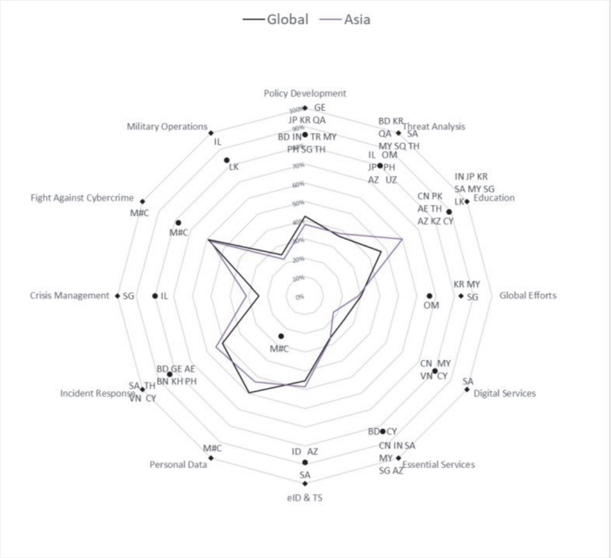


Figure 6 Cybersecurity focus in Asia and top scorers for each capacity

Regionally speaking, the threat analysis capacity is barely higher than the global average, with Bangladesh, Malaysia, Qatar, Saudi Arabia, Singapore, South Korea and Thailand having achieved a 100% completion rate. The education capacity in the region is better than the global average, with 61% of the sample countries achieving more than 50% of a completion rate. However, in global efforts, the Asian region scores lower than the global average, with South Korea, Singapore and Malaysia spearheading efforts (Figure 6).

As previously mentioned, the digital services protection trend in Asia is below the global average. Only Saudi Arabia reaches a 100% completion rate, while China, Cyprus, Malaysia and Vietnam score 80%. Essential service protection, from a regional perspective, is tied to the global trend. The top scorers of this capacity include Azerbaijan, China, India, Malaysia, Saudi Arabia and Singapore. eID and trust services are spearheaded by Saudi Arabia (100%) and Indonesia and Kazakhstan (89% completion rates) (Figure 6).

Data protection has been legislated in 30 countries, but the corresponding authority has only been found in 19 of them. Regional incident response capacity is slightly better than the global mean. Cyprus, Saudi Arabia, Thailand and Vietnam, lead with 100% completion rate (Figure 6).

Crisis management is the fifth lowest capacity in the region, but it is still better than the global average. Singapore leads with 100% completion rate, followed by Israel, with 80%. In the fight against cybercrime, the region scores slightly below the global average. Of the sample, 32 nations have evidence of some form of unit designated to tackle cybercrime and 19 have a governmental digital forensics unit. Finally, in the military operations capacity, Israel presents a 100% completion rate, followed by Sri Lanka at 83% (Figure 6).

Europe

Europe's capacities exceed the global average, and they are top performers in personal data protection. Their lower scores are focused on crisis management, global efforts, and military operations capacities. Greece, Belgium, Czech Republic, Germany and Lithuania are the top scorers with high completion rates; however, they are not the only ones (Figure 7).

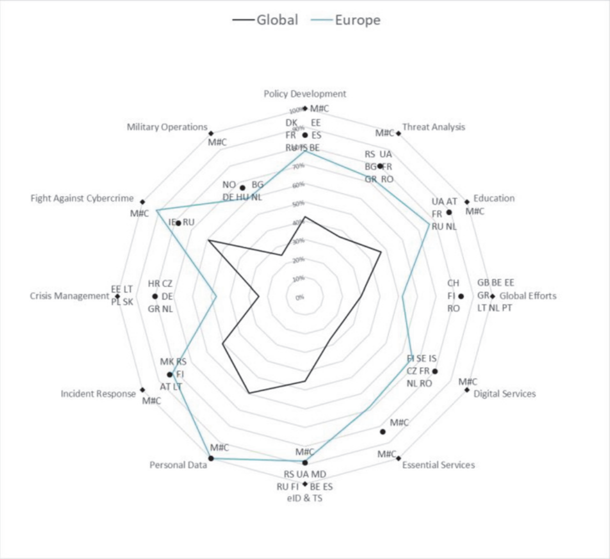


Figure 7 Cybersecurity focus in Europe and top scorers for each capacity

Out of the 39 countries of the region, 30 have established a cyber security policy unit, and have indicated a policy coordination format (but not necessarily the same countries). Only 36 nations have published a national cybersecurity strategy, and of those only 25 have a corresponding implementation plan. Regionally, the cyber threat capacity is regionally at a high level: thirty-four of the countries maintain a cyber safety and security website, 28 of them have established a cyberthreat analysis unit and 23 regularly publish their cyber threat reports.

The educational capacity is also well developed in the region. Master's degrees in cybersecurity topics are the most common educational level with 34 countries having some form of programme, and PhD level programmes are the least available in 24 countries. Global efforts are also quite spread out in the region. The United Kingdom, Belgium, Estonia, Greece, Lithuania, the Netherlands, and Portugal lead this capacity with 100% completion rate (Figure 7). The Budapest convention on cybercrime has been signed by 36 nations and all the countries in the region maintain representation in international cyber security cooperation formats.

Approximately 92% of the region has undertaken efforts to protect digital service providers, of which 28 nations have established cyber security responsibilities for digital service providers, while 26 countries have done so for the public sector as well. The essential services capacity is also widespread, 34 of the countries have identified their corresponding operators of essential services while 31 of those have legally required them to follow those minimum cybersecurity standards for their protection and 27 have established at least one competent corresponding supervisory authority.

The basis for eID and trust services has been well cemented in the region and cyber incident response is similarly almost universal (i.e., a regional average completion rate value that equal to the second top completion rate value, and close to 100%, for each capacity). However, the cyber crisis management capacity is the least developed in the region. Even though 32 countries have participated in international cyber crisis exercises and 20 have executed their own national level drills, only 12 nations have made public any kind of cyber crisis management plan and only 8 have legislated operational support from volunteers during cyber crises.

Finally, combating cybercrime is also a highly scored regional endeavour, while almost 85% of the region's countries present evidence of military cyber operation capacities

Oceania

Oceania's strengths surface relative to incident response, policy development and the fight against cybercrime. Its threat analysis capacity almost equals the global average trend; however, there's still a lot of work to be done in all the rest of the capacities since they are below the global average, and more specifically in terms of digital service protection, electronic ID and trust services and military operations. Australia and New Zealand spearhead the region, with high completion rates in 12 and 10 of the capacities, respectively (Figure 8).

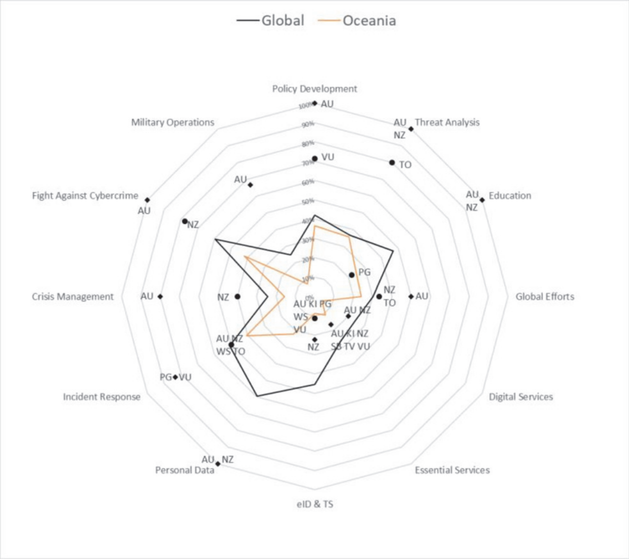


Figure 8 Cybersecurity focus in Oceania and top scorers for each capacity

The policy development capacity in the region it's led by Australia with a full completion rate, closely followed by Vanuatu with 71%. Threat analysis capacities in the region are led by Australia and New Zealand with 100% completion rate followed up by Tonga with an 80% completion rate. Regarding education only three countries register any completion rate, Australia, and New Zealand at 100% and Papua New Guinea at 22% (Figure 8).

Australia and Tonga are the only countries that have signed the Convention on Cybercrime, and Australia and New Zealand have endeavoured in cyber security capacity building activities for other countries and personal data protection. Nevertheless, all countries in the region maintain representation in international cooperation formats.

The protection of digital services is the most underdeveloped capacity in the region (with Australia and New Zealand's 20% completion rate) and the protection of essential services is led by a 17% completion rate by multiple countries. Cyber incident response has also been undertaken by two thirds of the nations and is spearheaded by New Zealand. Personal data protection is led once again by Australia and New Zealand with full completion rates, having passed personal data protection acts and established the corresponding authority. No other country in the region has advanced in terms of this capacity (Figure 8).

Cyber incident response has also been undertaken by two thirds of the nations, led the capacity by Papa New Guinea and Vanuatu with an 83% completion rate, while the rest of the countries follow at 50%. The crisis management capacity only shows endeavours in three countries Australia 80%, New Zealand 40%, followed by Tonga. In relation to the fight against cybercrime there has been much more activity in the region. Seven nations criminalize cybercrimes while Australia and New Zealand contain both cybercrime and digital forensics units. Finally in relation to the military cyber operations capacity only Australia has a cyber operations unit and has participated in international military cyber exercises (Figure 8).

Discussion and Recommendations

Globally, the snapshot provided in this study appears to demonstrate countries focusing upon reactionary measures rather than proactive endeavours. This is exhibited by the high scores in the fight against cybercrime and incident response capacities and the low scores in digital and essential services protection, cyber crisis management and threat analysis. Countries must implement and/or improve upon their proactive activities, in addition to being prepared to react to incidents and threats. With ever increasing levels of electronic and trust services throughout the world, all stakeholders should realize that cyber security is a concern for everyone. In that line of thought, global efforts (from those within the same region and to those across regional boundaries) must be redoubled and increased so that different capacities may be developed by those countries that need them. The shared data also shows that best practices can be implemented no matter the characteristics of the country or the type of government that it might have.

Africa's high score in personal data protection might have been the result of the adoption of the African Union Convention on Cyber Security and Personal Data Protection, since 2014, which states that the signatories would commit to establishing a legal framework relative to personal data protection. This brings up considerations that regional agreements and treaties might help push national cybersecurity towards improvement. It would be worth exploring if such a commitment for any of the other capacities would make a positive difference in the region. Given the region's young population, we advocate for less efforts into the military cyber operations capacity and more development of educational opportunities, coupled with the creation of the protective frameworks through crisis management mechanisms and the protection of the digital and essential services. Similarly threat analysis and policy development seem to be lagging behind, both of which are necessary components for robust level of national cybersecurity.

Generally speaking, government regulation of the private sector is not well seen in the Americas region. While this might not be the main or only reason behind the low scores in the digital and essential services protection, we believe it is still an important component. When talking about national cybersecurity multiple stakeholders have responsibilities in this context. The government must work with the private sectors and all other relevant parties to establish a baseline of minimum cyber security requirements and to ensure their application. An interesting phenomenon was identified in the Caribbean subregion, where island nations had scored for the protection of essential services. Closer inspection revealed that they had identified their essential services prior to the advent of modern ICT (identified by the dates of enactment of the legislation relative to natural disasters and essential services). These countries can work with the existing legislation so that in addition to natural phenomena crises they are also covered in case of cyber incidents. Next to Oceania and Africa, this region has also the lowest average score in regard to the education capacity; future efforts must focus on these components. With the ongoing development of the region, threat analysis and cyber crisis management must also become strategic priorities, especially for those countries lacking a national armed force.

Second to Europe, Asia’s focus on the education capacity is a step in the right direction for the future of the region. Nevertheless, efforts must not shun away from the protection of digital and essential services. With better scores in response crisis management and threat analysis than the global average, intra-regional efforts and cooperation should allow individual countries to reach a more homogeneous level. Policy development electronic identification trust services and personal data protection must also receive a boost.

Europe’s all around high levelled capacities could be attributed to the regional standards and common legislative instruments[6] that have pushed the issue of cybersecurity to the forefront. Nevertheless, the cyber crisis management capacity is still a bit lacking in this respect and further endeavours must be geared towards developing these components. The high scores of the education capacity should further be reflected into global efforts and cooperation. We believe the main risk to the region to be complacency and the maintenance of the status quo, which must never be the norm around always progressing cyber capacity building and technological advancements.

The sample of countries from Oceania is limited due to the lack of available infrastructure and hardware necessary for the maintenance of cyberspace in such remote nations. Similarly, to the Caribbean nations (in the American region), most of the countries have identified their essential services due to legislation dealing with emergency situations, caused specifically by natural phenomena. While not specifically related to the cybersecurity topic, the identification of such services gives them an advantage since, they can now build upon it with the corresponding cyber security legislation. Nevertheless, they must make sure that in the context of cyberspace they have identified all the necessary essential services for them to be fully protected. The military cyber operations capacity will be hard to improve within the remote island nations due to their inherent lack of armed forces. Rather, those efforts must be redirected into the protection of digital and essential services and the development of a cyber crisis management system.

[6] At first glance, inductively, more European Union (EU) countries have an increased number of 100% completion rates in multiple capacities, than non-EU countries. However, the M49 Standard of the Statistics Division of the United Nations Secretariat does not group all EU countries in the same region. Additionally, under this grouping, the term ‘non-EU countries’ include the Russian Federation, Switzerland, and the United Kingdom, which are all showcased in the region for their performance. Future research is recommended on supranational unions, specific subregions and/or categories.

Limitations and Future Research

The NCSI itself presents a couple of biases. The first one is that it was created within the context of the European Union and its understanding of cybersecurity, by an Estonian team. As such, some of the indicators were modelled after studying the best practices of the European region. Since the indicators are the components of the capacities and the 'all-or-nothing' approach is followed regarding the allotment of points in the event of evidence, this has an impact on the completion rate for the countries. Nevertheless, even if such indicators might provide a region with any apparent advantage, they are still some of the best practices in national cybersecurity that have been implemented and exist around the world. Any similar metrics, with a different degree of strictness, would still yield the same inductive trends (i.e., similarities and differences), and any different metrics are outside the scope of this paper, but a good starting point for future research. The second bias is the fact that the index only accepts publicly available evidence. In some countries cybersecurity is intricately connected with the concept of national security and as such, evidence might not be disclosed to the public. In such cases it is not possible to award the points if there is no publicly available evidence that can be shared. Nevertheless, the creators and administrators of the index believe that having a multinational index based on publicly available official information outweighs any downgrade in position that a country might suffer due to lack of transparency.

The article has presented how national cybersecurity is being undertaken throughout the world. Regional trends (i.e., similarities and differences) exist (as presented in the previous section), but globally, reactionary measures are being preferred rather than proactive ones. The paper also presents a number of countries from which best practices can be adopted for specific topics (as presented in the regional subsections of the 'Global and Regional Findings' section). As previously stated, this article serves as a global and regional snapshot and point of reference for any future single case or comparative studies of national cybersecurity. Since national cybersecurity includes so many individual components and since this article explores 161 countries in an overarching way, we believe there will never not be a lack of future research topics stemming from this document in this field. With this article we also wanted to showcase countries and regions that have arguably been underrepresented across academic literature and policy debates and give visibility to their efforts, i.e., non-major states and actors. Future case studies could start focusing on these countries through the whole 12 capacities lens or more in depth with some of the specific indicators. Similar comparative studies may be proposed among specific subregions and subcategories (i.e. developing, small, island, etc.) of nations, or supranational unions (i.e. African Union, European Union, Caribbean Community, etc.). Since the National Cyber Security Index is publicly available, such possibilities will remain on the table.

Disclaimers

The NCSI was originally developed through the "Development of a National Cyber Security Index" project, funded by the Ministry of Foreign Affairs of Estonia and managed by the e-Governance Academy. The author of this article has acquired and managed the country data for the NCSI and this article through the following projects: 2018 – 2020 "Shaping of Trusted Information Societies in Developing Countries"; 2020 – 2022 "Advancing Cybersecurity Capacities for Digital Transformation"; all funded by the Ministry of Foreign Affairs of Estonia and managed by the e-Governance Academy. The NCSI updated its methodology in November 2023. Nevertheless, all data from the previous methodology (i.e. that was used for this article) was saved for historical purposes and is publicly available.

Acknowledgements

I would like to extend my thanks and appreciation to my colleagues at the e-Governance Academy's Cybersecurity Competence Center (Ms. Merle Maigre, Ms. Epp Maaten, Ms. Kadri Kaska, and Mr. Hauke Schulz) and to all the national contributors who have helped to keep the NCSI up to date throughout the years.

Annex 1

NCSI Capacities and their Indicators	% value of corresponding Capacity
1. Cyber security policy development	100
1.1. Cyber security policy unit	43
1.2. Cyber security policy coordination format	29
1.3. Cyber security strategy	14
1.4. Cyber security strategy implementation plan	14
2. Cyber threat analysis and information	100
2.1. Cyber threats analysis unit	60
2.2. Public cyber threat reports are published annually	20
2.3. Cyber safety and security website	20
3. Education and professional development	100
3.1. Cyber safety competencies in primary or secondary education	11
3.2. Bachelor’s level cyber security programme	22
3.3. Master’s level cyber security programme	22
3.4. PhD level cyber security programme	22
3.5. Cyber security professional association	22
4. Contribution to global cyber security	100
4.1. Convention on Cybercrime	17
4.2. Representation in international cooperation formats	17
4.3. International cyber security organisation hosted by the country	50
4.4. Cyber security capacity building for other countries	17
5. Protection of digital services	100
5.1. Cyber security responsibility for digital service providers	20
5.2. Cyber security standard for the public sector	20
5.3. Competent supervisory authority	60
6. Protection of essential services	100
6.1. Operators of essential services are identified	17
6.2. Cyber security requirements for operators of essential services	17
6.3. Competent supervisory authority	50
6.4. Regular monitoring of security measures	17
7. E-identification and trust services	100
7.1. Unique persistent identifier	11
7.2. Requirements for cryptosystems	11
7.3. Electronic identification	11
7.4. Electronic signature	11
7.5. Timestamping	11
7.6. Electronic registered delivery service	11
7.7. Competent supervisory authority	33

NCSI Capacities and their Indicators	% Value of corresponding Capacity
8. Protection of personal data	100
8.1. Personal data protection legislation	25
8.2. Personal data protection authority	75
9. Cyber incidents response	100
9.1. Cyber incidents response unit	50
9.2. Reporting responsibility	17
9.3. Single point of contact for international coordination	33
10. Cyber crisis management	100
10.1. Cyber crisis management plan	20
10.2. National-level cyber crisis management exercise	40
10.3. Participation in international cyber crisis exercises	20
10.4. Operational support of volunteers in cyber crises	20
11. Fight against cybercrime	100
11.1. Cybercrimes are criminalised	11
11.2. Cybercrime unit	33
11.3. Digital forensics unit	33
11.4. 24/7 contact point for international cybercrime	22
12. Military cyber operations	100
12.1. Cyber operations unit	50
12.2. Cyber operations exercise	33
12.3. Participation in international cyber exercises	17

Annex 2

The 161 countries in NCSI and analysed in this paper are as follows: 37 countries from Africa, 35 from America, 41 from Asia, 39 from Europe, and 9 from Oceania.

Africa	America	Asia	Europe	Oceania
Angola	Antigua and Barbuda	Afghanistan	Albania	Australia
Algeria	Argentina	Armenia	Austria	Kiribati
Benin	Bahamas	Azerbaijan	Belarus	New Zealand
Botswana	Barbados	Bahrain	Belgium	Papua New Guinea
Burundi	Belize	Bangladesh	Bosnia and Herzegovina	Samoa
Cameroon	Bolivia	Bhutan	Bulgaria	Solomon Islands
Chad	Brazil	Brunei Darussalam	Croatia	Tonga
Congo (Democratic Republic of the)	Canada	Cambodia	Czech Republic	Tuvalu
Côte d'Ivoire	Chile	China	Denmark	Vanuatu
Egypt	Colombia	Cyprus	Estonia	
Ethiopia	Costa Rica	Georgia	Finland	
Ghana	Cuba	India	France	
Kenya	Dominica	Indonesia	Germany	
Liberia	Dominican Republic	Iran (Islamic Republic of)	Greece	
Libya	Ecuador	Israel	Hungary	
Madagascar	El Salvador	Japan	Iceland	
Malawi	Grenada	Jordan	Ireland	
Mali	Guatemala	Kazakhstan	Italy	
Mauritania	Guyana	Korea (Republic of)	Latvia	
Mauritius	Haiti	Kyrgyzstan	Lithuania	
Morocco	Honduras	Lao PDR	Luxembourg	
Mozambique	Jamaica	Malaysia	Malta	
Namibia	Mexico	Mongolia	Moldova (Republic of)	
Nigeria	Nicaragua	Myanmar	Montenegro	
Rwanda	Panama	Nepal	Netherlands	
Senegal	Paraguay	Oman	North Macedonia	
Seychelles	Peru	Pakistan	Norway	

Africa	America	Asia	Europe
Sierra Leone	Saint Kitts and Nevis	Philippines	Poland
Somalia	Saint Lucia	Qatar	Portugal
South Africa	Saint Vincent and the Grenadines	Saudi Arabia	Romania
South Sudan	Suriname	Singapore	Russian Federation
Sudan	Trinidad and Tobago	Sri Lanka	Serbia
Zambia	United States	Syrian Arab Republic	Slovakia
Zimbabwe	Uruguay	Tajikistan	Slovenia
Tanzania, United Republic of	Venezuela	Thailand	Spain
Tunisia		Turkey	Sweden
Uganda		Turkmenistan	Switzerland
		United Arab Emirates	Ukraine
		Uzbekistan	United Kingdom
		Vietnam	
		Yemen	

References

Amon, D. J., et al. (2022). My Deep Sea, My Backyard: a pilot study to build capacity for global deep-ocean exploration and research. Philosophical Transactions of the Royal Society B. http://doi.org/10.1098/rstb.2021.0121

Andrade, R. O., Cordova, D., Ortiz-Garcés, I., Fuertes, W., & Cazares, M. (2021). A Comprehensive Study About Cybersecurity Incident Response Capabilities in Ecuador. *Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-3-030-60467-7_24

Bada, M., Solms, B. Von, & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness for users and executives in Africa. *International Journal On Advances in Security*.

Bay, M. (2016). What is Cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal For Media Research*.

Berthelet, P. (2020). La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels. *Revue Québécoise de Droit International*. https://doi.org/10.7202/1067257ar

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*. https://doi.org/10.1080/01436597.2020.1729729

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Bie3: Boletín IEEE, ISSN-e 2530-125X, Nº. 2 (Abril-Junio), 2016, Págs. 950-966*.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*. https://doi.org/10.22215/timreview835

De la Fuente, B., et al. (2020). Built-up areas within and around protected areas: Global patterns and 40-year trends. *Global Ecology and Conservation*. https://doi.org/10.1016/j.gecco.2020.e01291

Dewar, R. S., Baezner, M., Cordey, S., & Robin, P. (2018). *National Cybersecurity and Cyberdefense Policy Snapshots*.

eGA. (2022). Upgrading National Cyber Resilience: National Cybersecurity in Practice 2. https://ega.ee/wp-content/uploads/2021/05/NCSI-Cyber-Resilience-Digi_F.pdf eGA. (n.d.-a). *National Cyber Security Index*. https://ncsi.ega.ee/

eGA. (n.d.-b). *NCSI - Methodology*. https://ncsi.ega.ee/methodology/. Last accessed October 2022.

eGA. (2020). *National Cyber Security in Practice*. https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

ENISA - European Union Agency for Network and Information Security. (2015). *Definition of Cybersecurity - Gaps and overlaps in standardisation*.

ENISA - European Union Agency for Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology*.

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts. *Journal of Business and Behavioral Sciences*, *30*(1), 63–71.

Field, J. G., Bosco, F. A., Kraichy, D., Uggerslev, K. L., Geiger, M. K. (2021). More alike than different? A comparison of variance explained by cross-cultural models. *Journal of International Business Studies, 52,* 1797–1816.

Guranda, V. (2021). La Cyber-sécurité. *Technical-Scientific Conference of Undergraduate, Master and Phd Students*.

Ham, J. Van Der. (2021). Toward a Better Understanding of “Cybersecurity.” *Digital Threats: Research and Practice*. https://doi.org/10.1145/3442445

ITU-D. (n.d.). ITU-D Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model (Methodology). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf

Jazri, H., & Jat, D. S. (2017). A quick cybersecurity wellness evaluation framework for critical organizations. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. https://doi.org/10.1109/ICTBIG.2016.7892725

Kruhlov, V., Latynin, M., Horban, A., & Petrov, A. (2020). Public-private partnership in cybersecurity. *CEUR Workshop Proceedings*.

Le Barreau, L., & Longeon, É. (2016). Les enjeux de cybersécurité en Arabie saoudite: Variables culturalistes et conceptualisation d’une stratégie nationale. *Études Internationales*. https://doi.org/10.7202/1039541ar

Loiseau, H., Millette, C.-A., & Lina Lemay, et. (2013). La stratégie du Canada en matière de cybersécurité : de la parole aux actes? *Canadian Foreign Policy Journal*. https://doi.org/10.1080/11926422.2013.805151

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., & Ioannidis, S. (2020). Cybersecurity in the Era of Digital Transformation: The case of Greece. *2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020*. https://doi.org/10.1109/ITIA50152.2020.9312297

Newmeyer, K., Cubeiro, E., & Sánchez, M. (2015). Ciberespacio, Ciberseguridad Y Ciberguerra. *II Simposio Internacional de Seguridad y Defensa: Perú 2015.*

Newmeyer, K. P. (2015). Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal*, *1*(3), 9–19.

NCSI. (2022). Happy New Year 2023!. In *News*. https://ncsi.ega.ee/88/happy-new-year-2023/

NCSI. (2023). Updated Countries January 2023. In *News*. https://ncsi.ega.ee/89/updated-countries-january-2023/

Pohlmann, N. (2019). Cyber-Sicherheit. In *Cyber-Sicherheit*. https://doi.org/10.1007/978-3-658-25398-1

Romaniuk, S., & Manjikian, M. (2021). *Routledge Companion to Global Cyber-Security Strategy (1st ed.)*. Milton: Taylor and Francis.

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, *10*(3), 21–45.

Shackelford, S., & Kastelic, A. (2014). Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2531733

Stevens, T. (2018). *Global Cybersecurity: New Directions in Theory and Methods.* https://doi.org/10.17645/pag.i92

United Nations. (2021). *Standard country or area codes for statistical use (M49): Geographic Regions*. Series M, No. 49. https://unstats.un.org/unsd/methodology/m49/

Urbanovics, A. (2022). Cybersecurity Policy-Related Developments in Latin America. *Academic and Applied Research in Military and Public Management Science*, *21*(1), 79–94.

Yarovenko, H. (2020). “Evaluating the threat to national information security.” *Problems and Perspectives in Management*. https://doi.org/10.21511/ppm.18(3).2020.17

Appendix 2

Publication II
Krivonosova, I. & **Serrano-Iova, R.A.** (2021). From the Parliament to a Polling Station: How to Make Electoral Laws More Comprehensible to Election Administrators. In: *Election Law Journal*, Vol 20(4), pp. 364–381. Meredith, M. (Ed.). Mary Ann Liebert, Inc.: U.S. doi:10.1089/elj.2020.0670. ETIS 1.1.

ELECTION LAW JOURNAL
Volume 20, Number 4, 2021
Mary Ann Liebert, Inc.
DOI: 10.1089/elj.2020.0670

From the Parliament to a Polling Station: How to Make Electoral Laws More Comprehensible to Election Administrators

Iuliia Krivonosova and Radu-Antonio Serrano-Iova

ABSTRACT

This article suggests that law modelling (using Business Process Model and Notation, BPMN) could make electoral laws more comprehensible to different stakeholders, and in particular, to election administration, especially in cases of complex elections with multiple voting channels. This solution helps election administrators to translate the complexity of electoral laws into clear instructions. By this, election administration can adapt to the frequent changes in laws, reach better regulatory compliance, and address the barriers they meet during the delivery of the elections, like overtasking and lack of institutional memory. As a proof of the concept, we demonstrate the applicability of the proposed solution by modelling one voting channel available in the 2019 parliamentary elections in Estonia, advance voting. The article contributes to the theory on election administration and suggests how this solution could be used in practice: in the field of the electoral law and outside of it.

Keywords: electoral law, law modelling, election administration, BPMN, Estonia, design science research

> "Laws can be visualised and modelled like other governmental processes and these models can be used as guidelines to develop workflows."
> (Olbrich and Simon 2008, 43)

INTRODUCTION

Electoral laws regulate who organizes elections and how they are organized. However, in practice, it is not always easy to transform electoral laws into clear instructions. First, the legal language of electoral laws might be difficult to comprehend for non-lawyers. Second, some electoral laws allow for multiple interpretations (Kropf, Vercellotti, and Kimball 2013; Suttmann-Lea 2020). Third, electoral laws change frequently, which does not make the task of implementing laws easier. To the contrary, "the potential for error increases when the law changes" (Alvarez and Hall 2006, 497). Given the frequency of modifications, some of

Iuliia Krivonosova is an early stage researcher at the DigiGov Lab, Ragnar Nurkse Department of Innovation and Governance, at Tallinn University of Technology in Tallinn, Estonia. Radu-Antonio Serrano-Iova is a PhD candidate at the DigiGov Lab, Ragnar Nurkse Department of Innovation and Governance, at Tallinn University of Technology in Tallinn, Estonia.

This work was supported by ASTRA "TTÜ arenguprogramm aastateks 2016–2022," Doctoral School in Economics and Innovation, Project code: 2014-2020.4.01.16-0032; Eesti Teadusagentuur [grant number PUT 1361]; ECePS ERA Chair European Union's Horizon 2020 research and innovation program [grant agreement No. 857622], and the PhD school of the Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology. We would like to thank Professor Dr. Robert Krimmer and Dr. David Duenas-Cid for providing invaluable feedback on earlier drafts of this article, and the attendants of the faculty seminar for commenting on the first draft of this article. We are grateful to the *Election law Journal*'s editor and reviewers.

them might "go unnoticed even for several decades" (Ciaghi, Weldemariam, and Villafiorita 2011, 33). Still, in the end, election administrators need to implement the laws and derive from them instructions for poll workers. The more difficult this process is, the less possible it becomes to deliver elections properly.

The process of transforming electoral laws into instructions affects not only election administrators and poll workers but also voters. Given that local election administration involves a high level of discretion (Hall, Monson, and Patterson 2009), the possibility of multiple interpretations of electoral laws might have significant consequences on the conduct of elections and on voters. Poll workers can also exercise discretion, and the more complicated the laws are, the more discretion poll workers can exercise (Atkeson et al. 2014). Thus, poll workers are street-level bureaucrats making "legal decisions on the fly on Election Day" (Alvarez and Hall 2006, 496). Discretion also allows poll workers to "decide to what extent they will follow laws and procedures" (Hall, Monson, and Patterson 2009, 508). As a result, the way electoral laws are implemented can impact the quality and integrity of elections.

This article aims to answer the research question: "How can electoral laws be made more comprehensible to election administrators?" It presents a new approach of how laws could be converted into instructions, which would clearly indicate actors and their activities. This article presents a proof of concept for Business Process Model and Notation (BMPN) as a heuristic tool that may be applied to electoral laws to make them more comprehensible to election administrators and poll workers, limiting individualistic interpretation in different contexts. Such models are especially important in contexts with complex elections with multiple voting channels. To demonstrate how the proposed tool works, we apply it to a case study of the Estonian electoral law, in particular, the Riigikogu [National Parliament] Election Act, in the version for the 2019 parliamentary elections (Riigikogu Election Act 2019).

The article proceeds with a theoretical framework which informs the problem identification (Fedorowicz and Dias 2010). The theoretical framework presents an interplay between the literature on election administration, usage of diagrams for law modelling, and, particularly, the applicability of the BPMN tool to electoral laws. A methodology section follows, before delving into the detailed explanation of how to use BPMN to model electoral laws, and its demonstration on a case of the Estonian electoral law. The discussion section presents the findings derived from the first application of the BPMN to the electoral law. The conclusion elaborates on the implications of this research.

THEORETICAL FRAMEWORK

The theoretical framework builds on three strands of literature. It starts with an overview of the literature on election administration, with the aim of introducing the problem of comprehensibility of electoral laws by election administrators and poll workers. Then, it proceeds to the literature on the usage of diagrams for the modelling of laws. After that, it narrows down to one particular tool for modelling (Business Process Modelling and Notation) and its application to the field of election administration.

Election administration

Globally, electoral law experiences frequent changes that cause some scholars to call it "an ever-changing field" (Geddis 2005, 60). Since the 1990s, "Italy shows a sort of 'hyperkinetic' attitude toward changing its electoral law" (Baraggia 2017, 274). In Canada, since the 2000s, "nearly every area of election law" has been reformed (Pal 2017). And the U.S. is not an exception (Kimball, Kropf, and Battles 2006; Levitt 2012). Election administration implements electoral laws, that is why they need to closely follow these changes.

Furthermore, to implement electoral laws, election administrators need to interpret them: laws constrain and direct election administrators, while still leaving "considerable room for interpretation" (Kropf, Vercellotti, and Kimball 2013, 244). This subjectivity could be partisan: election administrators could interpret laws in a way that helps their party (Kimball, Kropf, and Battles 2006; Kropf, Vercellotti, and Kimball 2013; Nussbaumer 2013). Ambiguity of electoral laws could also further contribute to "varying interpretations" (Suttmann-Lea 2020, 714) at the level of poll workers.[1] In fact, poll workers are the "most

[1] Poll workers have different titles in different jurisdictions, such as election judges. To be consistent with other research, we refer to them as poll workers in this article.

direct arbiters" (Suttmann-Lea 2020, 714) of electoral laws. In the case of poll workers from the city of Chicago, Suttmann-Lea (2020) finds that personal experiences of poll workers play a role in their interpretation of electoral laws. This subjectivity could challenge the consistency in law application, resulting in unequal treatment of voters. Furthermore, the issue of law interpretation is even more critical in federalist systems with decentralized election administrations, like in the case of the United States or Switzerland.

The need for law implementation requires election administrators and poll workers to have a good understanding of electoral laws and the electoral process. However, that is not always the case: the problem of not understanding their job has been reported by 21 percent of poll workers in the U.S. (Fischer and Coleman, 2008 as cited in Burden and Milyo, 2015), with some poll workers not understanding even basic election laws and procedures (Alvarez and Hall 2006) and some not being able to comprehend instructions (Douglas 2015). Nevertheless, particular moments of the electoral process demand a "nearly flawless peak-capacity performance" (Alvarez and Hall 2008, 830) from the election administrators and poll workers, which is difficult to achieve in such settings.

The abovementioned aspects of electoral law implementation require additional resources from election administration, which is frequently underbudgeted and overtasked (Hale and Slaton 2008; Kimball and Kropf 2006). Electoral activities demand the involvement of election administrators at the maximum capacity, which leaves limited resources for dealing with complicated electoral laws: "as election administration becomes increasingly complex, clerks may believe that they spend more energy complying with the requirements than actually helping citizens vote" (Burden et al. 2012, 743).

Training could potentially help increase comprehensibility of electoral laws and make law implementation more consistent. Training is also a way to address principal-agent problems in elections (Alvarez and Hall 2006). Nevertheless, recent research established in the case of the U.S. shows that the way training is organized now does not bring uniformity in law implementation (Burden and Milyo 2015). To the contrary, training results in a "wide variation in their [poll workers] level of understanding of basic election laws and procedures" (Alvarez and Hall 2006, 497), with poll workers finding training to be "difficult to understand" (Burden and Milyo 2015, 45). Furthermore, while this article operates mainly with two terms—election administrators and poll workers—the reality is more complex: terms for election personnel vary, and each of them can stand for an elected, permanently or part-time employed, or volunteer workforce. This can affect the training environment and subsequently the training outcomes.

Among possible improvements, poll workers suggest that they be provided with handouts/reference materials after a training. Another considered solution to address some aspects of the abovementioned problem is the development of standard operating procedures (Alvarez and Hall 2008; Alvarez, Hall, and Atkeson 2009; Brown and Hale 2020; Kropf, Vercellotti, and Kimball 2013) derived from electoral laws, in order to maintain "a minimum level of consistency" (Alvarez and Hall 2008, 830) in administering elections. Even though election administration in the U.S. has become ever more professionalized, and training has improved over time, there is still a need for training, expressed by both academics (Brown and Hale 2020; Kropf et al. 2020) and practitioners (Adona et al. 2019; McCormick 2020).

Institutional memory might also help in implementing laws with consistency. However, poll workers might have difficulties with accumulating considerable institutional memory. First of all, poll workers are not permanently engaged in these roles (Burden and Milyo 2015; James 2019). This results in high staff turnover. Therefore, there is a need for a tool that would allow new staff to learn quickly how to deliver elections, and who is responsible for what. Second, even experienced poll workers have few chances to "develop a shared set of organizational norms to ensure consistent running of elections" (Suttmann-Lea 2020, 2), or "retain their knowledge of election law and procedure from election to election" due to "the infrequent nature of elections" (Atkeson et al. 2014, 948). Third, even in the cases when all poll workers are well trained, situations of emergent replacement may arise, ranging from pandemics (Krimmer, Duenas-Cid, and Krivonosova 2020a) to national disasters (Stein 2015) to negligence[2] (OSCE/ODIHR 2018).

[2] In every fourth polling station in Italy, some polling station members did not show up and were replaced by volunteers.

These situations also require a tool for quick learning or at least understanding of the electoral procedures, derived from the electoral law.

We accept that in some environments poll workers do not work directly with the electoral law. They rather receive abbreviated instructions developed for them by a higher level of the election administration. However, in such instances, instructions cover solely responsibilities of a considered actor. As a result, the actors know only their own responsibilities: the instructions provide no vision of the overall election management. Given that the scope of the actors involved in election delivery is growing (Garnett and James 2020), the need for understanding what the other actors' activities and responsibilities are will be increasing.

Academics as well as practitioners emphasize the importance of providing poll workers with visual aids to assist them on the Election Day (AIGA Design for Democracy and Election Assistance Commission 2016; Election Assistance Commission 2016). Visual aids could simplify information, convey the meaning graphically, and serve as a precise summary or a reminder which could be used on Election Day. Training for poll workers frequently spreads the message that there is no need to memorize everything. Nevertheless, on Election Day, under significant time constraints, poll workers could find it more feasible to use a one-page diagram, rather than searching through lengthy handouts (Douglas 2015). Guides which are used nowadays by states and counties of the U.S. are considered to be "virtually unusable on Election Day" (Douglas 2015, 367) because of their length and complexity. The same applies to the checklists (Douglas 2015). The post-election audits in the U.S. confirmed that very detailed, but not user-friendly, guides were one of the reasons why some voters were disenfranchised by mistake (City Commissioner's Office 2013). An overview of national practices in the U.S. also claims that guides in the current form are ineffective and not sufficient to prevent poll workers' mistakes, and that poll workers "have little training and few resources to help them when issues arise," while "the right tools" would make mistakes avoidable (Douglas 2015, 354). That being said, the demand for other instruments is well articulated.

However, visual aids are always considered as supporting materials to those already used (e.g., handbooks, checklists), not as a substitution. Among the variety of visual aids, diagrams and flow charts are favored (Election Assistance Commission 2016).[3] In comparison to checklists or handouts, mostly designed for internal use, visual aids such as diagrams could be printed out and displayed as posters at the polling station for the benefit of all participants in the electoral process. This could boost confidence in the electoral process on the part of both election administrators and voters. Furthermore, diagrams are not only used for Election Day activities, but have been also applied to election audits (Alvarez, Hall, and Atkeson 2009).

Models, diagrams, and legislation

In general, public administration activities are more regulated than those of the private sector, with most of them being fixed in legal documents (Olbrich and Simon 2008). Therefore, the link between the law and processes is perhaps most evident in the field of public administration. Election administration, being a part of public administration, follows suit. First of all, it is heavily regulated at the subnational, national, and international levels (Venice Commission 2002). In addition, international organizations, such as the Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights (OSCE/ODIHR) and the Venice Commission, frequently assess national electoral laws and provide recommendations on how they could be improved.

Nevertheless, legislation is frequently written in a way so that sections constantly refer to other sections and subsections, without explicitly repeating the content. When implementing a piece of legislation, an actor might not know which subsections are relevant to a particular practical question, thus, "the reader has to work through all the text" (Smith and Schwarz 1987, 981). One of the available instruments to address this issue is diagrams. A diagram could help "to lead the user through relevant parts of the legislation only" (Smith and Schwarz 1987, 981). Diagrams could be also used to help new employees to understand their job, to "provide a document which would act as a reference when resolving difficult cases," and to "highlight ambiguities and impracticabilities" in the legislation (Smith and Schwarz 1987, 987).

[3] With some recent innovations like picture guides (see, e.g., St Louis City Board of Elections' developments). https://www.eac.gov/sites/default/files/document_library/files/Election-Day-Picture-Guide-sample.pdf

Process modelling brings together diagrams and processes. When considering what the difference is between models and diagrams, in short, a model is “a graphical presentation of a process, function or system” (Van der Waldt 2013), which could take the form of a diagram, but not exclusively: “a model simply enables the reader to visually register and comprehend all the variables and relationships among them” (Van der Waldt 2013). It is particularly good in dealing with complexities, and if implemented correctly serves as a “communication base” for all involved actors (Becker, Rosemann, and von Uthmann 2000, 31).

Comparative studies of electoral laws usually use content analysis (Blais, Massicotte, and Yoshinaka 2001). However, in the field of e-government, law modelling and analysis have been widely used, giving rise to the research field of legal informatics (Ciaghi, Weldemariam, and Villafiorita 2011), legal visualization, and visual laws (Boehme-Neßler 2011a, 2011b). Still, this modelling of laws and procedures is not necessarily conducted in favor of public administration (Ciaghi, Weldemariam, and Villafiorita 2011). Olbrich and Simon (2008, 43) present an overview of approaches to “visualizing legally-defined processes,” bringing evidence that laws have been illustrated since medieval times. One approach to law modelling they present is the translation of paragraphs of a law into process models. Such an approach follows the narrative of the law and builds models on a paragraph-by-paragraph/article-by-article basis. Nevertheless, such an approach might not allow following the sequence of processes from the beginning to the end, as the very same process might be mentioned in different parts of the law. Another strand of literature answers the question “how one derives requirements from a law?” (Siena et al. 2008, 1). A large share of this research field covers the production of software specifications from laws (Gorín, Mera, and Schapachnik 2010).

Business process model and notation

There are many ways of creating process models. Among the variety of modelling languages, we focus on Business Process Model and Notation, because it is considered as a “de facto standard for process modelling” (Walser and Schaffroth 2010, 4). The main difference between BPMN and diagrams is that BPMN is a standardized and widely adopted language, unlike diagrams, which are specific to the authors who produced them, meaning that different authors could depict the same processes with diagrams differently. Each element of BPMN has a defined meaning, clear to anyone who is familiar with the language. Diagrams are the drawing tools, while BPMN is the modeling tool. BPMN is also better in capturing complexities and being able to depict more complex processes in a precise manner.

The common language is of particular importance for contemporary election administration. In countries with decentralized election administration, there is a clearly articulated need for the common language: “at the core, election officials across the country want to do things well and follow the same general blueprint of how to get there,” as well as to “have a common understanding of how things work” (Hubler and Patrick 2020, 155).

BPMN is a standard developed by the Object Management Group to provide a notation that can be understood by all business users and that can bridge “the gap between the business process design and process implementation” (OMG 2011). BPMN was created by the consolidation of the best practices from other different notations into a single standard notation for the purpose of communicating process information in a simple way to a wide range of stakeholders (OMG 2011). It helps to show tasks/activities/responsibilities illustratively and linked, in time and between stakeholders. BPMN has the advantage of representing any organizational process through a dynamic lens, while being easy to comprehend by any reader and widely accepted in academia (Geiger et al. 2018; Mili et al. 2010).

BPMN has been applied to the field of e-government (for quality improvement of e-government services) (Corradini et al. 2011), public administration (for standardization and staff training) (Walser and Schaffroth 2010), and election observation (for attributing each activity to a particular actor and, based on that, for identifying overburdened actors, overlapping activities, and for attributing costs for every activity, by calculating the cost efficiencies of various ways of voting) (Krimmer et al. 2018; Serrano-Iova 2019). Walser and Schaffroth (2010) refer to the successful example of BPMN usage by the Federal Department of Foreign Affairs of Switzerland for training frequently changing staff. The Australian Department of Finance and Administration used BPM to model a parliamentary workflow which simplified staff communication (Villanova University 2020). The U.S. Department of Defense has been using BPMNs for improving processes and use of data for at least a decade (zur Muehlen, Wisnosky, and Kindrick 2010). BPMNs are extensively used in health care in order to create an "understandable graphical model, where management and improvements are more easily implemented by health professionals" (Rojo et al. 2008, 1). Electoral process modelling has been on the agenda of election administrators in the U.S. since 2013 (Hubler and Patrick 2020), in order to create "a visualization of a complex system that functions as a sort of road map for the who, when, and how of election administration" (Hubler and Patrick 2020, 156), and a learning tool.

Ciaghi et al. (2011) and Ciaghi and Villafiorita (2012) conduct law modelling with the help of BPMNs. They use BPMNs for "the visualization and formalization of business processes" (Ciaghi, Weldemariam, and Villafiorita 2011, 29). They differentiate two steps of research: (1) modelling procedures, and (2) analyzing procedures (based on the models). In Ciaghi et al. (2011), they conduct only law modelling, leaving the analysis for further research. In any modelling language, the mark-up of laws is usually conducted manually; hence, it is resource intensive. Nevertheless, the contemporary approaches to law modelling allow automatization of at least some steps in this process (Ciaghi, Weldemariam, and Villafiorita 2011), although it should be applied with care, given that laws frequently allow multiple interpretations.

Finally, a variety of free software is available for the development of BPMNs, thus making this tool accessible for wider populations and contexts. This means that in BPMN a reader finds all in one: a language, a method, a technique, and software for process modelling. For these reasons, we believe BPMN deserves to be tested as a solution for the outlined problems. At the same time, we are not advocating for a particular modelling language.

Table 1 summarizes the aforementioned aspects of the problem. The objectives of the proposed solution aim to resolve these issues.

METHODOLOGY

The aim of this research is to address a very particular administrative challenge in the field of election administration, by creating an artifact or a new practice (Romme and Meijer 2020) that could solve (at least some aspects of) the problem. For this purpose, this research follows the design science research strategy which brings rigor and generalizability to the research (Fedorowicz and Dias 2010) by allowing to "explore and demonstrate the possibilities of new artifacts" (Goldkuhl 2016, 445). So far, there are only a few examples of the design science in the field of election administration (Kasse, Moya, and Balunywa 2013), but it has been widely recognized in a broader field of public administration (Barzelay and Thompson 2010; Romme and Meijer 2020).

This article follows the steps of the design science process developed by Peffers et al. (2007):

- theory-informed problem identification and definition of the objectives for a solution,
- design and development of a solution,
- demonstration of a solution in some setting,
- evaluation of a solution, and communication of results.

Problem identification focuses on operational and institutional aspects of election administration. The demonstration is performed on a case which serves as a validation example of the proposed solution (Goldkuhl 2016). For a case, we chose a holistic (with a single unit of analysis) extreme/unusual case (Yin 2017), to serve as a proof of concept. For a case study, we focus on the Estonian electoral law. The main reason for choosing Estonia as a case was the complexity of the electoral context, yet simplicity in the presentation of the electoral law. This dichotomy makes Estonia an unusual case:

- Estonia provides to all eligible voters multiple voting channels. Many of them are provided simultaneously, at various locations. This increases the complexity of elections and the risks for double voting (Krimmer et al. 2018).
- Estonia has multiple stakeholders, both public and private, involved in the delivery of elections (Krivonosova 2019).
- Estonia has a 15-year record of using new voting technologies, in particular Internet voting (Krivonosova et al. 2019; Serrano-Iova 2019; Vassil et al. 2016; Vinkel and Krimmer 2017).

Moreover, the Estonian electoral law and its most recent updates are publicly available. The latest

Table 1. The Problem and the Solution's Objectives

Aspect of the problem	*Objective*
Complexity of electoral laws and frequent changes	The solution will not be able to decrease the complexity of electoral laws or changes to it, but it will allow local election officials to deal with this complexity with fewer resources.
Lack of time of local election officials to deal with complicated cases during Election Day(s)	Unlike lengthy handouts, the solution leads the user "through relevant parts of the legislation only" (Smith and Schwarz 1987, 981), could be depicted in one-page format and be displayed for the common use.
Local election officials might interpret electoral laws with subjectivity and/or partisan interests in mind, which results in voters not being treated equally	The solution will aim at unifying interpretation by providing clear and easy to comprehend instructions, thus, limiting the ability of local election officials to interpret electoral laws, but not eliminating discretion. However, the solution also provides opportunities for oversight (by voters, election observers, and others), which could result in a more consistent implementation of the electoral laws.
Non-efficiency of poll workers' training and lack of institutional memory in election administration	The solution will allow new staff to learn quickly how elections are delivered and who is responsible for what, especially in the situations of emergent replacement. The solution can help to provide poll workers with more uniform training. The solution will help to "develop a shared set of organizational norms" (Suttmann-Lea 2020, 2) and "retain […] knowledge of election law and procedure from election to election" (Atkeson et al. 2014, 948).
Need for visual aids for poll workers to assist them on the Election Day. Such visual aids should: • simplify information • convey the meaning graphically • serve as a precise summary or a reminder which could be used on the Election Day Current aids for poll workers are: • lengthy • complex • not user-friendly • "virtually unusable on Election Day" (Douglas 2015, 367) because of their length and complexity.	The proposed solution: • substantially simplifies organizational processes (Walser and Schaffroth 2010); • conveys the meaning graphically: "a model simply enables the reader to visually register and comprehend all the variables and relationships among them." (Van der Waldt 2013) • leads the user "through relevant parts of the legislation only" (Smith and Schwarz 1987, 981) • serves as "a document which would act as a reference when resolving difficult cases" (Smith and Schwarz 1987, 987) and "communication base" for *all* involved actors (Becker, Rosemann, and von Uthmann 2000, 31) • deals particularly with complexities • is scalable (smaller jurisdictions with less capacity can utilize and build on BPMNs created by bigger jurisdictions) Unlike checklists or handouts, mostly designed for internal use, the visual aids such as diagrams could be printed out and displayed as posters at the polling station for all participants in the electoral process. This could boost confidence in the electoral process of both, election administrators and voters. The solution could also be applied for (post-) election audits.

version of the law presents all the amendments and changes, thus eliminating the need to navigate among older versions to discover what is still valid. Furthermore, the state itself provides the official translation of the law into English.

This article focuses on the most recent elections, the 2019 parliamentary elections in Estonia. The time frame covers the election- and post-election periods of the electoral cycle (Krimmer, Triessnig, and Volkamer 2007). Following the approach of Goldkuhl (2016), the analysis builds on a detailed legal analysis, and the researchers' previous study and experience of work procedures and principles in the field of election administration. The primary source of the data for the modelling is the Riigikogu Election Act (Riigikogu Election Act 2019). Additionally, we complemented it by on-site observations of the electoral law implementation and interviews with the electoral stakeholders, conducted in groups of at least two people from the Cost of Democratic Elections research project. The article illustrates both steps of visualization (Ciaghi, Weldemariam, and Villafiorita 2011), modelling and analysis. The mark-up of laws is conducted manually, independently by each author of the article.

The limitations of this research lie in the narrative existing in the field of public administration regarding the application of private sector approaches to public administration research. According to this discourse, business approaches might not be fully applicable to the field of public administration (Lips 2019), due to some "fundamental differences between public administration and private/ commercial organizations" (Goldkuhl 2016, 447). However, BPMN has been proven to be applicable to different fields of public administration (as presented in the previous section), including election administration (Krimmer, Duenas-Cid, and Krivonosova 2020b; Serrano-Iova 2019) and immigration law modeling (Ciaghi, Weldemariam, and Villafiorita 2011). Furthermore, the studies on election administration favor solutions derived from the private sector (Douglas 2015), because they are politically neutral and do not require reform. Combined with the low resource-intensity of this solution, BPMN as a tool can be implemented at the polling sites immediately, thus demonstrating the intrinsic value of this solution. The limitations of the proposed approach lie in the extent to which it limits the discretion of poll workers: even the most comprehensible instructions might not convince poll workers to follow them. Previous research (Atkeson et al. 2014; Suttmann-Lea 2020) established that poll workers' beliefs and perceptions of fairness might more accurately explain variations in policy implementation. Another limitation relates to using the English translation of the law (even though the official one) which means we might be missing some (cognitive-) linguistic dimensions (Goldkuhl 2016).

DESIGN OF THE SOLUTION

Step 1

The analysis starts with the *identification of the relevant legislation(s).* A thorough reading is necessary. The initial reading will permit the identification of articles that describe processes and activities, and the actors involved in the mentioned activities. It will allow classification of each article as either irrelevant or relevant for the modelling. This way of classifying articles is not final, and the modeler might consider an irrelevant article relevant (or vice versa) depending on the scope of the modelling. Nevertheless, not reducing at all the number of articles to be modelled will lead to a situation probably encountered by Krimmer et al. (2018), where individual articles of the then Municipal Council Election Act or MCEA (Municipal Council Election Act 2017) were modelled with BPMN.

The example provided by Krimmer et al. (2018), and identified as the activity "Ascertaining voting results in a Voting District Committee," corresponds in its entirety to article § 54 of the MCEA (Municipal Council Election Act 2017). The model is quite detailed in some aspects, but less in others, and quite complex as it does not follow the BPMN guidelines. This was a model for a single individual activity, while Krimmer et al. (2018) state that "31 processes with 177 activities" were identified in the almost 85 articles of the MCEA (Municipal Council Election Act 2017). Among those, they selected "four major processes" consisting "of different sets of activities depending on voting channel and voting location" (Krimmer et al. 2018, 123). The selected 37 activity models ("22 activities for I-voting, 8 activities for early and advance voting, and 7 activities for election day voting" (Krimmer et al. 2018, 123) were individually created in order to apply an accounting approach to assist in the calculation of electoral costs. This level of detail is not necessary for electoral administrators attempting to understand the sequence and responsibility of processes for an election. As such, it is recommended to identify the relevant articles necessary for the scope of the modelling.

Step 2

The next step concerns *recognizing the different voting channels* available in the elections. Voting can occur remotely or in the polling stations, before or during the Election Day, and on a paper or electronic ballot. The specific combination of these components gives rise to the different voting channels available to cast a vote. For example, Internet voting refers to casting an electronic ballot remotely before the Election Day, while postal voting is a similar endeavor with a paper ballot, and advance voting happens on paper ballots at the polling stations before the Election Day. We strongly suggest that whatever the scope of the modelling is, to model according to the various voting channels, because it will help illustrate the process, events, and actors in a manner that can take advantage of the inherent sequence and conditional flows of BPMN and its other elements. Modelling per voting channel also allows the identification of the shared activities for all channels. For example, printing of ballot papers is usually centrally organized, and only then distributed to every paper-based voting channel. Therefore, this activity happens only once per elections, however, it concerns every paper-based voting channel.

Step 3

Once the voting channels have been identified, and those desired to be modelled chosen, *the various actors and processes they perform need to be assigned to them*. Some voting channels, like those for advance, early, and postal voting, are much more focused on local election administration than others (i.e., Internet voting). Internet voting is generally managed more centrally, at a higher operational level, and might even involve the national electoral bodies. In the other cases, many of the activities and responsibilities are managed at the local level of election administration.

Taking the example of modelling one voting channel, swim lanes can be used to distinguish each relevant actor. A pool would be used to represent an election management body, team, or actor, and lanes could illustrate specific responsibilities of exceptional individuals (such as the head of a polling station that must sign an affidavit or a final report), as presented in note 1 in Figure 1.

Step 4

Once assigned, *the correct sequence of processes must be established, and they must be connected to one another*. Since electoral process management is a multi-actor endeavor, the processes of a single voting channel may involve more than one electoral administrator. This is why it is of particular importance to model carefully with the help of the electoral law. For example, at the local level a large number of activities and checks must be performed in a specific sequence. There are also multiple conditions to verify the eligibility of voters. All of these activities should be attributed to the correct actors and in the correct sequence, both legislatively and logically. For example, voter eligibility checks should occur before handing the ballot to the voter but after setting up the polling station. Additionally, and as previously mentioned, there are shared activities that are homogeneous in most or all voting channels. These must be added to the BPMN in an accurate manner that reflects what is written in the law.

All activities are illustrated as rounded rectangles. There are some activities, named sub-processes in BPMN nomenclature, that might contain a complex net of sub-activities. They can be illustrated as collapsed rounded rectangles with a “plus sign” (like in Figure 1). When the plus sign is clicked on, the rectangles will expand (like in Figure 2). When expanded they will add a greater level of detail and will contain other activities, events, and connections between them. The level of detail of the model should be established by taking into consideration the capacities of the user and the creator of the model. By having the option to show or hide some of the activities, the same model can be used at both the local and higher electoral administration levels. The activities will be connected by a solid line with an arrowhead, which shows in which order the activities are performed.

Events are situations that happen anywhere in the process, and can also be used as the starting point of a process or sub-process. The Timer, Condition, and Message Events relate to a specific time, condition, or message/item, respectively, that must be fulfilled in order for the process to start or continue. The Timer Start Event can be used when there is a time precondition in the law for a certain activity, e.g., a specific date and/or time for starting advance voting (see note 1 in Figure 1). The Message Start Event describes the receipt of an item in order to start a process, e.g., receiving the voter’s ID in order to check a voter’s eligibility, or receiving the materials to prepare the polling place (see note 1 in Figure 2). The Conditional Start Event can be used for any other precondition that might need to be fulfilled in order to initiate a process. The events can also occur during the process, and the diagrams are a bit different, depending if the actor needs to receive or send (“catch”/receive or “throw”/send) something (see note 5 in Figure 1).

Gateways are used to indicate paths that either merge or fork depending on conditions. There are Exclusive, Parallel, and Event-Based Gateways. The Exclusive Gateway can be used when there is a *decision* to be made by the actor (see note 3 in Figure 1). The Parallel one can be used when the actor must accomplish different activities that themselves are not in a sequence, as described by the law (see note 2 in Figure 2). The Event-Based Gateway is an Exclusive Gateway but the precondition is an event, not a choice nor decision (like in the Exclusive Gateway).

Consistently following the naming conventions mentioned above will guarantee the comparability

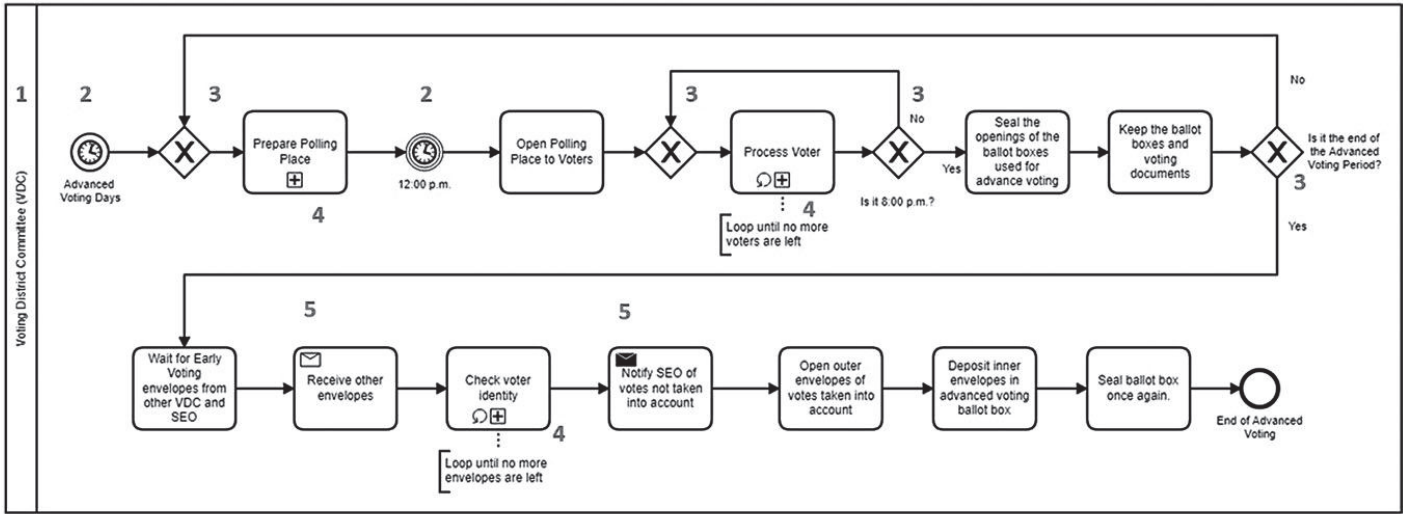

1
Voting District Committee (VDC)
2
Advanced Voting Days
3
Prepare Polling Place
4
2
12:00 p.m.
Open Polling Place to Voters
3
Process Voter
4
Loop until no more voters are left
3
No
Yes
Is it 8:00 p.m.?
Seal the openings of the ballot boxes used for advance voting
Keep the ballot boxes and voting documents
No
Is it the end of the Advanced Voting Period?
3
Yes
Wait for Early Voting envelopes from other VDC and SEO
5
Receive other envelopes
Check voter identity
4
Loop until no more envelopes are left
5
Notify SEO of votes not taken into account
Open outer envelopes of votes taken into account
Deposit inner envelopes in advanced voting ballot box
Seal ballot box once again.
End of Advanced Voting

FIG. 1. BPMN of the advanced voting delivery in the 2019 Parliamentary elections in Estonia. (1) The "pool" or exterior rectangle presents the whole process, which is attributed to the actor performing the modelled activities and sub-processes. (2) The "clock" sign illustrates when an activity depends on a specific time/deadline. The first clock starts the whole process, while the second one requires the time to be 12:00 p.m. before proceeding further. The reading for this model is following: the process starts only on advanced voting days, and the polling places open at 12:00 p.m. (3) The "cross" sign illustrates gateways in the model; either they indicate the points at which recurring activities are starting over, or where a decision must be taken (yes-no questions in this model) in order to proceed. (4) The "plus" sign illustrates a sub-process (i.e., the activity has sub-activities). In the application format, by clicking at this button, a list of sub-activities emerges. The model could be printed with or without displaying sub-activities. (5) The "envelope" sign demonstrates that the activities are dependent on receiving (white envelope) or sending (black envelope) physical artifacts. In this model, the envelopes are received and a physical notification (e.g., letter, e-mail, message, etc.) must be sent to the State Electoral Office (SEO).

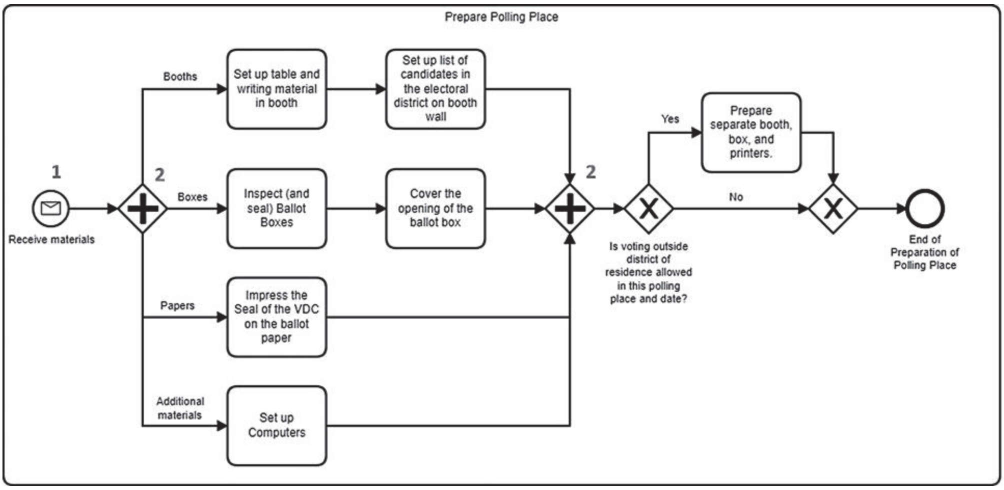

Prepare Polling Place
1
Receive materials
2
Booths
Boxes
Papers
Additional materials
Set up table and writing material in booth
Set up list of candidates in the electoral district on booth wall
Inspect (and seal) Ballot Boxes
Cover the opening of the ballot box
Impress the Seal of the VDC on the ballot paper
Set up Computers
2
Is voting outside district of residence allowed in this polling place and date?
Yes
No
Prepare separate booth, box, and printers.
End of Preparation of Polling Place

FIG. 2. Expanded sub-process "Prepare the Polling Place." (1) The "envelope" sign at the beginning illustrates when an activity depends on the reception of a specific message or item. In this model, preparing the polling place can only start after the materials have been received. (2) The "plus" diamond sign illustrates parallel gateways in the model; they indicate the starting and ending points where multiple activities should be undertaken in parallel. In order to proceed, all the parallel activities must be completed.

of models, which is one of the determinants of the quality of models (Becker, Rosemann, and von Uthmann 2000).

Step 5

Once the model is complete, *a review is necessary* to make sure that no process, component, actor, or relationship has been omitted. It is highly recommended to review the model from start to finish, with and without the law to see if something has been omitted or if something does not seem correct or logical. If, after consulting with the relevant legislation, there seem to be some incongruities, we recommend a final step.

Step 6

In the case that there are issues when modelling, lack of clarity in the electoral law, or just questions regarding to the process, *it can be complemented with observations and interviews with electoral management bodies (EMBs)*. This step could also serve as a check of the semantic correctness of a model, which "postulates that the structure and the behavior of the model is consistent with the real world" (Becker, Rosemann, and von Uthmann 2000, 32).

DEMONSTRATION: MODEL OF ADVANCE VOTING DELIVERY IN THE 2019 PARLIAMENTARY ELECTIONS IN ESTONIA

Distinct legislation regulates different levels of elections in Estonia: the Riigikogu Election Act 2019, or the Municipal Council Election Act 2019, or the European Parliament Election Act 2020, depending on the type of election being conducted, the national, local, or European Parliament elections, respectively. Even the eligibility of voters depends on the level of elections: those who are eligible to vote in local elections might not be eligible to vote in parliamentary elections. The legislation also differ in scope and designation of electoral administrators; however, most activities and processes remain similar. Besides, for every election, the central election administration prepares a handbook for poll workers. In the 2019 parliamentary elections, this handbook consisted of three parts: instructions regarding procedures at the polling station, the electoral law, and the form with checkboxes, with instructions prevailing. These instructions concerned solely the responsibility of poll workers, while the law mentions responsibilities of multiple actors. Still, the translation of the law into instructions takes more space than the law itself. Besides the handbook, poll workers in Estonia are provided training, either in person or in a digital environment.

Step 1: Identifying articles that explicitly refer to an actor involved in the management of elections and a process

The articles, irrelevant for the modelling, will be ones that describe the bases of the election system (Municipal Council Election Act 2019, para. 1; Riigikogu Election Act 2019, para. 1), specify the characteristics of individuals who are allowed to vote or participate as candidates (Municipal Council Election Act 2019, para. 5; Riigikogu Election Act 2019, para. 4), or state the competences of the electoral management bodies (Municipal Council Election Act 2019, paras. 12, 19; Riigikogu Election Act 2019, paras. 9, 15), among many others. These descriptive articles only indicate overarching characteristics of processes, rights, and obligations of individuals. These abstract concepts will not be modelled because they do not pertain to the concrete activities we are attempting to visualize.

As an example of the relevant articles, we have ones that describe the preparation for electronic voting (Riigikogu Election Act 2019, para. 48), the procedure for voting on a paper ballot (Municipal Council Election Act 2019, para. 45; Riigikogu Election Act 2019, para. 39), or ascertaining the voting results from different voting methods (Municipal Council Election Act 2019, paras. 54–55; Riigikogu Election Act 2019, paras. 57–60). These articles present a sequence of events, and/or the actors, thus concretely describing processes that must be undertaken during the elections.

Step 2: Identifying the corresponding voting channels

In the 2019 parliamentary elections in Estonia, voters could cast a vote through eight voting channels (see the Table 2). *Postal voting* was available to voters residing abroad, upon a written application submitted to the Estonian foreign mission in the country of a voter's habitual residence. The deadlines for submitting an application and returning a ballot paper were established individually by every foreign mission. *Voting in the diplomatic missions* was organized for at least two days from the 15th to the 10th day before the Election Day. *Internet voting* was available to voters on a 24-hour basis from the 10th to the 4th day before the Election Day. *Early voting in county*[4] *centers* means that the voting happened from the 10th to the 7th day before the Election Day in the designated polling stations where voters could vote irrespective of their residence. In 2019, most of such centers were located in supermarkets. *Advance voting* was organized at every polling station (county centers and ordinary Voting District Committees—VDCs), from the sixth to the fourth day before the Election Day. *Election Day voting* was available for 11 hours on Election Day at every polling station. *Home voting* happened on Election Day, on request by a voter, meaning that a part of the VDC took a mobile ballot box and the required voting materials and visited the voter at the voter's location. For the demonstration, we chose to illustrate advance voting at the polling station, due to the various local-level activities that must be undertaken, thus, active involvement of poll workers.

Table 2. Voting Channels in the 2019 Parliamentary Elections in Estonia

NN	*Voting channel*
1	Postal voting
2	Voting in the diplomatic missions
3	Internet voting
4	Early voting in county centers
5	Advance voting in county centers
6	Advance voting in ordinary polling stations
7	Election Day voting
8	Home voting

To demonstrate the concept of an activity shared by some voting channels, we consider the activity of processing the votes cast in advance. The paper ballots cast in advance of Election Day are centralized, sorted, and sent to the corresponding voting district at which a voter is registered. This activity would be shared for postal voting, voting in diplomatic missions, early, and advance voting.

Step 3: Assigning actors and processes they perform (see Step 1) to identified voting channels (see Step 2)

At the local level, the electoral management body is the VDC. Therefore, the model will have only one pool (as illustrated in Figure 1). The VDC has at least five members: the municipal council appoints

[4] A county is an administrative unit of Estonia. By law, every county should provide to voters at least one county center.

the chairperson and one half of the members, political parties appoint the other half. Therefore, election administrators in Estonia might be partisan.

Advance voting requires the VDCs to perform the following processes. The processes are presented in the sequence that they are mentioned in the electoral law (Riigikogu Election Act 2019):

- prepare polling place (Riigikogu Election Act 2019, paras. 34–37);
- seal the openings of the ballot boxes used for advance voting after the close of voting (Riigikogu Election Act 2019, para. 36);
- open polling place to voters (Riigikogu Election Act 2019, paras. 38–40);
- process voters (Riigikogu Election Act 2019, paras. 39–40);
- check voter identity (Riigikogu Election Act 2019, paras. 39–40);
- keep the ballot boxes and voting documents (Riigikogu Election Act 2019, para. 40);
- receive early voting envelopes from other VDCs and State Electoral Office (SEO) (Riigikogu Election Act 2019, para. 48);
- notify SEO of votes not taken into account (Riigikogu Election Act 2019, para. 48);
- open outer envelopes of votes taken into account (Riigikogu Election Act 2019, para. 48);
- deposit inner envelopes in advance voting ballot boxes (Riigikogu Election Act 2019, para. 48);
- seal ballot box once again (Riigikogu Election Act 2019, para. 48).

This sequence does not necessarily follow the logically correct sequence of the processes: for instance, the law mentions the process of sealing the openings of the ballot boxes before the process of opening the polling place and other processes happening during the voting. This emphasizes the importance of the BPMNs in easing the establishment of the correct sequence of electoral processes. Some of the mentioned activities also have subprocesses. Step 4 further analyzes them.

Step 4: Organizing the processes, within each identified voting channel, in the correct sequence, and connecting them to the corresponding actors with the correct relationship

Figure 1 illustrates a collapsed model of advance voting organized by the VDC. It initiates with a Timer Start Event because advance voting can only happen during specific dates. The Timer Start Event indicates that this process will only start when the Advanced Voting Day has been reached. A gateway is positioned next to catch the loop that will be explained further. Figure 1 has been streamlined, collapsing the expanded sub-processes, in order to better visualize the bigger picture. Thus, the Timer Start Event is followed by a collapsed sub-process “Prepare Polling Place.”

Figure 2 illustrates the sub-process “Prepare the Polling Place” as an expanded sub-process in order to demonstrate what happens when they undertake such activity. In order to start preparing the polling place, the VDC must receive the materials to set it up. Then, they must take each of these materials and fulfil some activities. The booths must have a table and writing materials in them, and the list of candidates must be placed on the wall of the booth. The ballot boxes must be inspected and sealed, and their openings further covered to prevent tampering. The ballots must be stamped with the VDC seal. With these activities in parallel accomplished, a choice divergence in the path appears.

The REA (Riigikogu Election Act 2019, para. 41) states that voters may vote outside their district of residence on specific dates in specific polling stations. If this is the case, such polling stations must prepare a separate booth, ballot box, and corresponding materials. Otherwise, nothing else needs to be done. This legal specification has been illustrated by the Exclusive Gateway and the corresponding sequence of activities. After any of the branches is followed, the polling place has been prepared and this sub-process ends. The model will carry onto the next activity.

After the “Prepare the Polling Place” activity, the team must “catch” an intermediate event, i.e., wait until it is 12:00 p.m. in order to “Open the Polling Place to Voters.” As the voters come in, the VDC team processes them (i.e., asking for their ID, verifying that they are eligible to vote at this polling station, handing them the ballot, stamping the ballot, and observing that the voter inserts the ballot correctly in the ballot box). This activity is compressed in Figure 1 in order to make the whole process legible. The activity is looped until there are no more voters. A gateway follows the “Process Voter” activity, and makes sure it continues until 8:00 p.m., which is the closing time of the polling station. At

8:00 p.m. the VDC team will seal the openings of the ballot boxes and keep them safe with the voting lists and documents.

The advanced voting is undertaken for a few days, so if the period has not ended, the process loops back to the beginning (i.e., the first gateway after the Timer Start Event), and the activities are repeated on the next day of the Advanced Voting Period. However, if the period has ended, then the VDC needs to fulfil other activities. They must now wait for the Early Voting Period envelopes from other VDC and, after receiving them, they must process them. The Early Voting Period envelopes contain two main pieces of information: the voter's identity on the (outer) envelope and an additional sealed (inner) envelope with the voter's ballot. The VDC team will check the voter's identity with the voting list, in order to determine if a voter was eligible to cast a vote in this polling station. If yes, the ballot envelope will be taken into account and a notation will be made in the voting list. If no, the ballot envelope will not be taken in account. Afterwards, the VDC team must notify the SEO of the votes that were not taken into account. The voter (outer) envelopes that passed the check will be opened and the (inner) envelopes containing the ballot will be inserted in the advance voting ballot box, after which the box will be sealed once again. After all of these activities, which in total have spanned the duration of a few days, the process of advance voting ends.

Step 5: Reviewing the BPMNs with the law to make sure it has been correctly translated

There are some details that are not specified by the REA (Riigikogu Election Act 2019). The activities illustrated in Figure 2 after the Parallel Gateway (with the exception of the computers) were only mentioned but not sequenced. Thus, when designing the model, it was up to the modeler to add such activities as a linear or parallel sequence of events. Since the activities are related to different kinds of materials, and knowing that the VDC contains more than one single member, the modeling was done in parallel. This reflects the reality that one polling station clerk can set up the booths while another checks and seals the boxes, and so on. Additionally, the described Exclusive Gateway had to be illustrated because the selection of which polling stations would be accepting voters coming from other electoral districts is done closer to the electoral dates and through another mechanism, not the REA (Riigikogu Election Act 2019).

Step 6: Complementing with observations and interviews where necessary or if doubts persist

Finally, the model was prepared, and on-site observations were conducted to improve it. The REA (Riigikogu Election Act 2019) does not say anything about computers or printers. However, through our observations of and interviews with VDC clerks we realized that they actually need to set up such devices and make sure that they are operational (i.e., a power and Wi-Fi source must be available to them). As such, we have decided to include such activity in the model, even though it is not explicitly mentioned in the REA (Riigikogu Election Act 2019).

DISCUSSION

The proposed approach allows translating the complexity of the electoral law into clear graphical instructions for poll workers, distilling the message spread through the multiple pages of the dense text of an electoral law into one model. Our demonstration shows how the electoral law of Estonia could be translated into one model with clear instructions. As a starting point, we had the Riigikogu Election Act (Riigikogu Election Act 2019), comprising 86 articles, covering all activities of the electoral cycle from campaigning to complaining, for all available voting channels, for all involved actors. We distilled this electoral law into one model of how one particular voting channel, advance voting, should be delivered.

The model differentiates activities by the actors performing them, thus, condensing the message even further: poll workers could see the whole picture about which other actors are responsible for advance voting implementation, but they also could concentrate only on their own responsibilities. This allows using the model for multiple purposes: for instance, for the training of new staff, a more detailed model, showing all actors and all subprocesses could be used, while for the voting day, a compressed model showing only responsibilities of a considered actor could instead be used. That could potentially decrease the perceived complexity of the electoral law and help the election administration deal with the electoral law with fewer resources. The model also explicitly shows the pre-conditions for the activities: a specific date and/or time, an item to be received, or any other condition(s) for starting an activity. Whenever applicable, the model asks yes/no questions, in order to navigate a poll worker to which scenario to proceed. This should potentially limit the ability for law interpretation. At the same time, a model does not substitute an electoral law, but serves as an additional means for cognition. Thus, a poll worker could do both: read the text of an electoral law and read a model.

BPMNs might be presented to poll workers in different forms: digital, printed, or even via an application, which might be particularly helpful for the navigation between different scenarios.

CONCLUSION

In this article, we present an artifact showing how BPMN could help to make the electoral law more comprehensible for election administrators and poll workers. BPMNs might be not so easy to create. Nevertheless, as soon as they are modelled, they could be understood and further used by a layperson. The question is who should be responsible for creating those models? Different countries and different contexts could ask for different approaches. If the aim is to decrease the discretion of the election administrators and poll workers, especially over the law interpretation, the delegation of the task of law modelling to a few trained public officials could be favored. However, it should be noted that such approach, besides bringing greater standardization, might result in greater centralization of the election administration.

Based on the argument of Ciaghi et al. (2011, 29), that "a graphical representation of a law can be of great advantage to those who want to understand or analyze it (e.g., citizens or jurists) as well as those who need to implement it," a side effect of applying BPMNs to electoral laws could be an increased understanding by the wider population of how elections are organized.

Modelling electoral laws might be particularly useful for the following environments:

- decentralized countries, where electoral procedures vary significantly between the territorial units, contributing to the confusion among voters and poll workers;
- supranational and intergovernmental entities, aimed at consolidation of electoral procedures;
- new democracies and after-conflict societies to deliver elections for the first time, or after a significant break. Firstly, the electoral process is still new to all actors involved in delivery. Therefore, they will be even more interested in having support in the form of a visualized model. Secondly, mistakes and problems with election administration in such countries could result in dramatic consequences (Laanela 1999), like electoral violence or return to a non-democratic regime;
- environments where poll workers do not follow the electoral laws consistently, hence, the society might be interested in checking whether every poll worker treats voters equally;
- international election observation missions, which need to guarantee that all election observers that they deploy to a country understand the nation's electoral processes;
- environments where the electoral processes should be reengineered due to introduction of a technology or a new voting channel, or an adjustment should happen due to some force-majeure reasons. By modelling the laws and analyzing the models, public administrators can see what actors and activities this change will affect. Such models and their analysis could help to build software requirements from the legislation, which might be particularly useful during the procurement and implementation processes;
- environments with understaffed and overtasked election administrations. Such models have potential of organizing staffing more efficiently, by clearly showing what actors are overtasked, or the delivery of which activities overlap.

Further studies might consider conducting experiments in which poll workers will be asked whether they find the benefit in having graphic process models in addition to other instructions. This could be done in three steps. First, by distributing BPMNs of the main electoral processes together with other instructions to the polling stations under the experiment. Second, by surveying poll workers under the experiment whether they utilized BPMNs on Election Day, in what situations, and whether they see room for improvement. The survey questions should also cover the aspects of a BPMN's user-friendliness and comprehensibility, in order to be able to control if the bad design affects the usability and comprehensibility of the tool. The third step would be to calculate the costs of producing such BPMNs. At the later stage, these costs could be related to the perceived usefulness of BPMNs. The study could also assess the comprehensibility of BPMNs in comparison to electoral laws and other instructions. Here, it is critical to remember that BPMNs are considered as a complementary tool, thus, while the control group will utilize the traditional instructions distributed to poll workers (checklists, diagrams, handouts), the experimental group will receive the same package, plus BPMNs. For assessing comprehensibility, one can develop a list of situations which a poll worker can encounter on Election Day, asking poll workers to describe how they would behave. The results of the two groups will be compared.

If the experiment is conducted under direct observation, researchers can also observe if poll workers refer to BPMNs when trying to find the correct behavioral strategy for each situation, or rather to the laws, handouts, or checklists. Furthermore, the proposed approach could be applied to all types of laws, not only to electoral ones. It will be particularly useful for the laws that mention many actors and processes.

REFERENCES

Adona, N., P. Gronke, P. Manson, and S. Cole. 2019. *Stewards of Democracy*. <https://democracyfund.org/wp-content/uploads/2020/06/2019_DemocracyFund_StewardsOfDemocracy.pdf> (January 18, 2021).

AIGA Design for Democracy, and Election Assistance Commission. 2016. "Top 10 Election Design Guidelines." *AIGA*, 6–8. <https://www.aiga.org/aiga/content/why-design/design-for-democracy/top-10-election-design-guidelines/> (January 13, 2021).

Alvarez, R. M., and T. E. Hall. 2008. "Building Secure and Transparent Elections through Standard Operating Procedures." *Public Administration Review* 68(5): 828–38.

Alvarez, R. M., and T. E. Hall. 2006. "Controlling Democracy: The Principal-Agent Problems in Election Administration." *Policy Studies Journal* 34(4): 491–510.

Alvarez, R. M., T. E. Hall, and L. R. Atkeson. 2009. *Auditing the Election Ecosystem*. CalTech/MIT Voting Technology Project Working Paper No. 85. <https://dspace.mit.edu/handle/1721.1/96617> (January 13, 2021).

Atkeson, L. R., Y. P. Kerevel, R. M. Alvarez, and T. E. Hall. 2014. "Who Asks for Voter Identification? Explaining Poll-Worker Discretion." *Journal of Politics* 76(4): 944–57.

Baraggia, A. 2017. "Italian Electoral Law: A Story of an Impossible Transition?" In *Election Law Journal: Rules, Politics, and Policy* 16(2): 272–79.

Barzelay, M., and F. Thompson. 2010. "Back to the Future: Making Public Administration a Design Science." *Public Administration Review* 70: s295–97.

Becker, J., M. Rosemann, and C. von Uthmann. 2000. "Guidelines of Business Process Modeling." In *Business Process Management*, eds. W. van der Aalst, J. Desel, and A. Oberweis, 30–49. Berlin: Springer.

Blais, A., L. Massicotte, and A. Yoshinaka. 2001. "Deciding Who Has the Right to Vote: A Comparative Analysis of Election Laws." *Electoral Studies* 20(1): 41–62.

Boehme-Neßler, V. 2011a. *Pictorial Law: Modern Law and the Power of Pictures*. Berlin: Springer.

Boehme-Neßler, V. 2011b. "Visual Law—The Law as Drama?" In *Pictorial Law*, 193–216. Berlin: Springer.

Brown, M., and K. Hale. 2020. "The Evolution of Professionalism in the Field of Election Administration." In *The Future of Election Administration*, eds. M. Brown, K. Hale, and B. A. King, 103–17. Cham: Springer International Publishing.

Burden, B. C., D. T. Canon, K. R. Mayer, and D. P. Moynihan. 2012. "The Effect of Administrative Burden on Bureaucratic Perception of Policies: Evidence from Election Administration." *Public Administration Review* 72(5): 741–51.

Burden, B. C., and J. Milyo. 2015. "The Quantities and Qualities of Poll Workers." *Election Law Journal: Rules, Politics, and Policy* 14(1): 38–46.

Ciaghi, A., and A. Villafiorita. 2012. "Law Modeling and BPR for Public Administration Improvement." In *Handbook of Research on E-Government in Emerging Economies: Adoption, E-Participation, and Legal Frameworks.*, eds. K.J. Bwalya and S. Zulu, 391–409. Hershey, PA: IGI Global.

Ciaghi, A., K. Weldemariam, and A. Villafiorita. 2011. "Law Modeling with Ontological Support and BPMN: A Case Study." *Cyberlaws 2011: The 2nd International Conference on Technical and Legal Aspects of the e-Society*, 29–34.

City Commissioner's Office. 2013. *Review of Provisional Ballots Cast in the 2012 Presidential Election*. Philadelphia. <https://controller.phila.gov/philadelphia-audits/butkovitz-audit-reveals-errors-mistakes-in-provisional-ballots-cast-in-philadelphias-2012-preside/>.

Corradini, F., D. Falcioni, A. Polzonetti, and B. Re. 2011. "Innovation on Public Services Using Business Process Management." In *2011 International Conference on E-Business, Management and Economics*, 25–29. Singapore: IACSIT Press.

Douglas, J. A. 2015. "A 'Checklist Manifesto' for Election Day: How to Prevent Mistakes at the Polls." *Florida State University Law Reveiw* 43: 353–398.

Election Assistance Commission, U.S. 2016. *Election Worker Successful Practices Manual*. Washington, DC: U.S. Election Assistance Commission.

European Parliament Election Act. 2020. <https://www.riigiteataja.ee/en/eli/ee/513012020006/consolide/current> (June 12, 2020).

Fedorowicz, J., and M. A. Dias. 2010. "A Decade of Design in Digital Government Research." *Government Information Quarterly* 27(1): 1–8.

Garnett, H. A., and T. S. James. 2020. "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity." *Election Law Journal: Rules, Politics, and Policy* 19(2): 111–26.

Geddis, A. C. 2005. "It's a Game That Anyone Can Play: Election Laws Around the World." *Election Law Journal: Rules, Politics, and Policy* 4(1): 57–62.

Geiger, M., S. Harrer, J. Lenhard, and G. Wirtz. 2018. "BPMN 2.0: The State of Support and Implementation." *Future Generation Computer Systems* 80: 250–62.

Goldkuhl, G. 2016. "E-Government Design Research: Towards the Policy-Ingrained IT Artifact." *Government Information Quarterly* 33(3): 444–52.

Gorín, D., S. Mera, and F. Schapachnik. 2010. "Model Checking Legal Documents." In *Frontiers in Artificial Intelligence and Applications*, JURIX 2010, 151–54.

Hale, K., and C. D. Slaton. 2008. "Building Capacity in Election Administration: Local Responses to Complexity and Interdependence." *Public Administration Review* 68(5): 839–49.

Hall, T. E., J. Q. Monson, and K. D. Patterson. 2009. "The Human Dimension of Elections." *Political Research Quarterly* 62(3): 507–22.

Hubler, K. O., and T. Patrick. 2020. "Building Terminology in the Field." In *The Future of Election Administration*, eds. M. Brown, K. Hale, and B.A. King, 155–68. Cham: Springer International Publishing.

James, T. S. 2019. "Better Workers, Better Elections? Electoral Management Body Workforces and Electoral Integrity Worldwide." *International Political Science Review* 40(3): 370–90.

Kasse, J. P., M. Moya, and W. Balunywa. 2013. "Towards an Electoral Process Reengineering Methodology." In *2013 IST-Africa Conference and Exhibition, IST-Africa 2013*, 1–8.

Kimball, D. C., and M. Kropf. 2006. "The Street-Level Bureaucrats of Elections: Selection Methods for Local Election Officials." *Review of Policy Research* 23(6): 1257–68.

Kimball, D. C., M. Kropf, and L. Battles. 2006. "Helping America Vote? Election Administration, Partisanship, and Provisional Voting in the 2004 Election." *Election Law Journal: Rules, Politics, and Policy* 5(4): 447–61.

Krimmer, R., D. Duenas-Cid, I. Krivonosova, P. Vinkel, and A. Koitmae. 2018. "How Much Does an E-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia." In *Electronic Voting*, eds. R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, and D. Duenas-Cid, 117–31. E-Vote-ID: International Joint Conference on Electronic Voting. Cham: Springer.

Krimmer, R., D. Duenas-Cid, and I. Krivonosova. 2020a. "Debate: Safeguarding Democracy during Pandemics. Social Distancing, Postal, or Internet Voting—the Good, the Bad or the Ugly?" *Public Money & Management* 41(1): 8–10.

Krimmer, R., D. Duenas-Cid, and I. Krivonosova. 2020b. "New Methodology for Calculating Cost-Efficiency of Different Ways of Voting: Is Internet Voting Cheaper?" *Public Money & Management* 41(1): 17–26.

Krimmer, R., S. Triessnig, and M. Volkamer. 2007. "The Development of Remote E-Voting around the World: A Review of Roads and Directions." In *E-Voting and Identity*, eds. A. Alkassar and M. Volkamer, 1–15. Vote-ID: International Conference on E-Voting and Identity. Bochum: Springer.

Krivonosova, I. 2019. "How Elections with Internet Voting Are Administered? The Case of the 2019 Parliamentary Elections in Estonia." In *Proceedings E-Vote-ID 2019*, 381–83. Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019. Tallinn: TalTech Press.

Krivonosova, I., R. Krimmer, D. Duenas-Cid, and R. Iova. 2019. "How Increasing Use of Internet Voting Impacts the Estonian Election Management." In *Proceedings E-Vote-ID 2019*, 226–28. Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019. Tallinn: TalTech Press.

Kropf, M., J. E. V. Pope, M. J. Shepherd, and Z. Mohr. 2020. "Making Every Vote Count: The Important Role of Managerial Capacity in Achieving Better Election Administration Outcomes." *Public Administration Review* 80(5): 733–42.

Kropf, M., T. Vercellotti, and D. C. Kimball. 2013. "Representative Bureaucracy and Partisanship: The Implementation of Election Law." *Public Administration Review* 73(2): 242–52.

Laanela, T. 1999. "Crafting Sustainable Electoral Processes in New Democracies." *Representation* 36(4): 284–93.

Levitt, J. 2012. "Election Deform: The Pursuit of Unwarranted Election Regulation." *Election Law Journal: Rules, Politics, and Policy* 11(1): 97–117.

Lips, M. 2019. *Digital Government: Managing Public Sector Reform in the Digital Era*. New York, NY: Routledge.

McCormick, C. 2020. "Election Integrity in Ensuring Accuracy." In *The Future of Election Administration*, eds. M. Brown, K. Hale, and B.A. King, 213–41. Cham: Springer International Publishing.

Mili, H.,G. Tremblay, G. B. Jaoude, É. Lefebvre, L. Elabed, and G. El Boussaidi. 2010. "Business Process Modeling Languages: Sorting through the Alphabet Soup." *ACM Computing Surveys* 43(1): article 4, 1–56.

zur Muehlen, M., D.E. Wisnosky, and J. Kindrick. 2010. "Primitives: Design Guidelines and Architecture for BPMN Models." *ACIS 2010 Proceedings*. 21st Australasian Conference on Information Systems, 32. <http://aisel.aisnet.org/acis2010/32> (January 28, 2021).

Municipal Council Election Act. 2017. <https://www.riigiteataja.ee/en/eli/ee/514112016001/consolide> (February 17, 2020).

Municipal Council Election Act. 2019. <https://www.riigiteataja.ee/en/eli/ee/502012019005/consolide> (June 12, 2020).

Nussbaumer, K. 2013. "The Election Law Connection and U.S. Federalism." *Publius* 43(3): 392–427.

Olbrich, S., and C. Simon. 2008. "Process Modelling towards E-Government—Visualisation and Semantic Modelling of

Legal Regulations as Executable Process Sets." *Electronic Journal of e-Government* 6(1): 43–54.

OMG - Object Management Group. 2011. "Business Process Model and Notation (BPMN) - Version 2.0." <https://www.omg.org/spec/BPMN/2.0/PDF> (November 23, 2020).

Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights (OSCE/ODIHR). 2018. "Italy, Parliamentary Elections, 4 March 2018." *OSCE.org*. <https://www.osce.org/odihr/elections/italy/369101> (March 24, 2021).

Pal, M. 2017. "Three Narratives About Canadian Election Law." *Election Law Journal: Rules, Politics, and Policy* 16(2): 255–62.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. 2007. "A Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems* 24(3): 45–77.

Riigikogu Election Act. 2019. <https://www.riigiteataja.ee/en/eli/ee/502012019007/consolide> (June 12, 2020).

Rojo, M. G., E. Rolón, L. Calahorra, F. Ó. García, R. P. Sánchez, F. Ruiz, N. Ballester, et al. 2008. "Implementation of the Business Process Modelling Notation (BPMN) in the Modelling of Anatomic Pathology Processes." *Diagnostic Pathology* 3: S22.

Romme, G., and A. Meijer. 2020. "Applying Design Science in Public Policy and Administration Research." *Policy and Politics* 48(1): 149–165.

Serrano-Iova, R. 2019. "I-Voting Costs: A Case Study of the 2019 Estonian Parliamentary Elections." TalTech. <https://digikogu.taltech.ee/en/Item/f673aea3-2901-486a-8dab-f59d69cce03e>

Siena, A., J. Mylopoulos, A. Perini, and A. Susi. 2008. "From Laws to Requirements." *RELAW '08: Proceedings of the 2008 Requirements Engineering and Law*, Barcelona, Spain, 6–10. <https://doi.org/10.1109/RELAW.2008.6> (March 9, 2020).

Smith, P. H., and V. Schwarz. 1987. "Logical Analysis of Legislation Using Flow Diagrams." *Journal of the Operational Research Society* 38(10): 981–87.

Stein, R. M. 2015. "Election Administration During Natural Disasters and Emergencies: Hurricane Sandy and the 2012 Election." *Election Law Journal: Rules, Politics, and Policy* 14(1): 66–73.

Suttmann-Lea, M. 2020. "Poll Worker Decision Making at the American Ballot Box." *American Politics Research* 48(6): 714–718.

Vassil, K., M. Solvak, P. Vinkel, A. H. Trechsel, and R. M. Alvarez. 2016. "The Diffusion of Internet Voting. Usage Patterns of Internet Voting in Estonia between 2005 and 2015." *Government Information Quarterly* 33(3): 453–59.

Venice Commission. 2002. *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report*. <https://rm.coe.int/090000168092af01> (March 11, 2020).

Villanova University. 2020. "Governments Using BPM to Increase Process Efficiencies." *Villanova University*. <https://www.villanovau.com/resources/bpm/bpm-use-in-government/> (January 28, 2021).

Vinkel, P., and R. Krimmer. 2017. "The How and Why to Internet Voting an Attempt to Explain E-Stonia." In *Electronic Voting*, eds. R. Krimmer, M. Volkamer, J. Barrat, J. Benaloh, N. Goodman, P. Y. A. Ryan, and V. Teague, 178–91. E-Vote-ID 2016: First International Joint Conference on Electronic Voting. Cham: Springer Verlag.

Van der Waldt, G. 2013. "Towards a Typology of Models in Public Administration and Management as Field of Scientific Inquiry." *African Journal of Public Affairs* 6(3): 38–56.

Walser, K., and M. Schaffroth. 2010. "BPM and BPMN as Integrating Concepts in EGovernment—The Swiss EGovernment BPM Ecosystem." In *Subject-Oriented Business Process Management*, eds. A. Fleischmann, W. Schmidt, R. Singer, and D. Seese, 106–20. Second International Conference, S-BPM ONE 2010.

Yin, R. K. 2017. *Case Study Research and Applications: Design and Methods*. Thouand Oaks, CA: SAGE Publications.

Address correspondence to:
Iuliia Krivonosova
DigiGov Lab
Ragnar Nurkse Department
of Innovation and Governance
Tallinn University of Technology
Akadeemia tee 3
12618 Tallinn
Estonia

E-mail: iuliia.krivonosova@taltech.ee

Received for publication June 14, 2020; received in revised form March 24, 2021; accepted April 2, 2021; published online July 16, 2021.

Appendix 3

Publication III
Serrano-Iova, R.A. & Watashiba, T. (2023). NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation. In: *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023*, Vol. 22(1), pp. 420–428. Andreatos, A. & Douligeris, C. (Eds.). ACI: UK. doi:10.34190/eccws.22.1.1168. ETIS 3.1.

NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation

Radu Antonio Serrano Iova[1] and Tomoe Watashiba[2]

[1]Ragnar Nurkse Department, School of Business and Governance, Tallinn University of Technology, Tallinn, Estonia

[2]School of Governance, Law and Society, Tallinn University, Tallinn, Estonia

raduantonio.serranoiova@taltech.ee
tomoetw@tlu.ee

Abstract: The ubiquity of ICT and the increase in cyber threats have pushed countries to view cybersecurity from a national perspective and draft appropriate national strategies on the topic. While containing similar terminology, these strategies are tailored to the national contexts and hence, differ across regions, cultures, and political contexts. Previous research of these documents has been focused on comparative analysis of countries that can either be considered well developed on this topic or for specific subtopics of cybersecurity. However, some of the subtopics have not been addressed, only now having become more prevalent due to current international conflicts and national / regional socio-political scuffles that have spilled into cyberspace. In our paper, we investigate all countries that have published a National Cyber Security Strategy - NCSS - (or any similar document under a different nomenclature, e.g., policy, decree, etc.), specifically in reference to their position on war, neutrality, and international cooperation. Countries maintaining an NCSS will first be identified using international databases, upon which further study of the aforementioned topics in the NCSSs will occur. We hypothesize, that while international cooperation will be present in most, if not all NCSSs, armed conflicts and neutrality will not be addressed at all nor in depth, in those that contain any reference to them. The resulting paper will present a near-global case study of these topics, which can then signify potential areas of improvement, capacity building, and strengthening of democratic coalitions, globally.

Keywords: National Cyber Security Strategy, International Cooperation, Neutrality, Conflicts, Cyberspace

1. Introduction

Russia's latest invasion of Ukraine was not only undertaken through physical means. Since 2014, the latter has been on the receiving end of targeted cyber attacks which only increased during the invasion. Satellite networks, border checkpoints, telecommunication service providers, banks, power stations, governmental services, and even non-governmental, charity, and aid organizations, among others, were attacked in the first two months of the conflict (Przetacznik and Tarpova 2022). Additionally, in 2022 only, Andorra, Australia, Bahrain, China, Costa Rica, Ethiopia, most EU countries (and its own Commission), India, Iran, Jordan, the Marshall Islands, Mexico, Pakistan, the U.K., the U.S.A., Vanuatu, and many other countries, have been targets (and sometimes even perpetrators) of cyber-attacks. Not even international humanitarian organizations, such as the International Committee of the Red Cross, have been exempted from such aggressions (CSIS no date).

These examples and the ubiquity of ICT have resulted in countries publishing their own National Cyber Security Strategies (NCSSs), or similar documents. Although these documents differ in their formatting characteristics, they all present their nation's official position on the issue of cybersecurity. Because of the invasion and the never-ending number of cyber-attacks, we decided to investigate all the countries' references on war, neutrality and international cooperation in these documents. We hypothesize that very few United Nations' (U.N.'s) members have declared their cybersecurity actions during war nor discussed neutrality in any way in their current NCSS. Moreover, we believe that all NCSSs will talk about international cooperation, given the borderless nature of cyberspace, and that countries will reference their allied preferences. This resulting paper will serve as a snapshot of the topics, allowing individual countries to improve themselves and their bi- and multilateral endeavors.

2. Strategy, topics and previous studies

Prior to anything, the concept of a National Cyber Security Strategy (NCSS), or similar document, should be defined. Traditionally, "[a] *strategy of a business forms a comprehensive master approach that states how the business will achieve its mission and objectives"* (Wheelen et al. 2017, p.50). Transposed to the public sector and scaled up to a larger context, a national strategy is *"the identification of national interests and ambitions and the use of various resources (national and other) to preserve or pursue those interests and ambitions"* (Cornish, Lindey-French and Yorke 2011). Framed more specifically toward the notion of the security of a country, it becomes then a national security strategy. These documents are usually addressed to "*adversaries or potential* *enemies*" (Drew and Snow 1988, p.48). However, by being public, in addition to serving as possible intimidation to an enemy, they might serve political purposes such as influencing public opinion, swaying specific constituencies (Caudle 2009), and even communicating with existing and potential allies, or non-aligned stakeholders. The cyberspace has become part of national security, as evidenced by multiple writings (e.g. Reveron 2012; Yannakogeorgos and Lowther 2016; Libicki 2018) throughout the years. Therefore, an NCSS is a document that identifies interests and ambitions related to national cybersecurity and communicates the use of resources to reach those goals.

Like national security strategy, an NCSS can "*vary widely in length, format and complexity*" (DuMont 2019), from country to country. Given that language, year of publication, and national contexts differ across the world's NCSSs, this variety can easily affect the title and contents of the document. However, as the logical offshoot of the former, some of an NCSS' characteristics are handed down. Some of these, compiled by DuMont (2019) include: having an endorsement by the governmental leader, reflecting national values, articulating national interests, declaring a strategic vision, identifying and assessing future challenges, and containing risk assessments, resources overviews, timeframes effectiveness measurements and implementation guidance. Therefore, a high-level document that presents most, if not all, of these elements would be considered as an NCSS and studied as one of its peers. Some outlier variations have been named 'national policy' or 'national doctrine'

Another variable that might have also affected the selection process is the 'cyber security' term. Sidestepping the linguistical connotations of having it in a single word, or not, some documents are titled using the terms information security, digital security, and Information and Communications Technology (ICT) security. While these were sporadic cases, and some even due to their translation into English or original date of publication, we have taken them all as synonyms. Von Solms and Van Niekerk's (2013) position on two of those terms (even though they acknowledge that cyber security and information security are often used interchangeably) could shed additional light for those inquiring about the similarities and differences in terminology. Nevertheless, it is within this variety of terminology and contexts that we felt that a global study was necessary to discover and present the countries' positions on the topic of warfare, neutrality, and cooperation.

2.1 Warfare / War/ Conflict

According to Merriam-Webster's dictionary, 'warfare' is defined as "*military operations between enemies (hostilities, war),*" also meaning "*an activity undertaken by a political unit (such as a nation) to weaken or destroy another.*" (Merriam-Webster no date) Oppenheim's International Law similarly defines war as "*a contention between two or more states, through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases*" (Lauterpach 1952, p.220). In understanding the use of 'warfare' or 'war' in our analysis, we have followed these general definitions, essentially understanding war or warfare as a hostile operation between two or more parties, usually involving extensive employment of forces aimed at countering the other(s). Conflict is a state where friction exists between parties, diplomatically, economically, politically, militarily and/or otherwise; yet to treat some conflicts as 'war' for states has significant legal implications and consequences, such as the application of the law of war and the law of neutrality, suspension of non-hostile relations (e.g. trade, diplomatic, treaty relations) between the belligerents, as well as the prohibition of the Use of Force under Article 2(4) of the U.N. Charter (Greenwood 1987). Therefore, in a factual sense, States avoid using 'state of war,' yet often, in the colloquial use of the terms, 'war', 'warfare' or 'conflict' are used more or less interchangeably. In this analysis, we, therefore, have followed the interchangeable usage of these three words.

2.2 Neutrality

In this analysis, the word 'neutrality' has been identified from two different angles, one from the law of neutrality as defined in the International Humanitarian Law (IHL) and the other from the internet/technological neutrality. The law of neutrality, when applied in cyberspace, entails duties such as abstention/non-participation, better expressed as "*…abstain*[ing] *from committing any acts of kinetic or cyber hostility against belligerents and providing them with military assistance, such as the provision of cyber weaponry or the recruitment of a cyber "corps of combatants"…"* or prevention, meaning *"…neither allow nor tolerate certain types of malicious activities on its territory and infrastructure…*" as well as the maintenance of impartiality, "*…apply[ing] every restricting measure and prohibition in the context of its neutral duties and rights in a non-discriminatory manner toward all belligerents.*" (Cordey and Kohler 2021, p.1). There are other elements, including the respect for a neutral state's territorial integrity and the ban of cyber operations against/from/through neutral nations, particularly for a belligerent country, with both neutral and belligerent states to be taken into account. The law of neutrality's applicability is confined to international armed conflicts (IAC) as defined in IHL and state actors.

Internet / technological neutrality is another aspect of neutrality that is relevant to this analysis, and it is generally understood to mean that Internet Service Providers (ISPs) ensure 'neutrality' in the flow of the internet traffic, treating equally, the contents that pass through their cables, cellular towers, satellites and other core infrastructures (Wu 2003), and "[w]*hen providing internet access services, providers of those services should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment*" (European Union 2015, Preamble (8)).

2.3 International Cooperation

In this analysis, we have approached the term 'international cooperation' from the perspectives of both development assistance with a closer connotation to capacity-building and part of confidence-building measures where information and intelligence sharing may be conducted between/among countries. The capacity-building, in general term, is defined by the U.N. as "*the process of developing and strengthening the skills, instincts, abilities, processes and resources that organizations and communities need to survive, adapt, and thrive in a fast-changing world*" (U.N. no date) and in a more specific case of 'cyber capacity-building,' we have followed the meaning of assistance or cooperation to "*strengthen a country's legal, technical, and policy capability, and protect against malicious cyber activity*" (Naylor, Painter and Hakmeh 2022). Confidence-Building Measures (CBMs) are considered to be "*a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation*" and they "*achieve this by establishing practical measures and processes for (preventive) crisis management between States.*" (Ziolkowski 2013, p.5). In the cyberspace context, CBMs could include sharing, providing, and exchanging information about cyber threats and vulnerabilities as well as best practices, facilitating communications through voluntary mechanisms such as the meeting of experts, provision of contact data, sharing of information through workshops, etc., at international and regional levels.

2.4 Past studies

Previous studies regarding NCSSs have compared EU and NATO cybersecurity strategies to national cyber security strategies (Štitilis, Pakutinskas and Malinauskaitė2017), attempted to discover governance trends (Shackelford and Kastelic 2014) and even present correlations between NCSS development to that of a digital economy (Teoh and Mahmood 2017). Other studies, for example, have focused on a comparative contents analysis of NCSSs of selected countries, often considered to be more 'advanced' or 'elaborate,' to identify differences and similarities, and to draw conclusions on recommended approaches and contents to be potentially considered by policymakers (OECD 2012; Luiijf, Besseling and Graaf 2013; Newmeyer 2015; Sabillon, Cavaller and Cano 2016; Shafqat and Masood 2016). In a similar vein, an attempt to utilize the quantitative analytical tool (e.g., Latent Dirichlet Allocation) for more comprehensive and automated analysis and understanding of texts has also been conducted (Kolini and Janczewski 2017), as well as more in-depth country-specific investigations (for example, see Daricili and Özdal 2018; Hurel 2020; Beecroft 2021).

3. Methodology

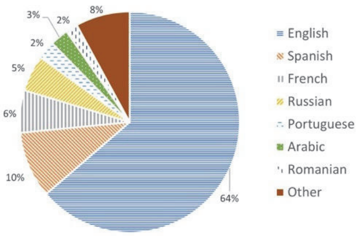
The methodology used for this article involved the systematic collection and synthesis of existing information, i.e. literature review. A literature review is a great way to summarize findings to uncover areas where research (Snyder 2019) or improvements are needed. As described by Snyder (2019), the aim of a systematic review allows for the identification of all evidence that fits a criterion to answer a particular question or hypothesis.

Out of the 193 member states of the United Nations, this study was conducted on the states that had publicly available National Cyber Security Strategies or similarly high-level national documents on the topic, in December 2022 and early January 2023. Identification of these states was conducted mainly through the eGA's National Cyber Security Index (available at https://ncsi.ega.ee/) and UNIDIR's Cyber Policy Portal (available at: https://cyberpolicyportal.org/). The former is *"… a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents …"* and *"… also a database with publicly available evidence materials and a tool for national cyber security capacity building."* (eGA no date) The latter is *"an interactive map of the global cyber policy landscape. It provides profiles of the cyber policies of all 193 UN Member States…"* and *"… seeks to support informed participation by relevant stakeholders in all policy processes* *and promote trust, transparency, and cooperation in cyberspace."* (UNIDIR no date) The benefit of these tools is that they provide direct links to official third-party websites that might contain the NCSS or similar document. The NCSS, of every country that had one, was checked to verify that it was an official document (i.e., published by official sources, the government of that country) and that it was the current version. For this latter characteristic, even if a NCSS had an expiry date, it would still be considered the current one if it was still publicly present in a governmental website and if no other NCSS had been published. For example, there was a nation that had a previous version of their NCSS in English, but the current one was only found in their official language. In this case, the one in the official language was the current official document.

After all corresponding NCSSs were identified, they were individually searched on the three proposed topics: warfare, neutrality and international cooperation. The keywords used were 'war', 'warfare', 'conflict', for the first topic, 'neutrality', 'neutral', for the second one, and 'cooperation', 'collaboration' in the international context, for the third one, with the corresponding terms in other languages. Their presence was noted, grouped, and analyzed further, as presented in the next section. For a more compact presentation of the results, the countries presented in the subsequent section have been noted using the ISO 3166-1 alpha-3 country codes, in the alphabetical order of their full names. The ISO 3166 standard can be found at: https://www.iso.org/iso-3166-country-codes.html

4. Results

In the end, 113 (out of the 194) U.N. member states had publicly accessible current NCSS, or a similar high-level document. Most NCSSs were presented in their national languages, but they also had a version in English, which allowed for an easier execution the topic search. After English, the NCSSs were found to be drafted in Spanish, French, Russian, Portuguese, Arabic and Romanian, with the remaining ones each in a different language (see



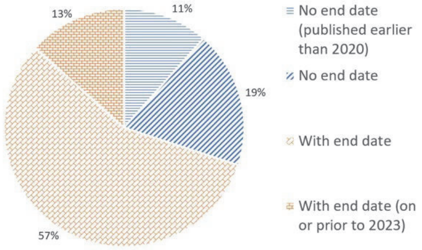
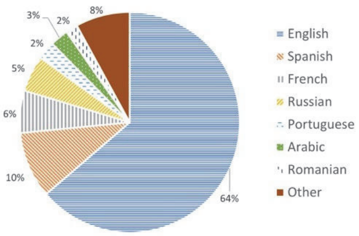


Figure 1 Language availability of the NCSSs Figure 2 NCSSs with and without end dates). While there is no obligation to publish an NCSS in English or any alternate language, the majority of the countries have done so, with some even specifying that the translation is a courtesy and should any discrepancies arise, the NCSS in their national language shall prevail.

The large majority of the NCSSs have been established for a definite period of time, i.e., 79 of them contain an end date. However, 15 of them have an end date of 2023 or prior, meaning that they are close to or already expired. The remaining 34 NCSSs do not have an end date, out of which 13 have been published prior to 2020, with the oldest entry dating back to 2003, followed by 2011.



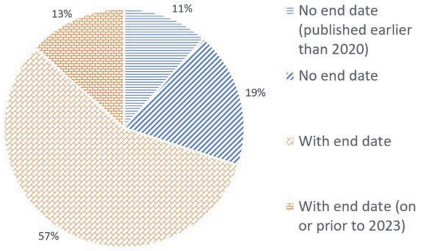
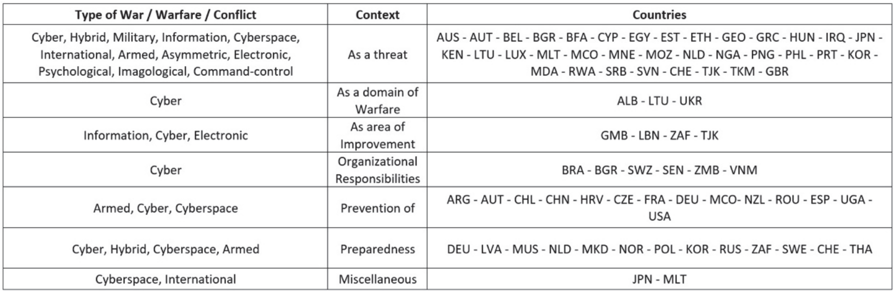


Figure 1 Language availability of the NCSSs **Figure 2 NCSSs with and without end dates**

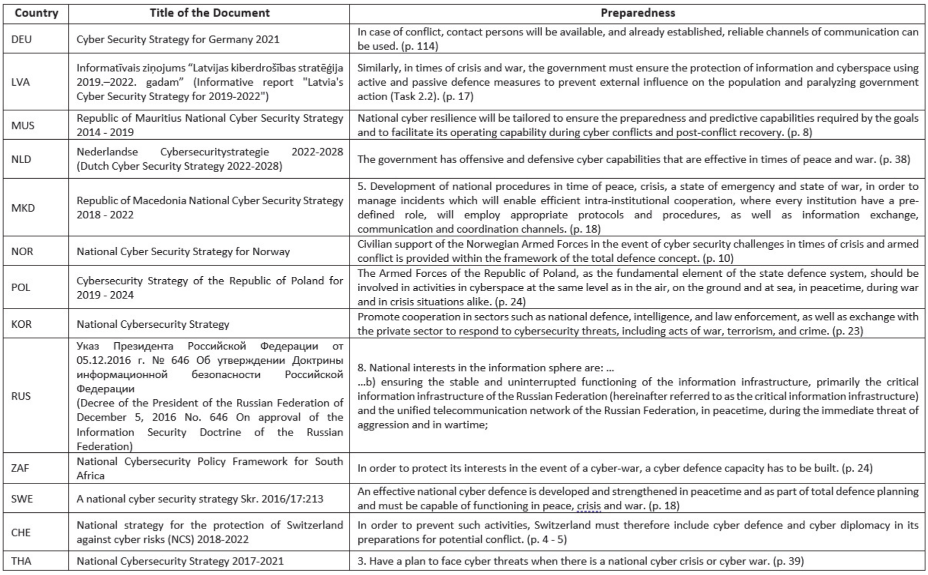
On the topic of warfare, 66 of the NCSS mention the terms 'war', 'warfare', 'conflict' and their types, in multiple lines of context, sometimes more than once in a single document (Figure 3). More than half of them allude to war / conflict, or a specific type thereof, as a threat to the nation, and in most cases in the sections describing the current situation of the country or the reasons behind the creation of the NCSS. As presented in Figure 3, in this context, we have the highest variety of descriptors referencing different types of warfare or conflict. The second most common context was regarding the prevention of war or conflicts. Similarly, there was not much specificity, with the common trend being the need to prevent such armed or cyber actions. Next, we have thirteen nations that talk about their preparations for or existing preparedness in case cyber, hybrid, armed or cyberspace warfare. These will be discussed in more detail in upcoming paragraphs describing Figure 4. In the less mentioned contexts, six countries clearly state the entity / organization responsible for cyber warfare, while four of them outright express that it is an area of improvement for their state, and three others declare that the cyberspace is a domain of warfare. Finally, in the miscellaneous context we have both Japan and Malta, since the former alludes to the necessity of international collaboration, while the latter that it would work to establish its own national position.



Type of War / Warfare / Conflict	Context	Countries
Cyber, Hybrid, Military, Information, Cyberspace, International, Armed, Asymmetric, Electronic, Psychological, Imagological, Command-control	As a threat	AUS - AUT - BEL - BGR - BFA - CYP - EGY - EST - ETH - GEO - GRC - HUN - IRQ - JPN - KEN - LTU - LUX - MLT - MCO - MNE - MOZ - NLD - NGA - PNG - PHL - PRT - KOR - MDA - RWA - SRB - SVN - CHE - TJK - TKM - GBR
Cyber	As a domain of Warfare	ALB - LTU - UKR
Information, Cyber, Electronic	As area of Improvement	GMB - LBN - ZAF - TJK
Cyber	Organizational Responsibilities	BRA - BGR - SWZ - SEN - ZMB - VNM
Armed, Cyber, Cyberspace	Prevention of	ARG - AUT - CHL - CHN - HRV - CZE - FRA - DEU - MCO- NZL - ROU - ESP - UGA - USA
Cyber, Hybrid, Cyberspace, Armed	Preparedness	DEU - LVA - MUS - NLD - MKD - NOR - POL - KOR - RUS - ZAF - SWE - CHE - THA
Cyberspace, International	Miscellaneous	JPN - MLT

Figure 3 Mentions of war / warfare / conflict in 66 NCSSs

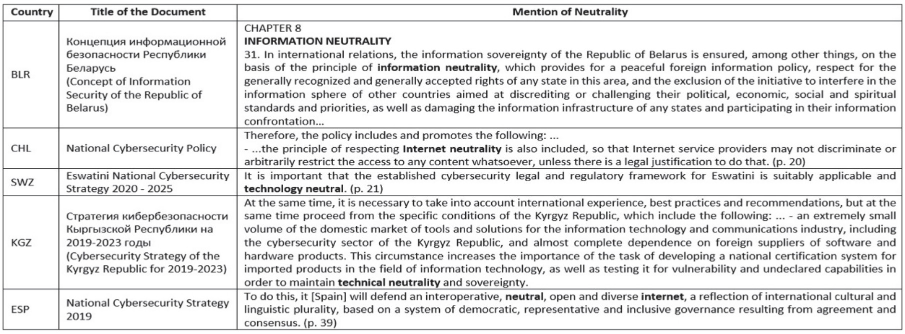
Figure 4 presents the 13 countries that reference their preparations and preparedness for or during times of war. Most of them allude to existing capabilities, albeit in extremely short descriptions, while a few of them state that they will or must prepare such capabilities. There is no other presential common trend apart from the fact that a majority of these NCSS are currently outside their ending date.



Country	Title of the Document	Preparedness
DEU	Cyber Security Strategy for Germany 2021	In case of conflict, contact persons will be available, and already established, reliable channels of communication can be used. (p. 114)
LVA	Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam" (Informative report "Latvia's Cyber Security Strategy for 2019-2022")	Similarly, in times of crisis and war, the government must ensure the protection of information and cyberspace using active and passive defence measures to prevent external influence on the population and paralyzing government action (Task 2.2). (p. 17)
MUS	Republic of Mauritius National Cyber Security Strategy 2014 - 2019	National cyber resilience will be tailored to ensure the preparedness and predictive capabilities required by the goals and to facilitate its operating capability during cyber conflicts and post-conflict recovery. (p. 8)
NLD	Nederlandse Cybersecuritystrategie 2022-2028 (Dutch Cyber Security Strategy 2022-2028)	The government has offensive and defensive cyber capabilities that are effective in times of peace and war. (p. 38)
MKD	Republic of Macedonia National Cyber Security Strategy 2018 - 2022	5. Development of national procedures in time of peace, crisis, a state of emergency and state of war, in order to manage incidents which will enable efficient intra-institutional cooperation, where every institution have a pre-defined role, will employ appropriate protocols and procedures, as well as information exchange, communication and coordination channels. (p. 18)
NOR	National Cyber Security Strategy for Norway	Civilian support of the Norwegian Armed Forces in the event of cyber security challenges in times of crisis and armed conflict is provided within the framework of the total defence concept. (p. 10)
POL	Cybersecurity Strategy of the Republic of Poland for 2019 - 2024	The Armed Forces of the Republic of Poland, as the fundamental element of the state defence system, should be involved in activities in cyberspace at the same level as in the air, on the ground and at sea, in peacetime, during war and in crisis situations alike. (p. 24)
KOR	National Cybersecurity Strategy	Promote cooperation in sectors such as national defence, intelligence, and law enforcement, as well as exchange with the private sector to respond to cybersecurity threats, including acts of war, terrorism, and crime. (p. 23)
RUS	Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации (Decree of the President of the Russian Federation of December 5, 2016 No. 646 On approval of the Information Security Doctrine of the Russian Federation)	8. National interests in the information sphere are: ... ...b) ensuring the stable and uninterrupted functioning of the information infrastructure, primarily the critical information infrastructure of the Russian Federation (hereinafter referred to as the critical information infrastructure) and the unified telecommunication network of the Russian Federation, in peacetime, during the immediate threat of aggression and in wartime;
ZAF	National Cybersecurity Policy Framework for South Africa	In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. (p. 24)
SWE	A national cyber security strategy Skr. 2016/17:213	An effective national cyber defence is developed and strengthened in peacetime and as part of total defence planning and must be capable of functioning in peace, crisis and war. (p. 18)
CHE	National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022	In order to prevent such activities, Switzerland must therefore include cyber defence and cyber diplomacy in its preparations for potential conflict. (p. 4 - 5)
THA	National Cybersecurity Strategy 2017-2021	3. Have a plan to face cyber threats when there is a national cyber crisis or cyber war. (p. 39)

Figure 4 Preparedness in case of war / warfare / conflict

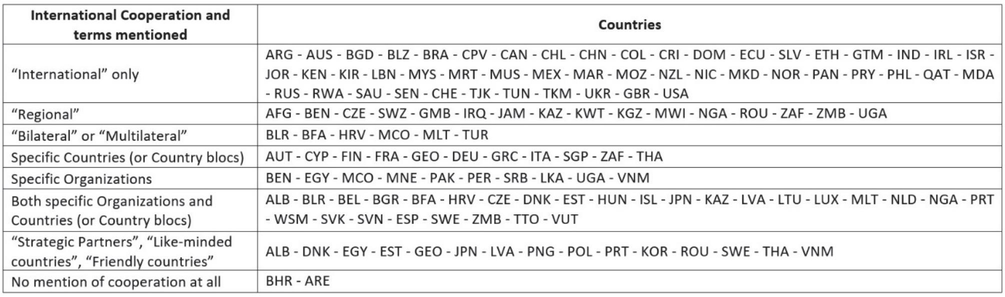
Out of the 133 NCSS, only five countries reference the concept of neutrality in their documents. Two of them refer to Internet neutrality, two others to technical/technological neutrality, and the last one to Information neutrality (Figure 5). No other NCSS explores the any neutrality concepts, associated or not, with cybersecurity.



Country	Title of the Document	Mention of Neutrality
BLR	Концепция информационной безопасности Республики Беларусь (Concept of Information Security of the Republic of Belarus)	CHAPTER 8 **INFORMATION NEUTRALITY** 31. In international relations, the information sovereignty of the Republic of Belarus is ensured, among other things, on the basis of the principle of **information neutrality**, which provides for a peaceful foreign information policy, respect for the generally recognized and generally accepted rights of any state in this area, and the exclusion of the initiative to interfere in the information sphere of other countries aimed at discrediting or challenging their political, economic, social and spiritual standards and priorities, as well as damaging the information infrastructure of any states and participating in their information confrontation...
CHL	National Cybersecurity Policy	Therefore, the policy includes and promotes the following: ... - ...the principle of respecting **Internet neutrality** is also included, so that Internet service providers may not discriminate or arbitrarily restrict the access to any content whatsoever, unless there is a legal justification to do that. (p. 20)
SWZ	Eswatini National Cybersecurity Strategy 2020 - 2025	It is important that the established cybersecurity legal and regulatory framework for Eswatini is suitably applicable and **technology neutral**. (p. 21)
KGZ	Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы (Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023)	At the same time, it is necessary to take into account international experience, best practices and recommendations, but at the same time proceed from the specific conditions of the Kyrgyz Republic, which include the following: ... - an extremely small volume of the domestic market of tools and solutions for the information technology and communications industry, including the cybersecurity sector of the Kyrgyz Republic, and almost complete dependence on foreign suppliers of software and hardware products. This circumstance increases the importance of the task of developing a national certification system for imported products in the field of information technology, as well as testing it for vulnerability and undeclared capabilities in order to maintain **technical neutrality** and sovereignty.
ESP	National Cybersecurity Strategy 2019	To do this, it [Spain] will defend an interoperative, **neutral**, open and diverse **internet**, a reflection of international cultural and linguistic plurality, based on a system of democratic, representative and inclusive governance resulting from agreement and consensus. (p. 39)

Figure 5 Mentions of neutrality in only 5 NCSSs

International cooperation was discussed in all the NCSS, apart from two countries. Forty-nine countries only mentioned international cooperation as general as possible, with the rest being a bit more specific and presenting a mixture of mentions ranging from 'regional', 'bilateral' and 'multilateral' to specific countries, country blocs and/or organisations. Additionally, fifteen nations used non-binding terminology such as 'strategic (foreign) partners', 'like-minded countries', 'friendly countries', 'strategic allied countries', 'ally/allies', 'similar thinking countries', 'partners abroad', 'international partners' (Figure 6). Two outlier cases used a different approach for noncommittal terms for international cooperation; the Russian Federation, which mentioned 'interested parties' and Brazil, declaring 'the largest possible number of countries'. The most mentioned country bloc was the EU, with appearances in twenty-six individual NCSS, and the most mentioned organizations were the NATO, the UN and the OSCE, with eighteen, sixteen and thirteen mentions respectively.



International Cooperation and terms mentioned	Countries
"International" only	ARG - AUS - BGD - BLZ - BRA - CPV - CAN - CHL - CHN - COL - CRI - DOM - ECU - SLV - ETH - GTM - IND - IRL - ISR - JOR - KEN - KIR - LBN - MYS - MRT - MUS - MEX - MAR - MOZ - NZL - NIC - MKD - NOR - PAN - PRY - PHL - QAT - MDA - RUS - RWA - SAU - SEN - CHE - TJK - TUN - TKM - UKR - GBR - USA
"Regional"	AFG - BEN - CZE - SWZ - GMB - IRQ - JAM - KAZ - KWT - KGZ - MWI - NGA - ROU - ZAF - ZMB - UGA
"Bilateral" or "Multilateral"	BLR - BFA - HRV - MCO - MLT - TUR
Specific Countries (or Country blocs)	AUT - CYP - FIN - FRA - GEO - DEU - GRC - ITA - SGP - ZAF - THA
Specific Organizations	BEN - EGY - MCO - MNE - PAK - PER - SRB - LKA - UGA - VNM
Both specific Organizations and Countries (or Country blocs)	ALB - BLR - BEL - BGR - BFA - HRV - CZE - DNK - EST - HUN - ISL - JPN - KAZ - LVA - LTU - LUX - MLT - NLD - NGA - PRT - WSM - SVK - SVN - ESP - SWE - ZMB - TTO - VUT
"Strategic Partners", "Like-minded countries", "Friendly countries"	ALB - DNK - EGY - EST - GEO - JPN - LVA - PNG - POL - PRT - KOR - ROU - SWE - THA - VNM
No mention of cooperation at all	BHR - ARE

Figure 6 International Cooperation expressed in NCSSs

5. Discussion

Overall, we found that the fact that 113 (out of the 194) member states have publicly accessible NCSS shows higher interest and need for this or similar types of policy documents for member states. Given the evolving nature of technology and its effect on the government and citizens, having an effective cyber security strategy for the operation and protection of national assets, including its infrastructure and people, has become one of the key national strategic issues to address at all levels of society. As NCSSs serve to define a vision for national cyber security and, sometimes, the implementation policies and plans for all stakeholders concerned, with significant implications for coordination of both technical and personnel resources within a given timeframe, it is commendable that the majorities of member states have fresh NCSSs with a definite period of time. With most of the dates being very recent, we can say that the formulation of NCSS is a recent, up-to-date phenomenon.

Also, with a sheer number of publicly available NCSSs and oftentimes with their translations in major languages, we see that one of their purposes is of an international nature, that is, to communicate how states perceive and act in terms of cyber affairs, particularly to other states – 'like-minded' or not. Therefore, in addition to domestic coordination and resource mobilization purposes, the critical aspect of NCSSs and their publication is sharing of the nations' positions and views about cyberspace governance with foreign policy implications, and our analysis of the three key aspects ('war', 'warfare', 'conflict'/ 'neutrality', 'neutral'/ 'cooperation', 'collaboration' in the international context) has given valuable comparative insight as to states' positions and views about these aspects.

In terms of ‘war’, ‘warfare’, and ‘conflict’, it is recognizable from the analysis that we could almost say that it is a common understanding among most states that the threat in cyberspace from foreign states or non-state actors is potentially at the scale and scope of ‘war’, ‘warfare’ or ‘conflict’. And from this rather collective use of ‘war’, ‘warfare’, and ‘conflict’ in the analysis, we understood that the inference might be made in terms of why the overwhelming number of NCSSs includes the term ‘international cooperation’ in varieties of contexts. One way of averting such a threat of ‘war’, ‘warfare’, and ‘conflict’ is through, for example, helping to eliminate ‘safe heavens,’ in the interconnected and transborder nature of cyberspace – filling the gap where potential loopholes exist for malicious exploitation of cyber vulnerabilities in other states by extending capacity-building assistance – and by establishing CBMs for more enhanced and organized information sharing. Thus, we understood that states see the merit of international cooperation as the mitigation of potential risks for their peace and security, both domestically and internationally, and have placed the importance, which is reflected in the number of NCSSs addressing international cooperation. Nevertheless, both hypotheses are validated given that only 13 countries have expressed their cybersecurity-related actions in case of war and most NCSSs discuss international cooperation.

In terms of the large appearance of the EU as a block and NATO as an organization for international cooperation, it is undiscernible from our analysis whether, for example, the need for these collective efforts to counter a threat of ‘war’, ‘warfare’, and ‘conflict’ in cyberspace is the result of more intensively felt or shared threat in the EU block or among NATO member states with a suggestion of a commonly perceived ‘enemy’, or whether, simply, it is because more collaborative frameworks exist in the EU or NATO context. Given that it is rather conclusive that states seek international cooperation as countermeasures to the threat of ‘war’, ‘warfare’, and ‘conflict’ in cyberspace, further study could be conducted, in more region or country-specific context, to excavate who is collaborating or seeking to collaborate in which context, which may assist states in refining their cybersecurity strategies.

Lastly, with a minimal number of references to neutrality, more or less confined to internet or technical/technological neutrality, and no mention of law of neutrality in the meaning of IHL in cyberspace, we can validate our first hypothesis and can only conclude that it is an area where decisive positions or views in terms of strategies are not yet prevalent among states, or states are still unwilling to express their positions to the outside world, maintaining a “*persistent policy of silence and ambiguity*” (Efrony and Shany 2018, p.588) that is rather frequent in issues pertaining to the identification of state practice or views in cyberspace. Given the complexity and uncertainty of the concept of neutrality itself in cyberspace, we understand that the overview of the fact of its absence is telling us of the difficulties ahead in terms of strategizing neutrality in cyberspace context both domestically and internationally.

6. Conclusion

This paper presented a global snapshot of the national positions on conflict, neutrality, and cooperation with regards to cybersecurity, of all countries (113) that have publicly released an NCSS. As hypothesized, very few countries (13) reference their cybersecurity-related preparations and preparedness for or during times of war (even though more than half discuss warfare in other general topics), and even less (5) delve into the topic of neutrality. With 111 nations discussing international cooperation, the other side of the hypothesis is similarly proven.

Future research might delve into individual national case studies, or more in-depth bi-/multi-lateral comparative studies of these topics within the cybersecurity context. While outside the scope of this study, during its course, we also discovered the existence of International Cybersecurity Strategies in some countries. It would be worthwhile to study those and compare them to their national counterparts, or between different countries. We also realize that the topic of war would be presented in more detail in (National) Defence Cyber Security Strategies; however great care must be undertaken to separate the national and institutional documents for such future studies.

By the time of this paper is published, some of the more ‘outdated’ NCSS might have been updated with newer versions. For them, and all new versions that will appear in the coming years, we wish to articulate the need to present a national position on war / conflict and neutrality, given the recent flare-ups between countries, as possible deterrence, CBMs, and communication instruments. This would also mean that it would be also necessary to make NCSSs publicly available. A few countries were not included in this study due to their NCSS not being publicly accessible nor available.

Acknowledgement

This article has been partially supported by the Doctoral School in Economics and Innovation, ASTRA "TTÜ arenguprogramm aastateks 2016-2022", Project code: 2014-2020.4.01.16-0032.

References

Beecroft Nick. (2021) *The UK's Cyber Strategy Is No Longer Just About Security* [Online]. Carnegie Endowment for International Peace, https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037.

Caudle Sharon L. (2009) "National Security Strategies: Security from What, for Whom, and by What Means." *Journal of Homeland Security and Emergency Management* 6(1): Article 22.

Cordey Sean and Kohler Kevin. (2021) *The Law of Neutrality in Cyberspace*. ETH Zurich.

Cornish Paul, Lindey-French Julian and Yorke Claire. (2011) *Strategic Communications and National Strategy*. The Royal Institute of International Affairs: Chatham House.

CSIS - Center for Strategic and International Studies. (No date) *Significant Cyber Incidents* [Online]. CSIS, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Daricili Ali B. and Özdal Barış. (2018) "Analysis of the Cyber Security Strategies of People's Republic of China." *The Journal of Security Strategies,* 14(28): 1–35.

Drew Dennis M. and Snow Donald M. (1988) *Making Strategy: An Introduction to National Security Processes and Problems*. Maxwell Air Force Base: Air University

DuMont Malia. (2019) *Elements of national security strategy* [Online]. Atlantic Council, https://www.atlanticcouncil.org/content-series/strategy-consortium/elements-of-national-security-strategy/.

Efrony Dan and Shany Yuval. (2018) "A Rule Book On The Shelf? Tallinn Manual 2.0 On Cyberoperations and subsequent state practice." *The American Journal of International Law* 112(4): 583–657

eGA. (No date) *NCSI – Methodology* [Online]. eGA, https://ncsi.ega.ee/methodology/.

European Union. (2015) *REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union*.

Greenwood Christopher. 1987. "The Concept of War in Modern International Law." *International and Comparative Law Quarterly* 36(2): 283–306.

Hurel Louise M. (2020) *Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future* [Online]. Internet Governance Project, https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/.

Kolini Farzan and Janczewski Lech. (2017) "Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies." *PACIS 2017 Proceedings* 126.

Lauterpach Hersch. (1952) *Oppenheim's International Law Volume 2, Disputes, War and Neutrality*. 7th edition. Longmans

Libicki Martin C. (2018) *Conquest in Cyberspace: National Security and Information Warfare, Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Luiijf Eric, Besseling Kim, and Graaf Patrick de. (2013) "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures* 9(1-2): 3–31.

Merriam-Webster. (No date) *Warfare Definition & Meaning* [Online]. Merriam-Webster, https://www.merriam-webster.com/dictionary/warfare.

Naylor Esther, Painter Christopher and Hakmeh Joyce. (2022) *How does capacity-building make cyberspace better?* [Online]. Chatham House, https://www.chathamhouse.org/2022/02/how-does-capacity-building-make-cyberspace-better.

Newmeyer Kevin P. (2015) "Elements of National Cybersecurity Strategy for Developing Nations." *National Cybersecurity Institute Journal* 1(3): 9–19.

OECD. (2012) *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. Paris: OECD

Przetacznik Jakub and Tarpova Simona. (2022) *Russia's war on Ukraine: Timeline of cyber-attacks* [Online]. EP, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Reveron Derek S. (2012) *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington D.C.: Georgetown University Press

Sabillon Regner, Cavaller Victor and Cano Jeimy. (2016) "National Cyber Security Strategies: Global Trends in Cyberspace." *International Journal of Computer Science and Software Engineering* 5(5): 67–81.

Shackelford Scott and Kastelic Andraz. (2014) "Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity." *New York University Journal of Legislation and Public Policy*, 2016, Kelley School of Business Research Paper No. 15-4.

Shafqat Narmeen and Masood Ashraf. (2016) "Comparative Analysis of Various National Cyber Security Strategies." *International Journal of Computer Science and Information Security* 14(1): 129–136.

Snyder Hannah. (2019) “Literature review as a research methodology: An overview and guidelines.” *Journal of Business Research* 104: 333–339.

Štitilis Darius, Pakutinskas Paulius and Malinauskaitė Inga. (2017) “EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis.” *Security Journal* 30, 1151–1168.

Teoh Chooi S. and Mahmood Ahmad K. (2017) “National cyber security strategies for digital economy.” *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*.

U.N. (No date) *Capacity-Building* [Online]. U.N., https://www.un.org/en/academic-impact/capacity-building.

UNIDIR. No date. *About* [Online]. UNIDIR, https://cyberpolicyportal.org/about.

Von Solms Rossouw and Van Niekerk Johan. (2013) “From information security to cyber security.” *Computers and Security* 38: 97–102.

Yannakogeorgos Panayotis A. and Lowther Adam B. (2016) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Florida: CRC Press

Wheelen Thomas, Hunger J David, Hoffman Alan N., Bamford Charles. (2017) *Strategic Management and Business Policy: Globalization, Innovation and Sustainability*. Harlow: Pearson Education.

Wu Tim. (2003) “Network Neutrality, Broadband Discrimination.” *Journal on Telecommunication & Hightech Law* 2: 141–175.

Ziolkowski Katharina. (2013) *Confidence Building Measures for Cyberspace – Legal Implications*. Tallinn: NATO CCDCOE.

Appendix 4

Publication IV

Dueñas-Cid, D., Krivonosova, I., **Serrano, R.**, Freire, M., & Krimmer, R. (2020). Tripped at the Finishing Line: The Åland Islands Internet Voting Project. In: *Electronic Voting. E-Vote-ID 2020. Lecture Notes in Computer Science, Vol. 12455*, pp. 36–49. Krimmer, R., et al. (Eds.). Springer: Cham. doi:10.1007/978-3-030-60347-2_3. ETIS 3.1

Tripped at the Finishing Line: The Åland Islands Internet Voting Project

David Duenas-Cid[1,2](✉), Iuliia Krivonosova[1], Radu Serrano[1], Marlon Freire[3], and Robert Krimmer[1,4]

[1] DigiGovLab, Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology, Akadeemia tee 3, 12618 Tallinn, Estonia
{david.duenas,iuliia.krivonosova,radu.serrano, robert.krimmer}@taltech.ee

[2] Management in Networked and Digital Societies, Kozminski University, Jagiellonska 57/59, 03-301 Warsaw, Poland
dduenas@kozminski.edu.pl

[3] Faculty of Engineering, University of Porto, Porto, Portugal
marlonfreirephd@gmail.com

[4] Johan Skytte Institute of Political Studies, University of Tartu, Tartu, Estonia

Abstract. The Åland Islands spent years preparing an internet voting system, to be implemented for the first time in October 2019 for Parliamentary Elections. Despite this, the project was canceled the evening before the expected release date. In this paper, we explore the causes of this failure using a two-pronged approach including Information System failure perspectives and the approach to e-voting Mirabilis, focusing on organizational elements which provoked the decision not to use the system.

Keywords: Åland Islands · Internet voting · System failure · Organizations · Convenience voting

1 Introduction: Three Contextual Questions

The Åland Islands were expected to introduce an internet voting system (IVS) during their last Parliamentary elections (October 2019), for expatriate voters, with the expectation to extend use of the same system to Municipal elections too and to all possible voters on the next possible occasion. Unexpectedly, internet voting was cancelled the day before it should have started. This paper explores this case approaching it from an Information System (IS) failure framework [18, 20], describing how interactions between the different stakeholders involved are a central element for understanding the final decision, and the e-voting Mirabilis frame, focusing on the organizational elements which provoked the decision to not use the system.

1.1 What Are the Åland Islands and How Does Their Electoral System Operate?

The Åland Islands are a Swedish speaking autonomous region of Finland comprising around sixty inhabitable islands and around six thousand small rocky islands not suitable

R. Krimmer et al. (Eds.): E-Vote-ID 2020, LNCS 12455, pp. 36–49, 2020.
https://doi.org/10.1007/978-3-030-60347-2_3

for human habitation or settlement. The archipelago is situated in the opening to the Gulf of Bothnia, bordering south-western Finland and central-eastern Sweden and is inhabited by 29,789 citizens, 11,743 of them living in the capital, Mariehamn. The autonomy of the Åland Islands was affirmed in 1921 by the League of Nations, through which Finland would protect and guarantee the continuation of the culture, language and traditions of the archipelago, and the Ålandic Government would have a say in foreigners acquiring franchise and land in the isles [4]. Similarly, the autonomy of Åland was reaffirmed by the treaty for admitting Finland into the European Union. Amongst other elements of self-government, the Åland Islands have their own Parliament (Lagting) and Government (Landskapsregering), elected in their own independent elections.

The uniqueness of Åland's status translates to implementation of its elections, relating to both the archipelago and Finland. The Åland administration is in charge of organizing Parliamentary and Municipal elections, and uses the electoral system of proportional representation, in which voters cast votes for a particular candidate, instead of for a party. Votes are transferred into seats using the D'Hondt method. Participation in elections is determined by acquiring the Right of Domicile in Åland, or after having been an inhabitant of any Ålandic municipality for one year prior to Election Day (the latter only applies for municipal elections). Legislation regulating these elections is covered in the Election Act for Åland [1], adopted by their Parliament in January 2019, on the occasion of introducing internet voting.

1.2 Why Were the Åland Islands Attempting to Use Internet Voting?[1]

As the head of election administration, Casper Wrede describes [21], the idea to implement this voting channel in the Åland Islands was following the general worldwide trend and popularity of internet voting in the late 1990s, but the initial debate and research which produced the recommendation not to introduce the system until voter integrity and identification issues had been resolved. The idea of postponing introduction of a remote voting system in the islands was reinforced by the Finnish failure in their attempt to use electronic voting machines in 2008 local elections. Using internet voting was again introduced to political debating chambers after discussions on the reform of the electoral system in 2014 where, amongst other proposals, the suggestion was voiced to start introducing internet voting as an additional advance voting channel, only applicable for people living outside the Åland Islands. The introduction of internet voting was expected to be facilitated in two steps: 1) in 2019, only for expatriate, overseas voters in Parliamentary Elections; and 2) in 2023, based on the results of the 2019 experience, internet voting would become available for all voters [21]. Three main elements are mentioned as key factors triggering implementation of internet voting: convenience, turnout, and international projection.

Given the geographic location of the Åland Islands, it has been a long term goal of electoral authorities [19] to make voting more convenient for remote voters, as well as a traditional element considered as a driver for internet voting. The logic is based on two assumptions that 1) a general demand for convenience voting channels exists among the

[1] For a more detailed development of this point, see our previous work on the preparation of Åland's internet voting project [5].

population; and 2) trust has been established towards remote voting channels, implemented in an uncontrolled environment. The Åland Islands have a legacy of convenience and remote voting channels being available to the population, since even before 2019 they were already offering, a number of voting channels consisting of 1) early voting at general voting locations not linked to the voter's place of residence, meaning that a voter could vote at any early voting polling station across the Ålands during an 11-day period; 2) early voting at care institutions; 3) Election Day voting; and 4) Postal voting for those who "are out of the country or are ill/handicapped and unable to vote in any other way"[2].

Advance voting channels are quite popular for the population and currently are used by around 1/3 of all voters who cast a vote (35% in 2019 and 2014 EU Parliament Elections)[3]. Said differently, Postal voting was not able to gain popularity due to the cumbersome procedure. During 2015 elections to the Legislative Assembly, around 150 people voted by post, constituting only 0.7% of all eligible voters [3], with about 10% of postal ballots arriving too late to be counted for the elections. Besides Postal voting, no other voting channels are available to voters residing overseas, outside of the islands. Åland does not have any embassies, representative agencies, or consulates and, as a result, voters do not have the option to vote in foreign missions. It is no coincidence that expatriates – 'absentee, overseas' voters - constituted a target group for initial use of internet voting.

The introduction of internet voting was also connected to projecting Åland to the outside world. In recent years, the Government of Åland provided IT-services for the public sector and contributed to overall digitization of the islands in various ways, through the public company ÅDA[4]. Both the development of internet voting and digitization of the islands are elements for creating a digital narrative of Ålandic identity and creating a positive image to promote the islands as a place where innovation thrives, and to highlight the positive impacts of their self-government.

In contrast, the reduced costs and time required are not amongst primary reasons for introducing internet voting. Cost savings were highlighted as a potential advantage for the long term [2, 3], under the assumption that a realistic assessment of cost-efficiency would only be possible once the system had been consolidated and the number of users increased. Regarding time savings, another dimension which is often highlighted as a potential positive outcome of using internet voting, the small size of the electorate would limit the potential impact of using the system in this regards.

1.3 Why Are We Writing This Paper?

Discussions on the convenience of introducing internet voting to the Åland Islands were held for more than 20 years, intensifying during the last months of preparatory work. The first use of internet voting seemed to be ready for 'go live' on October 2019 but,

[2] As described in the leaflet produced by the government of Åland to explain how Elections function to citizens: "Election on Åland, 18 October 2015".

[3] Statistics and Research Åland, URL: https://www.asub.ax/sv/statistik/valet-europaparlamentet-2019.

[4] Åland Digital Agenda, see: www.ada.ax/.

at the very last minute and after the system had been set up, the use of internet voting was cancelled hours before elections opened. Our initial goal with this research was to approach the Ålandic case in order to observe their initial use of internet voting and conduct a cost-efficiency calculation of multichannel elections as we had already done for the case in Estonia [9, 10]. The fact that elections were cancelled when our team was already in-place and on site and we had already conducted extensive preparatory work (analysis of electoral law, preliminary interviews, initial study visit) made us direct our gaze towards analyzing the reasons for failure. We had the rare and unexpected opportunity to directly observe management of an electoral crisis and to interview the relevant actors. Our aim is to pinpoint the different elements which may have contributed to this final decision and try to extract lessons to be applied by other electoral managers and for implementing voting technologies. Failures help unveil processes which would remain hidden when assertions are made for systems that are successful [14], in this particular case, the complexity of electoral management and technological innovation and the interaction of different stakeholders.

To do this, we will propose and use a framework describing the Information System (IS) failure and interactions between the different stakeholders involved, relying on interviews conducted during our study visits to the islands.

2 Stakeholders and Models of Failure

Several studies targeted the issue of Information Systems (IS) failures [5, 6, 8, 12, 16, 22] over the last few years, and some proposed explanatory frameworks described the concept of IS failure and tackling the determinants for successful implementation [18, 20]. Definitions of an IS failure are generally in line with the two categories Ewusi-Mensah described [8]: either the system fails due to inability to perform to users' levels of expectations or due to the inability of producers to produce a fully-functional, working system for users. Sauer [18] considers the definition of an IS system failure as a system abandonment due to stakeholder dissatisfaction.

Sauer [18] developed an explanatory framework describing IS failure based on three key elements: 1) Supporters, 2) Project Organization and 3) IS. In it, he creates a triangle of dependencies between these three elements and there must be interaction between them to prevent eventual failure occurring. In his analysis, failure is presented as the outcome of the interplay between context, innovation process and support. Flaws occur if the context is inadequately addressed in the innovation process, and, if flaws should accumulate, the system loses support and faces risk of failure. Sauer also highlights the importance of system supporters and their perceptions regarding the system itself, rather than solely focusing on technological characteristics of the IS. In his interactive framework, the IS serves the supporters, while they in turn support the project's organization, and this last component innovates the system. According to Sauer's way of thinking, failure is seen as total abandonment of a system, which occurs when this triangle of dependencies breaks down. The role of Project Organization is seen as a middleman between stakeholders and the IS. What is more, the role of project organization is not limited to this: it also serves as "a mediator" between context, system and stakeholders.

Toots [20] iterated and adapted Sauer's model in order to develop an analytical framework for contextualizing and explaining factors which influence system failure for e-participation. The framework proposed by Toots consists of four key elements, focusing on: a) Innovation Process; b) Contextual Factors; c) Processes with contextual factors interacting with innovation process and stakeholders and; d) Project Organization, where they have the power to change influential contextual factors or if it can, to align the system to the context. The sub-elements of context include technology, organizational variables, and politics. In both frameworks mentioned above from Sauer and Toots, the elements complement one another, creating an interactive triangle of dependencies which allows us to understand the reasons for failure in exchanges occurring between different elements.

The Supporters in Sauer's model can be also viewed as stakeholders in Toots' model, but Toots includes a differentiation between "Project Organization" and "Stakeholders", based on the following logic: *stakeholders need the project organization to develop IS according to their interests* (p. 548). Therefore, Project Organization is viewed as a middleman between stakeholders and the IS, but the role is not limited solely to this, serving also as "a mediator" between context, system and stakeholders.

Even if Toots' efforts bring the causes for e-participation IS failure closer to the case we are analyzing, her model does not apply in full for understanding reasons for the Åland Islands' failure. Of the four key assumptions presented, only two of them are indicative for our case:

1. *"Implementation of an e-participation system may be regarded as an innovation process characterized by uncertainty and susceptibility to changes in the context;*
2. *While contextual factors and changes are not the immediate cause of failure, context may constitute an important trigger for failure."*

However, even these assumptions do not apply fully in our case, because Toots, following Macintosh's [13] definition of e-participation, explicitly distinguishes *e-participation from other e-democracy instruments such as e-voting* (p. 546). Ålands' IVS is a type of e-voting and thus could not fully benefit from applying a framework designed for e-participation, even if it is an excellent fulcrum for developing a new iteration of the model.

Some of the arrangements proposed for Toots' model relate to the role stakeholders play and the fact that the technology was never used. One of Toots' arguments is that if using an e-government system is not satisfactory for those who must use it, they will abandon its use and condemn the system to failure. In the case under analysis, the IVS was never used by stakeholders, so their impact is minor. On the contrary, the role of Project Organization and the Context in which the IVS is framed play a more relevant role, since the unequal discourses collected from Election Managers and Vendors highlight the existence of a difference in criteria towards the system. Also, some of the difficulties highlighted for developing IVS relate to adapting to the context, either legal or technological, of the Ålandic environment.

Taking one step forward, for iteration and for adapting Toots' framework to the case of the Åland Islands, we can detect different elements proposed in the framework mentioned: 1) Project Organization existed and managed creation, development and implementation of the system (here, also, a difference to Toots' model, since the role of Project Organization was not to innovate an IS which already existed, but to implement a brand new one); 2) the IS was in-place but never used; 3) the Supporters never accessed the system, but they could track developments through the media and further discard the system; 4) external contextual factors might have facilitated failure of implementation, such as the Data Protection Authority arriving late or integration of the IVS in the Finnish e-Government environment. Failure, in our case is transposed to being the decision to not proceed with internet voting, even with the system in-place, giving more relevance to the interaction between the different elements than to the IS itself.

Since some of the elements included in the frameworks proposed by Toots and by Sauer cannot be included in the same manner as has just been described, their models need to be iterated and adapted to the conditions of the case study. For this reason, we refer to the conceptual model analyzing e-voting implementation – the E-voting Mirabilis [11]. Including this allows enlarging the context in which the IVS is implemented. It focuses on four macro dimensions influencing application of ICT in elections:

- technological dimension;
- legal dimension;
- political dimension;
- social dimension.

For the technological dimension, we consider what supporting infrastructure for internet voting was already in place (in particular, voter register and voter identification). For the legal dimension, we trace how the legal framework has been amended to adjust for internet voting, and whether it covers such aspects as secure processing of voters' personal data. For the political dimension, we analyze what groups of voters' internet voting was supposed to enfranchise, how the IVS was evaluated, and what was the overall political discussion on its introduction. The social dimension focuses on citizens' understanding and level of trust in IVS.

The E-voting Mirabilis is also helpful for stakeholder categorization, distinguishing between Voters, Politicians, Election managers, Vendors, and Media representatives and election monitors or observers. Combined with Toots' model, distinguishing between stakeholders and project organization, categorization should look like this:

- Stakeholders: Voters; Politicians; Media representatives and election observers;
- Project organization: Vendors; Election managers, Project managers.

Therefore, our theoretical framework builds on the conceptual model of the 'E-voting Mirabilis' [11] and an adaptation of the information system failure framework by Toots [20]. Based on these, we propose and use the "Mirabilis of internet voting System (IVS) failure". Toots' 'e-Participation System' was replaced by the IVS, and inside it we find Krimmer's e-voting components. All around, the 'contextual factors' (Toots) or 'four main macro dimensions' (Krimmer) *that explain the areas that influence e-voting deployment* [11]. Afterwards, Krimmer's five stakeholder groups which help to apply ICT to the electoral process, are grouped as either a 'Stakeholder' or 'Project Organization', according to Toots' framework and to their direct involvement in implementation of internet voting. Relationships between IVS, Project Organization and Stakeholders have remained similar (with some minor changes) to Toots' original diagram (Fig. 1).

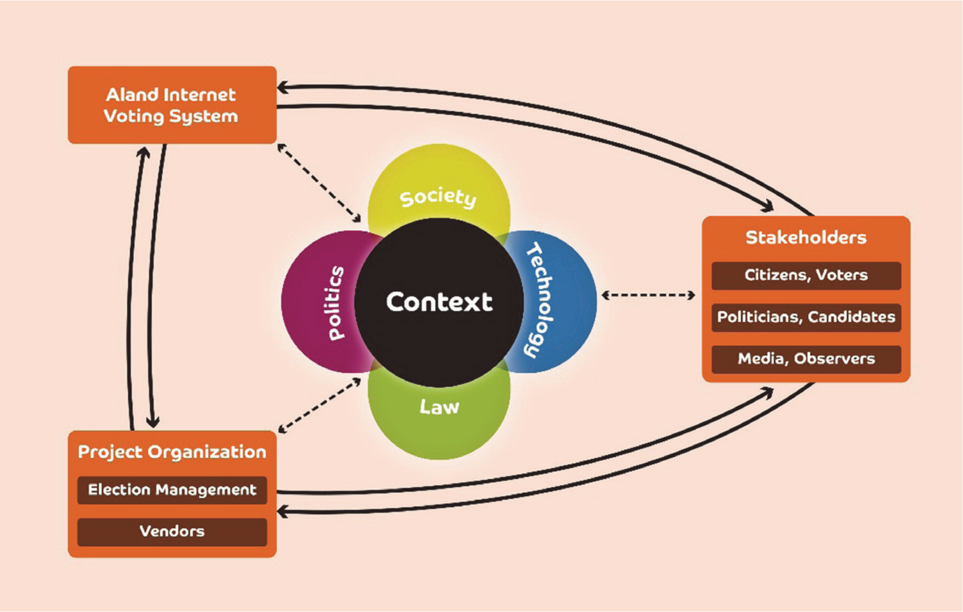


Fig. 1. Mirabilis of IVS failure.

In the context of the Åland Islands, project organization will be represented by the vendor (Scytl) and the organization responsible for the IVS procurement (ADA) and project management (Electoral Management Body). The rest of the actors will fit into the category Stakeholders: voters, government, election administration, parties, Data Protection Authority, and others. Stakeholders send requirements of IVS to project organization and provide them with the resources to fulfill those requirements. The IVS produced should satisfy stakeholders, otherwise, they will not use it. In other words, the IVS produced should meet the expectations of key stakeholders. In the context of the Åland Islands, this first and foremost concerns the stakeholders responsible for the decision on whether to start using internet voting. Already at the stage of modelling, we can observe that there is a possible mismatch between stakeholders' requirements formulated to project organization at the start of IVS development, and expectations which the final IVS should satisfy.

In this conceptual model, the context plays the key role: it shapes the demands of stakeholders, thus affecting the requirements they will send to project organization; it constrains or defines what is possible for project organization to fulfil the requirements; and the final IVS should serve the context.

3 Methodology

Data collection for developing this case study took place between March and December 2019. During this period, we conducted two visits to Mariehamn in teams of two researchers: 9–16 June and 14–22 October. Most of the interviews and observations included in this research were carried out during these visits to Åland, although we had completed some preparatory interviews with the Ålandic Electoral Management Body (EMB) before the first visit, and arranged some digitally mediated interviews after the second visit. A total of 20 semi-structured interviews were conducted with EMB, ADA, Scytl, Central Committee for Elections, Data Protection Authority, local politicians, and voters. Many interviews had more than one respondent and some interviewees were contacted at different times. In all, a total of 20 people were finally interviewed, and the interviews were anonymized (see Table 1). Data was analyzed using NVIVO qualitative data analysis software following a multi-stage inductive approach consisting of identifying a set of core themes during transcription (including, amongst others, 1) the electoral process, 2) government, 3) introduction of internet voting, 4) cancellation of internet voting and 5) voting organization) and the further coding of interviews based on the above themes. This inductive method was aligned with re-focusing of the research plan described below, allowing us to include the information collected in a context of crisis and relate our conclusions to the literature on Information Systems failure.

Table 1. List of interviewees, anonymized[a].

Occupation	Date
Head of election administration	March, 2019
Head of IT-unit at Ålands Landskapsregering	June, 2019
System administrator at Ålands Landskapsregering	June, 2019
Legal Director, Government Offices, Unit for Legal and International Affairs	June, 2019
CEO of Åda Ab	June, 2019
Project Manager at Åda Ab	June, 2019
Data Inspector	June, 2019
Minister	June, 2019
Minister	June, 2019
Head of election administration (II)	June, 2019
Voter	October, 2019
Voter	October, 2019
Head of election administration (III)	October, 2019
Data Inspector (II)	October, 2019
Head of IT-unit at Ålands landskapsregering (II)	October, 2019
CEO at Åda Ab (II)	November, 2019
Worker at Åda Ab	November, 2019
Worker at Scytl	November, 2019
Worker at Scytl	November, 2019
Worker at Scytl	November, 2019
Worker at Scytl	November, 2019

[a] The numbers in brackets refer to the number of times the person was interviewed.

The case of the Åland Islands was selected due to the fact that they intended to implement internet voting for the first time and it represented a good comparison to research already conducted by the research team. The size of the country and administration allowed swift, effective communication and privileged access to data. Also, it would have covered a relatively unexplored dimension of electoral analysis, the costs of initial implementation of voting channels and their evolution over time.

We must point out here that the methodological plan was reframed during the research, due to cancellation of the IVS. Whilst applying the methodology for calculating costs, the initial plan followed on from previous research [3, 4] and research mentioned in a previous publication on the same case [5]. Cancelling implementation of internet voting took place during the research team's second visit to the Åland Islands, at a time at which the analysis of electoral law and modelling of the electoral processes had already been completed, as well as several interviews for understanding and describing the electoral system, its management and the costs involved. The fact that the research team was on-site during the cancellation, allowed them to observe and conduct interviews about management of the crisis, which were followed by a second round of interviews with the key stakeholders. Hence, this publication is the result of refocusing our research goals, given the opportunity to gather information on a critical case study relating to management of an electoral crisis due to cancellation of a voting channel. As a result of this, the interview design was modified (*the contents of the questionnaire)* in the course of the data collection process, paying special attention to integrating the different steps of data collection in the final analysis of the data.

The value of the data collected is derived from the opportunity and the uniqueness of the situation but, at the same time, it may involve some limitations given that it was not possible to plan such a methodological reconfiguration in advance. Amongst the strengths of our data collection process: 1) we developed a deep analysis of the electoral system prior to cancellation, and so were able to rapidly identify the key stakeholders to interview and the key processes to direct our attention to; 2) the presence of our research team on the ground allowed us to gather first impressions and reflections after cancellation and to experience the moment of cancellation on-site: direct observation of events provides us some interpretative clues which it would not be possible to gather through other data collection methods [7]. Amongst the limitations: we could not access some information on grounds of secrecy and confidentiality; the sources which, according to some discourses, could shed light on legitimacy of their claims.

4 Data Analysis

The context surrounding the Åland IVS looked promising for implementation of the new voting channel. At a socio-political level, no objections were raised against the system, the media did not pay much attention to implementation of the voting channel and no political party openly opposed it. There were more concerns about lowering the age of voters to 16 years of age for example, a reform discussed simultaneously to introduction of internet voting.

The overall political discussion on internet voting was fairly positive. Stakeholder evaluation varies from feeling *fairly optimistic* (I-1) to endorsements: *I always thought* *that this is a good thing, this is something we need to do* (I-13). The Parliament also has not seen much of the debate on internet voting, besides *some discussion on the security issues* (but) *in general, all parties in Åland responded positively to this voting channel* (I-13). Media outlets in the Åland Islands were not interested in internet voting, until almost right before voting started: *here is not big interest because everybody's focused on the transformation of the municipalities* (I-13), *I think, as a journalist, the interest in the elections will awaken in the end of August, when the campaign starts* (I-13).

This smooth political development crystalized in the decision that, during the first binding trial during the 2019 Parliamentary elections only expatriates (*overseas, absentee voters*) were eligible to vote via the Internet, *most of [the expats] are young people, they are studying or have been studying and stay for some years after studying* (I-3). This decision was considered as a clear improvement of voting conditions for expat voters (*a very strong urge from the younger generation to have a simplified voting procedure, possibly electronic* – I-5*)* since they could avoid the problems associated with using postal ballots to cast their votes (*last election 10% of our postal votes came back too late to count* – I-5).

As a result of which, *the whole new electoral act passed unanimously* (I-3). The legal dimension, in accordance with Krimmer [11], regulates how the electoral code can be changed in order to permit votes cast by electronic means and to provide the level of accountability required to the voter and should further: 1) provide the voter with the ability to see how personal data are processed; 2) include the principle of proportionality when handling personal data; and 3) serve as a guiding indicator. The Election Act for Åland, issued on May 2019, consists of 15 chapters and 122 individual sections (or articles), and defines all voting channels including postal voting, advance voting, Election Day voting and contains *new provisions on internet voting* (I-5). The legal dimension was further bolstered by the 'Registerbeskrivning'[5] or Privacy Policy (2019) which describes processing of personal data in connection with implementation of the Parliamentary and Municipal elections in Åland, including a description of the personal data required, its use during various stages of the election process, and the entities responsible which may interact with it, either directly or indirectly.

In order to specifically implement internet voting, the government *decided quite early [for] the procurement process*, that they *should buy a service, not the system* and that they *need[ed] someone else to run* it (I-10). To this end, the law and the procurement requirements were written in "parallel". As confirmed by an interviewee, this was *not ideal, perhaps theoretically. But in practice, it was quite good because we could adjust the wording and the law, according to what we experience, what is possible and how things should be* (I-10). This procurement process was run by ADA, resulting in a bicephalous organizational structure from the side of the government: ADA for managing the contract and the Electoral Management Body for management of elections, both interacting with the vendor.

The development of IVS was accompanied by audits and evaluations. The checks and balances are prescribed by law: *the government [...] should check and to have a third party to check everything, all the processes. So, we will also have somebody to check*

[5] Available at: https://www.val.ax/sites/default/files/attachments/subject/behandling-av-personuppgifter.pdf. Last accessed 15 June 2020.

when the election takes place that everything is [OK] (I-4). However, in June 2019, the independent body which would check and review the i-voting system had not yet been defined. The notions of who this independent body could potentially be were still vague: *It could perhaps be some authority from the Finnish state government, but it must be independent from the vendor and from the government… (…) it could also be some representatives from the Finnish authorities. Could be representatives from Estonia, for example. I mean, experts on internet voting, would be possible. Or it could be some audit company like KPMG, or whatever* (I-9).

At some point during development of the IVS, the Data Protection Authority of Åland became interested in auditing the process [17], for the following reasons: *Well, the biggest reason is because this is a new project, that has not been done before. And also, since this is a democratically critical process, pertaining to a lot of sensitive personal information or other special categories of personal information as in political opinions… since that kind of data is being processed […] That is the kind of processes that the data protection authorities should be auditing to make sure that they're safe (I-17).* The arrival of the Data Protection Authority brought a new along with it player to the table; since it was not possible to conduct the audit on their own, it was necessary to outsource this to an external consultant for *auditing the security documentation sent by [the vendor]. And to see if they fulfilled the safety requirements* (I-17). The main findings of the audit, were that the Data Protection Impact Analysis (DPIA) has not been completed[6].

From a technological perspective, the IVS used the digital infrastructure provided by Finnish government – e-ID systems (e-ID Cards and Mobile-ID) – and private institutions (e-Banking), and consisted of main elements such as an e-ballot box, a list of voters and candidates, voter identification and authentication as well as vote verification.

During the development process of the IVS, a number of deficiencies were detected with the e-Identification system: in relation to integration *during the first pilot we found errors in the Suomi.fi implementation. So when I cast a vote, I was not successfully logged out from the authentication* (…) *And then they have corrected one mistake in Suomi.fi identification but there was still one loop, one error more.* (I-19); *In June already. And then in July again and in August, again* (I-15). Discovery of these problems was motivation for outsourcing a penetration test to an external vendor who dealt directly with the vendor in charge of IVS. The interaction between both vendors presented some problems in relation to accessibility to the source code of the voting system, since the vendor in charge of the penetration test was allowed access to the code but in the premises of the IVS provider, in a different country, and this option was not accepted and delayed the auditing process[7]: *The argument that they were unable to access the source code for me is not a valid argument (…) they were invited… but even if they decided to not to come, this particular issue has been tested* (I-20).

[6] For further details on the General Data Protection Regulation in the Alandic elections, see the work of Rodríguez-Pérez [17].

[7] In this regard, it is worth noting that it was not possible to interview the vendor in charge of the penetration test due to a disclosure agreement. The views collected in this research might be distorted due to this issue.

According to the vendor's position, the problems detected challenged the development of the system: *during such integration, [or] maybe during any sort of customization or development, when you test, you find things, with the objective to correct them, fix them (*I-20*); The main challenge here is that, since we are not (…) Finnish, we don't have Finnish ID, so we have few test credentials that we can use in our tests to automate them (…) the personnel both from ADA and the government (were) very helpful as well in providing (them) to us (*I-20*).* Problems were resolved according to their position, and the system was in place and ready to run during the elections as expected: *this issue with the verification of the digital signature. It was corrected, and was said that was corrected (by the vendor).*

The report from the vendor in charge of the penetration test was finished very late on (*we got the report from the security company very late, so it was not so much time to evaluate that and also to have a meeting with them and to discuss about – I-19*) and, even if the problems might have been solved, *we have not run the pilot from start to end (…), never ran it from beginning to end in a test environment (…), it doesn't feel right to do it (run the elections)* (I-19). The result was, cancellation of using internet voting at the very last moment.

5 Discussion and Conclusions

In the complex environment of electoral management, many factors can tip the scales towards failure if these are not perfectly aligned. In the case analyzed, even if there was a long process of preparation, training and a well-documented Electoral Management Body with members and experienced vendors, their joint efforts did not match up to initial expectations and the IVSs could not be implemented. It is not our role (nor our aim) to blame anyone for this outcome, but to understand the process in order to gain some useful knowledge and experience for others who aim to implement similar systems.

As we described, the context in which the IVS was to be implemented appeared to be quite friendly, accommodating, and welcoming: positive political discussions, lack of external agents discussing the suitability of the decision taken. The law was approved on time, as was the procurement process too. The problem, then, relied on the process of adjusting the IVS and the interaction between the members of the project organization, particularly with relation to timing. The accumulation of delays in some deliveries, responses and interactions, combined with organizing pilots during the summer period (in June and in August) reduced the time available for resolving problems detected (problems of integrating IVS into the Finnish e-ID system). Developing two Penetration Tests in a relatively short period of time and the presumed problems of collecting data for the audits delayed the responses until a time when they were already redundant and no longer required. The Data Protection Authority's appearance late in June, and creating a new parallel legal and document audit probably superimposed a new layer of complexity onto implementing the system. Even if problems could have been resolved, as the vendor in charge of the IVS states, the authorities 'confidence in reliability of the system had already been damaged and the decision to cancel the elections could seem reasonable for those who were legally qualified to make it. Paraphrasing the idea expressed by Oostven and Van den Besselaar [15], *a voting system is only as good as the Administration* ("public" in the original version) *believes it to be.*

The key takeaway we can extract from this case is the relevant role which organization of the overall process plays in successful implementation. In the case under analysis, time management appears to be the main limiting factor for effective resolution of problems identified. We believe that with better time-management, four critical factors could have been managed more effectively: 1) the vendor could have resolved the problems detected in a timely manner, 2) project organizers would have had time to make sure these issues were resolved, 3) the final version of the system could have been tested, and hence, 4) the system could have been operated securely in real time. In addition to this, other factors, that without time constrictions could have had an irrelevant impact, in the case analyzed played an important role. Firstly, the bicephalous structure followed for project management divided the knowledge available on the side of project organizers, that is the technical knowledge separate from contract management and adding to the complexity of the process. Due to this fact, the process was slowed down at critical moments when a more directed management structure could have forced the vendor to react more swiftly in order to solve problems encountered. Secondly, the unexpected problems encountered related to the integration of the Finnish e-Identity system and their late resolution, damaged the trustability of the IVS. A faster detection and a smooth resolution of these problems could have walked the process to a different ending.

In contrast to the case proposed by Toots [20] in which the e-participation system failed due to a lack of a meaningful connection with stakeholders, in the case of the Åland Islands, failure originated on the side of interaction between project organization and the IVS itself, showing, in the end, the relevance of the organizational factor for creating, developing and implementing technological innovations.

Acknowledgements. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857622, and from the Estonian Research Council, under grant agreement PUT 1361.

References

1. Åland Culture Foundation: International Treaties and Documents Concerning Åland 1856–2009. http://www.kulturstiftelsen.ax/traktater/eng_fr/ram_right-enfr.htm
2. Arbetsgruppen för Internetröstning: Rösta per Internet? Mariehamn (2001)
3. Arbetsgruppen för översyn av vallagstiftningen: Slutrapport, Mariehamn (2015)
4. ÅSUB - Statistics and Research Åland: Åland in Figures, Mariehamn (2019)
5. Bartis, E., Mitev, N.: A multiple narrative approach to information systems failure: a successful system that failed. Eur. J. Inf. Syst. (2008). https://doi.org/10.1057/ejis.2008.3
6. Beynon-Davies, P.: Information systems 'failure': the case of the London ambulance service's computer aided despatch project. Eur. J. Inf. Syst. (1995). https://doi.org/10.1057/ejis.1995.20
7. DeWalt, K., DeWalt, B.: Participant Observation: A Guide for Fieldworkers. Altamira Press, Plymouth (2011)
8. Ewusi-Mensah, K.: Software Development Failures: Anatomy of Abandoned Projects. The MIT Press, Boston (2003)

9. Krimmer, R., Duenas-Cid, D., Krivonosova, I., Vinkel, P., Koitmae, A.: How much does an e-vote cost? Cost comparison per vote in multichannel elections in Estonia. In: Krimmer, R., Volkamer, M., Cortier, V., Goré, R., Hapsara, M., Serdült, U., Duenas-Cid, D. (eds.) E-Vote-ID 2018. LNCS, vol. 11143, pp. 117–131. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00419-4_8
10. Krimmer, R., Duenas-Cid, D., Krivonosova, I.: New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? Public Money Manag. 1–10 (2020). https://doi.org/10.1080/09540962.2020.1732027
11. Krimmer, R.: The Evolution of e-Voting: Why Voting Technology is Used and How it Affects Democracy. TUT Press, Tallinn (2012)
12. Lyytinen, K., Robey, D.: Learning failure in information systems development. Inf. Syst. J. (1999). https://doi.org/10.1046/j.1365-2575.1999.00051.x
13. Macintosh, A.: Characterizing e-participation in policy-making. In: Proceedings of the Hawaii International Conference on System Sciences (2004). https://doi.org/10.1109/hicss.2004.1265300
14. Mitev, N.: Are social constructivist approaches critical? The case of IS failure. In: Howcroft, D., Trauth, E. (eds.) Handbook of Critical Information Systems Research: Theory and Application, pp. 70–103. Edward Elgar Publishing, Cheltenham (2005)
15. Oostveen, A.-M., Van den Besselaar, P.: Security as belief User's perceptions on the security of electronic voting systems. Electron. Voting Eur. Technol. Law Polit. Soc. **47**, 73–82 (2004)
16. Poulymenakou, A., Holmes, A.: A contingency framework for the investigation of information systems failure. Eur. J. Inf. Syst. (1996). https://doi.org/10.1057/ejis.1996.10
17. Rodríguez-Pérez, A.: My vote, my (personal) data: remote electronic voting and the General Data Protection Regulation. In: Krimmer, R. et al. (eds.) Fifth International Joint Conference on Electronic Voting, E-Vote-ID 2020. Springer, Cham (2020)
18. Sauer, C.: Why Information Systems Fail: A Case Study Approach. Alfred Waller Ltd. Publishers, Oxfordshire (1993)
19. Szwed, K.: Głosowanie elektroniczne na Wyspach Alandzkich – idea bez pokrycia czy realny scenariusz? PRZEGLĄD PRAWA Konst. **4**(50), 13–32 (2019)
20. Toots, M.: Why E-participation systems fail: The case of Estonia's Osale.ee. Gov. Inf. Q. Preprint (2019). https://doi.org/10.1016/J.GIQ.2019.02.002
21. Wrede, C.: E-voting in a Small Scale – the Case of Åland. In: Krimmer, R. et al. (eds.) The International Conference on Electronic Voting. E-Vote-ID 2016, pp. 109–115. TUT Press, Bregenz (2016)
22. Yeo, K.T.: Critical failure factors in information system projects. Int. J. Proj. Manag. (2002). https://doi.org/10.1016/S0263-7863(01)00075-8

Appendix 5

Publication V
Serrano-Iova, R.A. (2023) [Forthcoming]. Pitfalls at the Starting Line: Moldova’s IVS Pilot. In: *Electronic Voting. E-Vote-ID 2023. Lecture Notes in Computer Science.* ETIS 3.1

Pitfalls at the Starting Line: Moldova's IVS Pilot

Radu Antonio Serrano Iova[1]

Abstract: The Republic of Moldova has been interested in internet voting since 2008. However, it is only now that preparations are currently ongoing to pilot an internet voting system (IVS) for its future use in elections. In this short paper, we explore the current endeavors to set it up, through the perspective of the Mirabilis of IVS failure, in order to identify current pitfalls that are affecting the process, and that could still be addressed in time.

Keywords: Moldova; Internet Voting; Convenience Voting

1 Introduction

The Republic of Moldova has been interested in automating elections since 2008, when a corresponding law was passed. However, the interest on this endeavor fluctuated throughout the years. It was only recently that the concrete actions have been actively undertaken to move forwards with the piloting of an internet voting system (IVS). This short paper presents Moldova's efforts and explores them through the Mirabilis of IVS failure. While Moldova's Internet Voting Project cannot yet be categorized as either success or failure, the Mirabilis is solely used as a tool to identify current pitfalls that are affecting the process and that could still be addressed in time.

2 The Republic of Moldova and i-Voting

The Republic of Moldova is a landlocked country bounded by Ukraine and Romania. It has a population of 2,6 million inhabitants [Mol23] and has a diaspora between 1,11 and 1,25 million people (according to 2021 data) [Mak21]. Primarily because of this last number, the applicability of distance voting was researched in 2007. Back then, the diaspora was smaller (comparatively to the 2021 data) but still accounted for 1/3 of the country's population. The study presented the possibility of voting by traditional mail, via the Internet, and via SMS or PDA. However, in addition to the lack of legal framework in all three cases, technological, organizational and societal constraints affected the two electronic methods [CG07]. In May 2008, the Parliament of Moldova passed Law 101

[1] Tallinn University of Technology, Ragnar Nurkse Department of Innovation and Governance, Akadeemia tee 3, 12618 Tallinn, Estonia raduantonio.serranoiova@taltech.ee

which adopted the concept of the Automated State Information System 'Elections' and mandated the Central Electoral Commission (CEC) to develop, regulate and implement it, and the Government to finance it, assist the CEC and develop and implement the corresponding legislative frameworks [Mol08]. The system was conceived for the purposes of automating the processes of preparing, conducting and totalizing the results of elections and referendums, with the first focus being the numbering of the votes until the corresponding legal, technical and organizational frameworks were developed and put into place for the rest of the responsibilities[Mol08; VG18]. Since then, many technical building blocks for internet voting were legislated, developed and implemented (due to so many of them being also relevant to the digitalization endeavors of the country, e.g. digital registries, digital identity, identification and signatures, data protection, e-ID cards, e-Government solutions, etc.) [VG18]. However, they still need to be interconnected for an election, and the IVS is also missing. That's where Moldova's Internet Voting Project comes in. In 2019, the CEC's strategic 4-year plan included concrete steps to develop an IVS. In December 2021 a first Interinstitutional Working Group (between govern-mental entities, like the CEC, the Ministry of Justice, the Public Services Agency, among others, and Civil Society Organizations) was created to develop the IVS Con-cept (I-1, I-2). This document includes the description and implementation method of the IVS in the electoral process, defines its basic notions and describes the basic principles that the IVS must follow. It also contains, as an Annex, proposed amendments to the electoral code [Com22]. With the approval of this concept, the CEC was allocated funds by the Parliament by October 2022. A second Interinstitutional Working Group (similar in composition to the first one, except for the Ministry of Justice) was created to oversee the implementation of the IVS, which includes drafting the specifications, contracting the corresponding company that will create the system, and piloting the IVS (I-1). The specifications were unveiled for public consultation in March of 2023. As of the writing of this short paper, the final specifications have not been published, and no progress appears to have been made in the search for the corresponding vendor to create and pilot the IVS.

3 Methodology

Data collection for this short paper took place between January and May 2023. During this period, multiple visits were conducted to Chisinau. Most of the interviews were conducted during these visits, with some in another country, to reach out to Moldova's voting diaspora. A total of 5 semi-structured interviews were carried out with the CEC, representatives of Civil Society Organizations (CSOs), a member of the Moldovan diplomatic corps and a citizen living outside of Moldova (see Table 1). The CSOs interviewed were the ones actively participating in the Interinstitutional Working Groups. The author also attended online two internet voting awareness events that the authorities of Moldova held for their citizens in February and March 2023.

The data was analyzed using an inductive approach consisting of identifying the core components of the Mirabilis of IVS failure (e.g. stakeholders, IVS, project organization,

Number	Occupation	Date
I-1	Deputy Head of the CEC	February 2023
I-2	Representative I of CSO	March 2023
I-3	Representative II of CSO	March 2023
I-4	Moldovan Ambassador	March 2023
I-5	Citizen outside the country	March 2023

Tab. 1: List of interviewees, anonymized.

context dimensions) and the relationships between them. The Mirabilis of IVS failure was introduced to analyze the failed implementation of Internet Voting Project of the Åland Islands [Da20]. Moldova's Internet Voting Project is still in development and cannot be categorized as a success or failure, yet. The Mirabilis is used as a tool to identify the current pitfalls that are affecting the process and that could still be addressed in time for the successful implementation of internet voting in Moldova.

4 Analysis

The CEC's vision is the adaptation of the Estonian model, i.e. IVS implementation for the whole country (I-1). However, the benefit will be felt primarily by the diaspora (I-1, I-2, I-3, I-4, I-5). The pilot IVS will not have any legal validity, will be conducted outside any electoral cycle and will only be available for those having a valid digital ID and/or signature (I-1). Applying the Mirabilis, the context seems contain multiple pitfalls for IVS implementation. The technological dimension is severely lacking in regard to the national adoption of a digital national ID card and signature. Seven percent of the population is able to identify themselves digitally (I-1), but the cost-benefit does not make it at-tractive to the population [VG18]. Regarding the law dimension, the electoral code does not contain articles on internet voting. A draft of the changes was attached to the IVS Concept, and it is planned to amend it by the time the pilot of the IVS (I-2), but due to the characteristics of the pilot, this step seems like a recommendation and not a necessity. The political dimension is lacking an official attitude toward internet voting. On one hand, the Parliament allocated the budget for the development of the IVS pilot, but on the other, members of the Parliament ignore invitations to workshops and discussions on the topic (I-1, I-2, I-3). On the societal dimension, the level of citizens' trust has not been effectively measured, and it is being put to the test by the war next door (I-4) and the Transnistria breakaway region. Regarding the elephant in the room/Mirabilis, the IVS has not yet been developed. After the completion of the final specifications, a public international bid will be launched to find and select the IVS supplier. The project organization is effectively being managed by the CEC and the Interinstitutional Working Group (I-1, I-2, I-3). The two member CSOs are actively participating in the implementation of the IVS. However, the rest of the stakeholders do not seem to be interested in the process. People only seem interested in elections when one is approaching (I-3, I-4). Nevertheless, the CSOs and the CEC have been actively trying to inform the citizens, via media campaigns and their two public events (I-1, I-2, I-3).

5 Discussion and Conclusion

The context of this whole endeavor is incomplete. All the dimensions are lacking key items that are necessary for the successful implementation of an IVS. If these are ignored, possibly due to this being a pilot IVS and not the real deal, the failure of the pilot would set back or even annihilate any possibility of future IVS implementation in the country. The lacking context also deforms the demands of the stakeholders and might undermine their trust in the electoral process, the IVS and the government. The implementation environment of the IVS pilot seems to be indifferent, with the exception of the people working on it. Politicians, candidates, the media and observers are not willing to be troubled or to be engaged long enough on the topic. Additionally, the requirements for the IVS are primarily coming from the project organization, not from the stakeholders. This might lead to a mismatch between the expectations of the IVS among the stakeholders and the project organization, culminating in a system that does not satisfy the needs of the stakeholders. As it currently stands, there are failures appearing in-between the context and the stakeholders, and them and the project organization. The pitfalls identified should be resolved in a timely manner, since they might lead to the failure of the pilot, and in the long-term, to that of any IVS implementation. Further monitoring of the pilot and future efforts is warranted, to see if Moldova will be able to implement an IVS.

Acknowledgements

The data was collected as part of the MOLDOVA CYBERSECURITY RAPID ASSISTANCE project funded by the European Union and implemented by the e-Governance Academy.

References

[CG07] Ion Cosuleanu and Constantin Gaindric. “Distance voting (e-voting): the ways of its applicability in Moldova”. In: *Computer Science Journal of Moldova* 15.3(45) (2007), pp. 354–380.

[Mol08] Parliament of Moldova. *Law 101/2008 Regarding the Concept of the Automated State Information System Ëlections"*. 2008.

[VG18] Ina Vîrtosu and Ion Guceac. “Democracy at the one-click distance: Is electronic voting the best option for Moldova?” In: *CEE e|Dem and e|Gov Days 2018*. Facultas Verlags- und Buchhandels AG, 2018, pp. 359–372.

[Da20] David Duenas-Cid and al. "Tripped at the Finishing Line: The Åland Islands Internet Voting Project". In: *Electronic Voting. Fifth International Joint Conference, EVote-ID 2020*. Springer International Publishing, Cham, 2020, pp. 33–49.

[Mak21] Kanat Makhanov. *Emigrant Moldova and the Changing Concept of Migration*. In: Eurasian Research Institute website. Last accessed 2023/05/10. 2021.

[Com22] Central Electoral Commission. *Decision 572/2022 Regarding the Concept of the Internet Voting System "e-Votare"*. 2022.

[Mol23] Statistica Moldovei. *Populația*. In: Statistica Moldovei website. Last accessed 2023/05/10. 2023.

Curriculum vitae

Personal data

Name:	Radu Antonio Serrano Iova
Date of birth:	14.05.1991
Place of birth:	Panama City, Panama
Citizenship:	Panamanian, Romanian

Contact data

E-mail:	raduserrano@hotmail.com

Education

2020–2024	Tallinn University of Technology, PhD student, Public Administration, Ragnar Nurkse Department of Innovation and Governance
2017–2019	KU Leuven, Münster University, Tallinn University of Technology, Erasmus Mundus Master of Science in Public Sector Innovation & eGovernance
2013–2016	Universidad del Istmo, Bachelor's Degree in International Business Administration

Language competence

Romanian	Mother tongue
Spanish	Father tongue
English	Fluent
French	Fluent
Italian	Fluent

Professional employment

2018–current	e-Governance Academy, Tallinn, Estonia, Expert in the Cybersecurity Competence Center
2012–current	Panama, Freelance Multilingual Certified Public Translator and Interpreter
2018	European Research Center for Information Systems, Münster, Germany, Graduated Student Assistant
2016–2017	AmCham Panama, Panama City, Panama, Trade Specialist
2016	Ministry of Foreign Affairs of Panama, Panama City, Panama, Protocol & Liaison Officer for the Inauguration of the Expanded Panama Canal
2015	PROINVEX - Ministry of Commerce and Industries of Panama, Panama City, Panama, Investment Promoter
2015	Ministry of Foreign Affairs of Panama, Panama City, Panama, Bilateral Meetings Coordinator for the VII Summit of the Americas
2014–2015	Profesionales Aduaneros S.A., Panama City, Panama, Intern
2013–2014	Ministry of Foreign Affairs of Panama, Panama City, Panama, Foreign Affairs Analyst
2011–2012	Academia Europea, Panama City, Panama, Language Teacher

Elulookirjeldus

Isikuandmed

Nimi:	Radu Antonio Serrano Iova
Sünniaeg:	14.05.1991
Sünnikoht:	Panama City, Panama
Kodakondsus:	Panama, Rumeenia

Kontaktandmed

E-post:	raduserrano@hotmail.com

Hariduskäik

2020–2024	Tallinna Tehnikaülikool, doktorant, avalik haldus, Ragnar Nurkse innovatsiooni ja valitsemise instituut
2017–2019	KU Leuven, Münsteri Ülikool, Tallinna Tehnikaülikool, Erasmus Munduse teaduste magister avaliku sektori innovatsioonis ja e-valitsuses
2013–2016	Universidad del Istmo, bakalaureusekraad rahvusvahelises ärijuhtimises

Keelteoskus

Rumeenia keel	emakeel
Hispaania keel	isakeel
Inglise keel	vaba keelekasutus
Prantsuse keel	vaba keelekasutus
Itaalia keel	vaba keelekasutus

Teenistuskäik

2018–praegu	E-riigi Akadeemia, Tallinn, Eesti, küberturvalisuse pädevuskeskuse ekspert
2012–praegu	Panama, vabakutseline mitmekeelne sertifitseeritud tõlkija ja tõlgendaja
2018	Euroopa Infosüsteemide Uurimiskeskus, Münster, Saksamaa, kraadiõppuri assistent
2016–2017	AmCham Panama, Panama City, Panama, kaubandusspetsialist
2016	Panama välisministeerium, Panama City, Panama, laiendatud Panama kanali avamise protokolli- ja kontaktametnik
2015	PROINVEX – Panama kaubandus- ja tööstusministeerium, Panama City, Panama, investeeringute edendaja
2015	Panama välisministeerium, Panama City, Panama, Põhja- ja Lõuna-Ameerika VII tippkohtumise kahepoolsete kohtumiste koordinaator
2014–2015	Profesionales Aduaneros S.A., Panama City, Panama, praktikant
2013–2014	Panama välisministeerium, Panama City, Panama, välisasjade analüütik
2011–2012	Academia Europea, Panama City, Panama, keeleõpetaja

ISSN 2585-6901 (PDF)
ISBN 978-9916-80173-4 (PDF)