INTERNET POLICY REVIEW

Volume 14 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Lessons from small and highly-digitalised Estonia: Decision-making in the aftermath of cybersecurity crises

Logan Carmichael *University of Tartu*

DOI: https://doi.org/10.14763/2025.3.2028

Published: 13 August 2025
Received: 13 August 2024 **Accepted:** 13 December 2024

Funding: This work was supported by European Union's Horizon 2020 research and innovation program under grant agreement No 857622 "ERA Chair in E-Governance and Digital Public Services — ECePS".
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Carmichael, L. (2025). Lessons from small and highly-digitalised Estonia: Decision-making in the aftermath of cybersecurity crises. *Internet Policy Review*, *14*(3). https://doi.org/10.14763/2025.3.2028

Keywords: Cybersecurity governance, E-governance, Estonia, Crisis management, Cybersecurity management

Abstract: As governments across the world increasingly undergo digitalisation processes, ensuring cybersecurity of these provisions cannot be 100% guaranteed. How, then, can governments best respond to a cybersecurity crisis in order to bolster cybersecurity in the future? Even Estonia, one of the earliest and most pervasive examples of e-governance globally, has not been without cybersecurity crises. Using four key Estonian examples, this paper examines the components of government decision-making in the aftermath of cybersecurity crises, which aim to bolster future cybersecurity. Three key approaches emerged from the crises examined: 1) decision-making is derived from prior knowledge and experience; 2) communications around cybersecurity crises is clear, coordinated, and transparent; and 3) innovation and planning should take place in times of non-crisis, as crises often expedite decision-making. Ultimately, this paper offers insight into how governments can make decisions following cybersecurity crises, in contexts beyond Estonia, as they undergo digitalisation processes and increasingly face cyberattacks.

Introduction

Across the world, governments are increasingly digitalising their service provisions, a process that has been ongoing over recent decades but was expedited in many places with COVID-19 lockdown restrictions (Härmand, 2021; Carmichael, 2021). At the same time, cyberattacks and other malicious activity in cyberspace have been increasing in frequency, sophistication, and severity, with targets across myriad sectors, including governments (see, for example, Tasheva, 2021; Pranggono and Arabo, 2020). Thus, the topics of cybersecurity and e-governance have become increasingly intertwined, with conversations around how digitalised provisions should be secured becoming an inherent and crucial part of the digitalisation process. Despite proactive measures to enhance cybersecurity, crises – broadly, 'disruptive' events with the elements of threat, urgency, and uncertainty – in the cyber domain can, and do, still eventuate (Boin et al., pp. 5-7). Thus, this paper addresses the following core question: how can governments, and their ministries and agencies responsible for cybersecurity, respond in the aftermath of a cybersecurity crisis, in order to bolster the future cybersecurity of their digitalisation initiatives?

Estonia, a nation of 1.3 million people on the southern shores of the Baltic Sea, is an illuminating case in both the study of e-governance and cybersecurity. This is because of its early and pervasive adoption of e-governance practices, including electronic identification (eID) and nationwide internet voting (i-voting) dating back to the early 2000s (Alvarez et al., 2009; Vassil et al., 2016). The country also faced one of the earliest instances of a publicly-acknowledged DDoS cyberattack on a nation-state in 2007, and crafted new legislation and governance structures in its aftermath, predating most of its counterparts globally. Although deemed a global leader in this space, Estonia has not been without cybersecurity crises, even those impacting its e-governance model. This paper looks at four key crises in the Estonian experience with e-governance and its cybersecurity: the aforementioned 2007 DDoS cyberattacks, impacting government, news media, and banking sites; the 2017 'eID' crisis where a vulnerability in eID cards was discovered; the COVID-19 pandemic, and the cybersecurity realities associated with a public health crisis and lockdowns; and the 2022 Russian full-scale invasion of Ukraine, which coincided with cyberattacks against Ukraine's allies. Though the latter two events are not uniquely cybersecurity crises, they did come with unique new cybersecurity realities, and along with the former two events, meet the criteria set forth in crisis management literature to constitute a crisis, in order to observe the evolution of decision-making on said topics in the Estonian government.

The Estonian case demonstrates the importance of learning from experiences, growth, and continuous improvement to cybersecurity mechanisms, especially in an instance of such pervasive digitalisation. There was a time when Estonia was a unique case purely because of the existence of its e-governance structure, but today, other countries have 'caught up' in the digitalisation process. As an earlier adopter of e-governance and, in turn, cybersecurity practices, when faced with crises in these spaces, Estonia often found itself crafting new responses, rather than following global precedent that did not yet exist, given that governments did not typically publicly acknowledge cyberattacks at that time. Thus, the value of the Estonian case lies in its maturity, continuing to learn from the cybersecurity challenges that can befall digitalised provisions. As other governments, at various levels of governance, are embarking on the earlier stages of digitalisation and associated cybersecurity considerations, they stand to learn from the Estonian experience, where the government has been grappling with the topics of cybersecurity surrounding digitalised provisions for more than fifteen years, arguably leading to a more secure e-governance system over time.

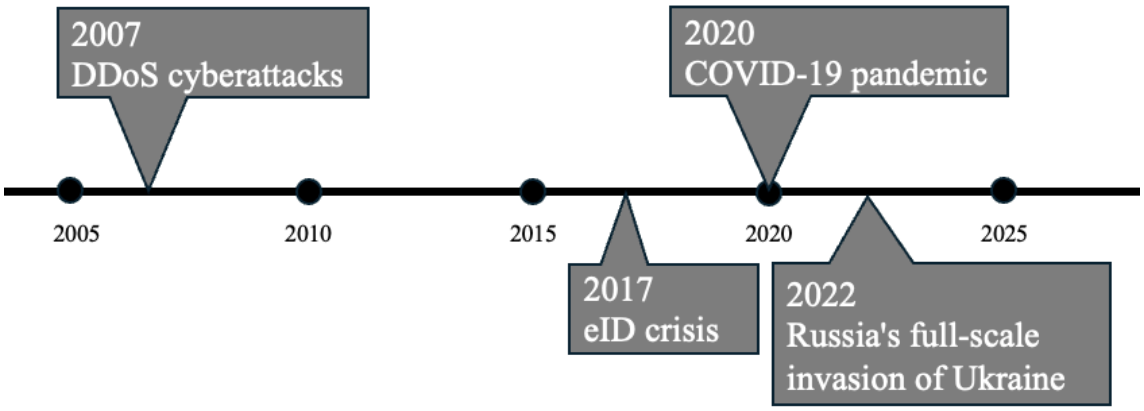

FIGURE 1: Estonian cybersecurity crises examined in this paper.

State of the art

While 'crisis' can be described as a "broad term related to disruptions of some kind" (Coombs et al., 2019, p. 31), then crisis management is "a set of factors designed to combat crises and to lessen the actual damage inflicted by" them (Coombs, 2018, p. 1). In their foundational work on political crisis management, Boin and colleagues (2017) acknowledge the wide range of domains – including terrorism, natural disasters, and humanitarian emergencies – in which crises have been experienced over prior decades (p. 1). Furthermore, crisis management scholarship has

proposed a number of different models for crises themselves and for carrying out crisis management. This has included Boin and colleagues' (2017) criteria for determining what constitutes a crisis; these specific criteria, utilised in this paper, are outlined in greater detail in the following section. Further models in crisis management have included Pearson and Clair's (1998) model of the crisis management process, with focus on the environmental context, individual and collective reactions, situated before and after a triggering event, respectively (p. 66). More recent work from Jin et al. (2023) proposed a 'readiness' model, as a multi-level approach to threats, risks, conflicts, crises, and sticky crises, to bolster preparedness (pp. 4-5). The crisis management model most relevant to this paper is Jaques' (2007) relational model of crisis management, which clusters parts of the crisis management process into four parts, situated before, during, and following a crisis (pp. 150-151). The approach to crisis response undertaken in this paper corresponds to what Jaques (2007) calls 'post-crisis management,' namely, the recovery and business resumption, post-crisis issue impacts, and evaluation and modification (p. 150). As with the crises criteria aforementioned, further detail on this approach will be elaborated upon in the following section.

According to Boin et al. (2017), cybersecurity represents a new domain in which crisis management can be studied (p. 3). As a result, there is a limited but emerging body of literature in the particular field of cybersecurity and crisis management. Various works apply elements of the broader study of crisis management into the cyber arena. In earlier literature, Areng (2013) looked at international mechanisms for broaching cyber crises, especially *vis-à-vis* more 'traditional' toolkits for crisis management. Boeke (2017) similarly articulated that states struggle to adapt existing institutional structures to cope in instances of cyber crisis, using the cases of Estonia, Denmark, the Netherlands, and the Czech Republic. Conversely, Backman (2020) looked at cyber crisis as fitting within broader trans-boundary crisis literature. Collier (2017) examined governmental institutional structure for crisis, NGO involvement, and international initiatives.

The Estonian cyberattacks of 2007 provided a case study in several of these articles, including Areng, Boeke, Backman, and Collier, while the latter two have compared Estonian and United Kingdom cyber crisis response. Boeke (2017) acknowledges that Estonia has been a pre-eminent case study in cyber crisis management, indeed as one of the first such instances of a state needing to develop a response to a cyber crisis; this article also adopts such reasoning. Divergent from this common case study, the work of Østby and Katt (2019) proposes a model of role distribution in cyber crisis management, compared side-by-side with conventional crisis

management roles, using municipal-level governance in Norway as their case. In work examining the components that shape institutional definitions of cybersecurity, Fichtner (2018) asserts that approaches can be shaped by threats, assets protected, measures or policies utilised, and responsibilities given to particular actors, all governance approaches built upon in this paper.

In the Estonian context, typically literature broaches the topics of digital governance or cybersecurity, with only a limited number of works examining these topics together. For example, scholars such as Ernsdorff and Berbec (2007), and Kitsing (2008) looked at the early development and success of Estonian e-governance. More recent work from scholars including Kerikmäe et al. (2019), Solvak et al. (2019), and Stephany (2020) have looked at nuanced aspects of Estonian e-governance, such as public perceptions, adoption rates, and elements influencing the success of the Estonian model. Estonian cybersecurity has been studied as an example of a global norm-setter (Crandall and Allan, 2015), while specific attention has been paid in several works to the 2007 cyberattacks: the political decision-making and legal reforms that followed, as well as rhetoric surrounding whether this represented an instance of cyber warfare, by scholars including Czosseck et al. (2011), Herzog (2017), and Rid (2017). Early literature on the study of cybersecurity and the Copenhagen School of thought outlined the "systemic threats" in the process of securitising digital systems, encompassing critical infrastructures and a broad range of digitalised provisions, a precursor to e-governance (Hansen and Nissenbaum, 2009, pp. 1160-1161). Works on e-governance and cybersecurity, together, in Estonia, have come from Paršovs' (2020a; 2020b) and Skierka's (2023) studies of the 2017 eID crisis, a crisis also explored in this paper. This paper aims to make a theoretical and conceptual contribution at the nexus of these three core strains of literature: crisis management, cybersecurity governance, and e-governance. As such, it contributes to the emerging literature examining crisis management specifically in the domain of cybersecurity and its governance; it does so by looking at crisis responses as they affect e-governance provisions, specifically drawing from a mature Estonian context, albeit one with useful applicability to crisis management, cybersecurity, and digitalisation contexts globally.

Theoretical and conceptual background

Empirically, this paper employs a historical institutionalist theoretical approach, as a useful means to view governance and decision-making in the wake of cybersecurity incidents affecting the Estonian digital governance structure, though methodologically, it takes a constructivist approach, valuing experiences and ideas derived

from government officials' encounters with crisis. Together, these theoretical groundings frame the topics of cybersecurity and digital governance in an Estonian context through institutional path dependencies over time, with cybersecurity crises as critical junctures to study, deriving findings based on the experiences and ideas from decision-makers at the forefront of these junctures. Mahoney et al. (2016) define critical juncture as "a relatively short period in time during which an event or set of events occurs that has a large and enduring subsequent impact" (p. 77). Indeed, these concepts play a prominent role in historical institutionalist scholarship, as indicated by Fioretos et al. (2016) that critical junctures mark the start of path-dependent processes, whereby future outcomes, decisions, or processes are a result of those that came before them (p. 9).

The approach to historical institutionalism employed in this paper specifically draws upon Pierson and Skocpol's (2002) idea that historical institutionalists must look to critical junctures and long-term processes, to understand "overarching contexts and interacting processes that shape and reshape states, politics, and public policmaking [sic]". In employing this approach, this paper examines cybersecurity crises as critical junctures, and the 'markers' of path dependencies aforementioned, to look at how governance processes surrounding cybersecurity have been shaped and impacted over time. Here, the four key crises have been selected as useful and illustrative to study, and their particular relevance and applicability is outlined in greater detail below. This article looks less so at the crises themselves, but rather from a governance perspective, looking at how political decision-making was undertaken in the aftermath of said crises to further improve the security underpinning Estonia's digital infrastructure. While, in the broader context of the study of critical junctures in historical institutionalism, the 15-year time period of this project is relatively short, considering how recently cybersecurity and digital governance have developed, this approach is justified given that this comprises most of the history of these topics studied here. Crises in the domains of cybersecurity and digital governance in Estonia have tended to involve and impact various actors across the political landscape and society; thus, these crises in the Estonian context are particularly illuminating critical junctures for the study of governance processes undertaken in response.

This paper employs a comprehensive definition of cybersecurity, encompassing the security of technological systems and software, free of manipulation or disruption, and the protection of information contained in these systems from alteration, corruption, deletion, unauthorised access, or dissemination (Craigen et al., 2014). Thus, cybersecurity governance is the institutional and organisational structure

and decision-making related to cybersecurity, as aforementioned (Urgessa, 2020; Von Solms and Von Solms, 2018). This paper derives its terminology of e-governance from the work of D'Agostino et al. (2011), and Bannister and Conolly (2012), assuming an 'interactive dynamic' between the government and citizenry, and a fundamentally digitalised model of governance differing substantively from its analogue predecessors.

Specifically, this paper draws its definition and criteria for a crisis from Boin et al. (2017) in *The Politics of Crisis Management,* a second edition that has been updated to include cyberattacks in a list also encompassing natural disasters, terror attacks, and collapses of financial systems. They write that such crises "routinely shatter the peace and order of societies" testing governance today (p. 3). They set forth the key criteria of a crisis as threat, a "sense that the core values or life-sustaining features of a system have come under *threat,*" urgency (although this is typically socially constructed and can be used instrumentally, i.e. urgency as a tool in a hostage situation, and can vary by proximity to the crisis), and uncertainty, a lack of clarity about what will happen next (pp. 5-7). Furthermore, while these crises meet the criteria set forth by Boin et al., the particular crisis management response studied in this paper correlates with the "post-crisis management" cluster of Jaques (2007) relational model of crisis management (p. 150). The 'critical function' of this post-crisis cluster is "looping back to and preparing for and managing future crises," by looking at: 1) recovery and business resumption (in this case, of e-governance processes in particular), 2) post-crisis issue impacts, and 3) evaluation and modification, all of which align with the core research question of this paper, focusing on post-crisis learning to bolster future cybersecurity surrounding digitalisation (Jaques, 2007, p. 150).

This paper uses four cases, representing critical junctures in the overall cybersecurity and e-governance history of Estonia; they also all meet the criteria of a 'crisis' set forth by Boin et al. These cases were initially selected based on a review of literature and examined *vis-à-vis* yearly government reports on cybersecurity. This was further validated when interviewees were asked about crises that should be studied, indicating that these were the pre-eminent crises impacting Estonian e-governance throughout its history, though some did refer to external crises that were also impactful. Ultimately, interviewing indicated common themes across these crises: building upon prior knowledge and experiences, clear and transparent communications, and crisis as an expeditor of change, thus necessitating innovation in times of non-crisis.

2007 cyberattacks

Estonia shares a complex and tense relationship with its much larger neighbour, Russia; the country was occupied by the Soviet Union during the Second World War and did not regain independence until 1991. One key historical legacy is an often-wary and 'securitised' relationship between the country's ethnically-Estonian majority and its Russian minority (Jašina-Schäfer and Cheskin, 2019, pp. 1-2). Thus, after the removal of a controversial Soviet-era monument from central Tallinn in April 2007, violent political protest erupted, resulting in one death, followed by three weeks of distributed denial-of-service (DDoS) cyberattacks on news media, banks, and government and politicians' websites (Ehala, 2009; BBC News, 2007). These cyberattacks threatened the functioning of government websites, some digital services, and banking services; though there was less digitalisation than today, functionality was certainly significantly impacted. There was a sense of urgency to bring these websites back online, as they were crucial to the effective functioning of services. Furthermore, there was uncertainty about how and when the cyberattacks would end, and how an investigation and attribution could occur, especially as the cyberattacks reached a peak on 9 May 2007, Victory Day, and as the Russian government refused to cooperate (Pernik, 2018, p. 57; STRATCOM Centre of Excellence, 2019, pp. 52, 58).

2017 eID crisis

In the summer of 2017, Czech researchers found a return-of-the-coppersmith (ROCA) cryptographic key generation vulnerability in approximately two-thirds of Estonian eID cards, alongside technologies used in other countries including Austria and Spain (Nemec et al., 2017). This posed a major security threat, as the eID cards represent a core means for authentication within the Estonian e-governance system, and this unpatched vulnerability could be exploited by malicious actors at any time for myriad nefarious purposes. Indeed, Skierka (2023) maintains that electronic identification is "an indispensable pillar of Estonia's digital society," with heavy dependence across Estonian society for access to public and private digital services and digital signatures; "its failure would have dramatic consequences for Estonia's 'e-state' and large parts of society" (p. 2). There was urgency to find a patch to the vulnerability, and to deliver messaging to the general public, especially considering that local elections were coming up, for which eID was vital for voter authentication. Uncertainty existed up until the moment that a patch was developed, as the eID cards, and some of their functions, including elections, could be manipulated by malicious actors.

2020 COVID-19 pandemic

With lockdowns onset by the spread of the COVID-19 virus, traditionally in-person interactions worldwide moved online very rapidly. At this time, there was a global increase in instances of cyberattacks (Saleous et al., 2023; Interpol, 2020). Though Estonian government services were highly digitalised before the pandemic, many adjustments – such as a move toward online education and real estate transactions – were necessary and had associated cybersecurity concerns. There was a threat to existing e-governance provisions as cyberattacks experienced an increase globally, compounded with the necessity of new e-services resulting from the pandemic, which needed to incorporate security parameters. Additionally, there was urgency to move online in the earliest days of the pandemic in order to stop the spread of the COVID-19 virus itself, but also to have necessary digital provisions in place, securely. There was also uncertainty surrounding the COVID-19 virus and the range of sociopolitical ramifications it may have in the long and short term, as well as how digital provisions could serve as a potential solution to these concerns.

2022 Russian full-scale invasion of Ukraine

After eight years of warfare in the Donbas region of eastern Ukraine, Russia launched a full-scale invasion of the country on 24 February 2022. Russia has long experimented with its offensive cyber capabilities on Ukraine, but has also targeted Ukraine's allies, including Estonia (Baezner, 2018, p. 41; Greenberg, 2019). There emerged a threat to Estonia and its Baltic neighbours through much of 2022, via DDoS attacks on various critical systems, often coinciding with political events to which Russia objects (RIA, 2023). There was urgency for the cyberattacks to be repelled in a timely manner, especially as they impact digitalised governmental provisions and other critical systems, whether in the public or private sector. Furthermore, there was uncertainty around the broader landscape of Russia's war in Ukraine, its use of hybrid tactics, and employment of cyberattacks targeting Estonia and its allies moving forward.

TABLE 1: Defining significant cybersecurity crises affecting e-governance in Estonia.

EVENT	WHAT HAPPENED	THREAT?	URGENCY?	UNCERTAINTY?
2007 CYBERATTACKS	REMOVAL OF A CONTROVERSIAL SOVIET-ERA MONUMENT, RESULTING IN POLITICAL VIOLENCE AND THREE WEEKS OF DISTRIBUTED DENIAL-OF-SERVICE (DDOS) CYBERATTACKS ON NEWS MEDIA, BANKS, AND GOVERNMENT WEBSITES.	*THREAT* TO THE FUNCTIONING OF GOVERNMENT WEBSITES, SOME DIGITAL SERVICES, AND BANKING SERVICES.	*URGENCY* TO BRING THESE WEBSITES BACK ONLINE, AS THEY WERE CRUCIAL TO THE EFFECTIVE FUNCTIONING OF VARIOUS DIGITAL SERVICES,	*UNCERTAINTY* ABOUT WHEN THE CYBERATTACKS WOULD PEAK, WHEN THEY WOULD END, AND HOW AN INVESTIGATION AND ATTRIBUTION OF THE CYBERATTACKS COULD OCCUR.
2017 EID CRISIS	CZECH RESEARCHERS FOUND A RETURN-OF-THE-COPPERSMITH (ROCA) CRYPTOGRAPHIC KEY GENERATION VULNERABILITY IN APPROXIMATELY TWO-THIRDS OF ESTONIAN EID CARDS.	SECURITY *THREAT* TO ESTONIAN ELECTRONIC IDENTIFICATION; UNPATCHED VULNERABILITY COULD BE EXPLOITED BY MALICIOUS ACTORS FOR NEFARIOUS PURPOSES.	*URGENCY* TO FIND A PATCH TO THE VULNERABILITY, DELIVER MESSAGING TO THE GENERAL PUBLIC, AND DO SO QUICKLY, WITH LOCAL ELECTIONS REQUIRING EID FOR AUTHENTICATION UPCOMING.	*UNCERTAINTY* UP UNTIL THE MOMENT THAT A PATCH WAS DEVELOPED, AS THE EID CARDS, AND SOME OF THEIR FUNCTIONS, INCLUDING ELECTIONS, COULD BE MANIPULATED BY MALICIOUS ACTORS.
2020 COVID-19 PANDEMIC	GLOBAL ONSET OF LOCKDOWNS, WHICH COINCIDED WITH A GLOBAL INCREASE IN INSTANCES OF CYBERATTACKS. ESTONIAN GOVERNMENT SERVICES WERE HIGHLY DIGITALISED EVEN BEFORE THE PANDEMIC, NEW E-SERVICES ALSO EMERGED AND HAD ASSOCIATED	*THREAT* TO EXISTING E-GOVERNANCE PROVISIONS AS CYBERATTACKS EXPERIENCED AN INCREASE GLOBALLY, COMPOUNDED WITH THE NECESSITY OF NEW E-SERVICES DURING THE PANDEMIC, WHICH NEEDED TO INCORPORATE	*URGENCY* TO MOVE ONLINE IN THE EARLIEST DAYS OF THE PANDEMIC IN ORDER TO STOP THE SPREAD OF THE COVID-19 VIRUS, BUT ALSO TO HAVE NECESSARY DIGITAL PROVISIONS IN PLACE, SECURELY.	*UNCERTAINTY* SURROUNDING THE COVID-19 VIRUS ITSELF, AND THE RANGE OF SOCIOPOLITICAL RAMIFICATIONS IT MAY HAVE IN THE LONG AND SHORT TERM, AS WELL AS HOW DIGITAL PROVISIONS COULD LESSEN THESE ISSUES.

	CYBERSECURITY CONCERNS.	SECURITY PARAMETERS.		
2022 RUSSIAN FULL-SCALE INVASION OF UKRAINE	RUSSIA LAUNCHED A FULL-SCALE INVASION OF UKRAINE ON 24 FEBRUARY 2022. RUSSIA HAS LONG EXPERIMENTED WITH ITS OFFENSIVE CYBER CAPABILITIES ON UKRAINE, BUT HAS ALSO TARGETED UKRAINE'S ALLIES, INCLUDING ESTONIA.	*THREAT* TO ESTONIA AND ITS BALTIC NEIGHBOURS THROUGH MUCH OF 2022 AND EARLY 2023, VIA DDOS ATTACKS ON VARIOUS CRITICAL SYSTEMS, OFTEN COINCIDING WITH POLITICAL EVENTS TO WHICH RUSSIA OBJECTS.	*URGENCY* FOR THE CYBERATTACKS TO BE REPELLED IN A TIMELY MANNER, ESPECIALLY AS THEY IMPACT DIGITALISED GOVERNMENTAL PROVISIONS, OR OTHER CRITICAL SYSTEMS, WHETHER IN THE PUBLIC OR PRIVATE SECTOR.	*UNCERTAINTY* AROUND THE BROADER LANDSCAPE OF RUSSIA'S WAR IN UKRAINE, ITS USE OF HYBRID TACTICS, AND EMPLOYMENT OF CYBERATTACKS AND TARGETING OF ESTONIA MOVING FORWARD.

Methodology

This paper uses qualitative research design, consisting of semi-structured expert interviews with decision-makers at the time of these key junctures (Bogner et al., 2009). Prior literature outlines the valuable interpretive and procedural knowledge provided by experts and its relevance to social and political sciences research (Littig, 2009, p. 99), and as generating important insights "about the 'what' and 'how' of political processes and events" (Von Soest, 2022, p. 284). A great deal of political science scholarship employing qualitative interviews focuses on elites rather than experts (Von Soest, 2022, p. 278). However, here the interviewees arguably constitute both, as the government elite who "occupy top positions in… political structures" and "exercise significant influence" including over decision-making (Hafner-Burton et al., p. 369), while expertise is "based on real knowledge" (Von Soest, 2022, p. 278). Indeed, this overlap of experts and elite is acknowledged in the work of Littig (2009, p. 108). These interviewees were both responsible for decision-making at the times of crisis examined in this paper, as well as possessing expertise in the emerging domain of cybersecurity necessary to undertake that decision-making in the first place. As such, the interviewees constitute 'inside' experts, those "decision makers who actually shaped the political or social process of interest," in this case, cybersecurity governance and policy processes, whose main advantage is their direct participation in such processes (Von Soest, 2022, p. 279).

These interviews have, firstly, been triangulated against each other, as the intervie-

wees came from different parts of the Estonian government, and thus, different segments of the governance process in relation to the crises examined. Furthermore, the interviews have been triangulated with official government messaging, news reportage, and political and public discourse. Interviewees were determined initially via purposive sampling, following preliminary research to determine decision-makers; as interviewing ensued, I used snowball sampling, as interviewees suggested other decision-makers whom I could interview (Turner, 2010). I conducted ten interviews with Estonian government officials between November 2022 and April 2023. The interviewees came from key decision-making entities across the Estonian government between 2007 and 2022, including the Ministry of Economic Affairs and Communications (MKM), Ministry of Defence (MOD), State Information System Authority (RIA), Central Election Committee, and Presidency of Estonia. Given the smallness of the Estonian state, its government, and cybersecurity community, ten interviewees represented a sizable cross-section of the personnel in decision-making positions at the time of these crises.

Additionally, Estonian cybersecurity and e-governance personnel have moved around between the public and private sector throughout the time period of focus; while this enriched my paper for the varied perspectives on decision-making that it provided, it also made it difficult at times to determine where a former decision-maker is currently situated. However, given that the cybersecurity and e-governance communities in Estonia are tight-knit, previous interviewees often provided personal introductions or referrals, as an overwhelmingly effective means of overcoming this potential limitation. This community is, naturally, limited in the government of a small country and therefore, there was not a large number of responsible decision-makers whom I could speak with. While there remained a small number of decision-makers who did not respond to a request for an interview, I reached a saturation point where, by the end of the interviewing period, the same or similar ideas were arising again and again.

Before participating in an interview, all interviewees were sent a questionnaire; interviewees were then able to select which blocks of questions covered crises over which they had purview in a decision-making capacity. The questionnaire followed the same structure for each of the four crises: 1) what was the interviewee's role in decision-making at the time of the crisis, 2) what responses were undertaken in the aftermath of the crises, 3) how was this response arrived upon, and 4) what alternative responses were considered but not undertaken. Follow-up questions and clarifications were sought where necessary throughout the interviews. Interviewees were also asked to sign an informed consent form, consenting for the an-

swers of their interview to be used in this paper, and selecting whether they wished to remain anonymous. Four interviewees consented to be quoted by name in this paper, while six interviewees requested to be identified by their position (or former position). The interviews were conducted in-person, where possible, and online via video-calling. For the former, interviews were recorded using a voice recorder and uploaded to a secure online storage platform; for the latter, interviews were recorded using the video-calling platform's recording function and uploaded to a secure online storage platform. All interviews were then transcribed, with the original recording deleted.

As outlined above, the interviewing process was undertaken in line with ethical considerations surrounding interviews in qualitative research (King, Horrocks, and Brooks, 2019, pp. 33-35), while consent was obtained and data handled in compliance with Estonian research ethics guidelines (University of Tartu, 2017). Subsequently, the transcripts were coded using a concept-driven 'coding down' approach, initially employing descriptive coding followed by interpretive coding to cluster topical ideas (King et al., 2019, p. 204). This coding was intended to 'specifically name' and 'systematically connect' the concepts and processes examined in the interviews (Strauss and Corbin, 1998, p. 176). An initial code book was derived with a first layer devoted to each of the four crises, in addition to 'external crises' that shaped Estonian cybersecurity preparedness, an idea that emerged during interviewing. Subsequently, a second layer of codes was devoted to the outcomes of each respective crisis; for example, with the 2007 cyberattacks, nine codes were devoted to developments including 'initial cooperation with banks and private entities,' 'physical security during Bronze Night political violence,' 'national cybersecurity strategy,' and 'cybersecurity governance structures.' This process was repeated for each crisis. However, a third layer derived common themes amongst these crises; namely, 1) building upon prior knowledge, 2) transparent and coordinated communications, and 3) crisis as an expeditor of policy or other related initiatives. These multiple layers of coding were intended to align with the research question, as well as the crises selected for this paper, and the governance outcomes of said crises.

Some possible limitations in interview data did arise due to the timeframes examined in this paper, given the amount of time that has passed since 2007; however, in most instances it is possible to triangulate the events described in interviews with publicly available information. Overall, given the small size of Estonia and its government, there were a small number of possible decision-makers who could be interviewed for this paper. Furthermore, these interviewees represent an elite

cross-section of responsible decision-makers within the Estonian government, but given that the paper's focus is on governance and decision-making processes, these decision-makers were the most appropriate respondents to gain the insights sought in this paper. These interviewees represented a sizable cross-section of personnel responsible for responses to the crises examined in this paper, and as previously mentioned, a saturation point was reached amongst interviewees, whereby similar ideas arose repeatedly across the interviews. Thus, efforts were made to address these potential limitations as much as was possible.

Analysis

2007 cyberattacks

Interviews with decision-makers across the Estonian government at the time of the 2007 cyberattacks revealed an extensive list of responses in the immediate and longer-term aftermath of this crisis. The newness of a DDoS attack targeting the public and private sector of a country so pervasively was unprecedented and prompted various initial responses (Herzog, 2017, pp. 67-68). Generally, respondents outlined a lack of access to vital governmental services and web pages, or the defacement of government web pages, and lack of access to the services of the private sector, namely banks (Former cybersecurity official, interview, n.d.; former electoral official, interview, n.d.). This is reflected in both news reporting from the time of the cyberattacks and existing scholarship surrounding the event (BBC News, 2007; Czosseck et al., 2011).

The government faced choices surrounding messaging: at this time, there was little precedent for communications surrounding a cyberattack. While the initial debate posited that the Estonian government admitting to facing cyberattacks could be "embarassing" or "detrimental" to its international image, the decision was ultimately made to publicise the cyberattacks (Former cybersecurity official, interview, n.d.; Former senior MOD official, interview, n.d.). The result was a transparent approach to government messaging, which has been employed by the Estonian government in subsequent cyber crises ever since. Ultimately, the cyberattacks proved a uniting crisis: respondents noted that the 2007 cyberattacks themselves were not divisive amongst government officials, contrary to the broader political events within which they took place; rather, the cyberattacks prompted significant collaboration between government and the private sector (Former senior MOD official, interview, n.d.).

After the cyberattacks abated, it became apparent that new governmental struc-

tures and strategies for tackling cyberattacks were necessary moving forward. The MOD took the lead on developing a cybersecurity strategy, whereby ministerial responsibility for cybersecurity should preeminently be a civilian rather than military task, and the MOD would allocate this primary responsibility to the MKM (Former senior MOD official, interview, n.d.; former cybersecurity official, interview, n.d.). The outcome was the first Estonian National Cybersecurity Strategy, published in 2008 and one of the first of its kind globally; to reconfigure governance structures overseeing cybersecurity inside the Estonian government; and to collaborate more closely with the private sector. Multiple respondents pointed out that the shift in cybersecurity purview empowered both RIA and the Estonian Computer Emergency Response Team, CERT (Former RIA official, interview, n.d.; former cybersecurity official, interview, n.d.; L. Areng, interview, n.d.; former senior MOD official, interview, n.d.). RIA, home to some of the most knowledgeable technical personnel, became situated under MKM, and became mandated to conduct audits on other entities within the Estonian government, to ensure compliance with cybersecurity requirements (Former senior MOD official, interview, n.d.).

Several respondents also noted that the 2007 cyberattacks prompted the creation of the Cyber Defence League (now the Cyber Unit of the Estonian Defence League), and opened up myriad new educational and training pathways for cybersecurity. The latter resulted in the first cybersecurity Masters programmes at Tallinn Technical University and the University of Tartu, with resourcing from the MOD and, later, the Ministry of Education (former RIA official, interview, n.d.; former government cybersecurity official, interview, n.d.; L. Areng, interview, April 3, 2023; former MOD official, interview, n.d.). Another major outcome of the 2007 cyberattacks, mentioned by almost all of the respondents, was the establishment of the NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn in 2008 (Former electoral official, interview, n.d.; former MOD official, interview, n.d.; T.H. Ilves, interview, March 14, 2023). Respondents pointed out that the idea for the CCDCoE to be based in Tallinn had begun three years prior to the cyberattacks, but suggested that the cyberattacks garnered support for this idea to actualise (T.H. Ilves, interview, March 14, 2023). The CCDCoE's main aims are to provide "cyber defence research, training and exercises covering the focus areas of technology, strategy, operations and law" to NATO allies and their partners, with research and cyber training exercises taking place in Estonia (Cooperative Cyber Defence Centre of Excellence, n.d.).

Reflecting on the overall process of post-2007 cyberattacks decision-making, a former Ministry of Defence official (interview, n.d.) noted that there were 'lessons

learned' papers crafted internally, but weren't released publicly, like in some later cybersecurity crises. This instigated a process of governmental introspection that would derive lessons for future cybersecurity crises.

eID crisis

Interviews with decision-makers within the Estonian government at the time of the eID crisis showed that the initial decision-making response was threefold: developing internal communications on the topic, crafting public messaging, and working on establishing and deploying a patch to the vulnerability. After being informed by Czech researchers of the vulnerability, which existed in the chip cards used not only in Estonia, but elsewhere in Europe, communications began between RIA, whose knowledge of the technology underpinning eID was the most sophisticated; the Police and Border Guard, who issued the card; and Gemalto, the private company that produced the physical smart card (Former RIA official, interview, n.d.; T. Peterkop, interview, April 3, 2023). The initial response included RIA's endeavour to establish a patch to the vulnerability, as well as internal attempts from RIA personnel to exploit the vulnerability themselves, and monitoring the dark web to see if an exploit emerged (T. Peterkop, interview, April 3, 2023). Though the vulnerability was not exploited, an exploit was ultimately found to be sold on the dark web after the decision was made to suspend certificates on the vulnerable ID cards (T. Peterkop, interview, April 3, 2023).

Firstly, it was determined that the government would take a clear and coordinated approach to their communications on the crisis; RIA communications personnel crafted the term "transparent risk management" to describe their approach (Former RIA official, interview, n.d.). Ultimately, then-Prime Minister Jüri Ratas became the spokesperson for the government in this crisis, beginning with a press conference six days after the vulnerability was disclosed by Czech researchers. Though there were some alternative courses of action suggested, one being that the head of the Police and Border Guard deliver the messaging, ultimately it was deemed a "political decision" for Ratas to take on this role (Peterkop, interview, April 3, 2023). Messaging was selected carefully, attempting to frame the crisis in an understandable and accessible manner for the general population, to maintain the public's trust in the government and the technology (Former RIA official, interview, n.d.). Respondents from across the Estonian government applauded Ratas' response as visible, transparent, and explained the situation in a palatable way, while simultaneously taking the situation seriously (Former cybersecurity official, interview, n.d.; former MOD official, interview, n.d.). While the Estonian government faced criticisms or concerns with other aspects of the eID crisis, such as internet voting out-

lined below, the response to the government's communications strategy was overwhelmingly positive. One Estonian journalist, Aivar Pau, was particularly critical of the communications response at the time of the eID crisis, claiming it sowed panic that was 'unjustified' (Pau, 2017a; Pau, 2017b). However, Pau's works have been rebutted by the likes of former Entrepreneurship and IT Minister Liisa Oviir and former President Toomas Hendrik Ilves, who maintained that informing the public of a cybersecurity crisis is a natural course of action, while a government cover-up of the crisis would have been a far worse option (Oviir, 2017; Beltadze, 2017). This is reflected in scholarship on the eID crisis as well (Skierka, 2023, p. 4; Ventsel and Madisson, 2019, pp. 136-137).

A further concern that arose was internet voting, as local elections were upcoming in October 2017, and eID cards were a key tool for verifying and authenticating voters. A former electoral official (interview, n.d.) noted that some inside the Estonian government advocated against the use of internet voting in the 2017 local elections, but these ideas were dismissed rather quickly. A former senior cybersecurity official (interview, n.d.) noted that there was less concern about compromised electoral integrity as a result of the vulnerability, but rather, other forms of manipulation – ie. financial exploitation – prior to the deployment of a patch. Several respondents pointed out the eID was not "an exclusive e-service" for the purpose of authentication, that other methods of government-authorised identification could be used or that voters could vote in-person on-paper (Former MOD official, interview, n.d.; former cybersecurity official, interview, n.d.; Peterkop, interview, n.d.). Despite concerns that i-voting turnout would decrease significantly with the eID crisis, the overall level of voting and i-voting usage did not fundamentally change during the 2017 local elections (Valimised, n.d.).

Ultimately, by late October and early November of 2017, patches to the vulnerability were developed, tested, and deployed, albeit with some eventual queues to receive new ID cards and some online glitches (Former RIA official, interview, n.d.). Overall, respondents considered this to be a successful response to a cybersecurity crisis, as the vulnerability was not exploited before a patch was deployed, and also from a communications standpoint. Multiple respondents indicated that the precedent of clear and transparent messaging around a cybersecurity crisis was derived from the 2007 cyberattacks (Former cybersecurity official, interview, n.d.; T. Peterkop, interview, April 3, 2023). Beyond the experience gained from the 2007 cyberattacks, one respondent noted that there was preparedness for such a crisis derived from regular cybersecurity exercises and simulations; earlier that year, a national exercise had simulated a vulnerability with eID, although the respondent

noted that eID officials had been adamant that such a scenario would never unfold (ERR, 2015; MKM, n.d.; L. Areng, interview, April 3, 2023). Multiple respondents also drew attention to the fact that there was a 'lessons learned' paper drafted in response to the eID crisis, and unlike the 2007 cyberattacks before it, this paper was made publicly available (RIA, 2018; Former cybersecurity official, interview, n.d.; Former senior MOD official, interview, n.d.). Furthermore, a former MoD official (interview, n.d.) suggested that, beyond RIA, other ministries and agencies generally made better crisis plans for themselves as a result of the eID crisis.

COVID-19 pandemic

Initially COVID-19 represented a public health emergency, but the move online necessitated by lockdowns quickly encompassed various elements of Estonia's e-governance and the cybersecurity of these provisions. At the onset of the pandemic, a respondent from the National Situation Centre (interview, n.d.) noted that the government began to collate information and knowledge from across sectors, especially in the digital space, so that the government could craft potential responses. With the move online taking place rapidly, initial issues were less surrounding cybersecurity, and more about accessibility and usage issues, such as insufficient broadband or ineffective VPNs (Former cybersecurity official, interview, n.d.; Former electoral official, interview, n.d.; Former National Situation Centre official, interview, n.d.; L. Areng, interview, April 3, 2023). There were also concerns around the security of popular video-calling platforms such as Microsoft Teams and Zoom, around espionage or unauthorised persons entering these calls. The remedy to these concerns was a review of best practices in cyber hygiene, which one respondent noted was already particularly strong in Estonia, with training provided within the government, as well as made publicly available by companies such as Cybexer Technologies (Former cybersecurity official, interview, n.d.).

Despite global upticks in cyberattacks, in Estonia several respondents noted that there wasn't a significant wave of cyberattacks from Russian cyberattackers, as might have been expected, but rather, "petty cybercrime" with a quite standard combination of phishing, DDoS, and ransomware attacks, experienced in many other countries as well (Former National Situation Centre official, interview, n.d.; Former cybersecurity official, interview, n.d.; L. Areng, interview, April 3, 2023). What Estonia was more concerned with was the prospect of "more organised, state-backed, state-organised attacks that could take down critical infrastructures," or target the fundamental functioning of Estonian digital governance, but that this sort of attack did not eventuate during the pandemic (Former cybersecurity official, interview, n.d.). These ideas are also reflected in RIA's yearbook for 2020 (RIA,

2021).

While most e-services had been available online in Estonia prior to the pandemic, there were some that had not; two such key services were e-education and real estate transactions. Several respondents outlined how the move online of schooling was highly decentralised, that decisions around the technologies used and their security mechanisms, were largely determined on a case-by-case basis in individual educational settings (Former MOD official, interview, n.d.; Former cybersecurity official, interview, n.d.; L. Areng, interview, n.d.). Indeed, literature and reporting from that time show that the security of new and decentralised e-education provisions posed learning curves, as one e-education platform even suffered DDoS cyberattacks and concerns emerged about the functionality of fully-online e-learning and e-health (Carmichael, 2021, p. 38; Eesti Ekspress, 2020; McBride, 2021). To allow real estate transactions to move online, existing technologies from the Estonian company Veriff, used for the Estonian e-Residency programme, were repurposed to allow real estate transactions to take place remotely (Carmichael, 2021, pp. 40-41). Throughout this process, RIA was consulted to ensure optimal security mechanisms in this process, and the Computer Security Incident Response Team (CSIRT) became involved in assisting service providers (L. Areng, interview, April 3, 2023). Furthermore, one respondent revisited RIA audits, which were being carried out on a regular basis, dating back to the 2007 cyberattacks, to ensure cybersecurity compliance and preparedness across government (Former senior MOD official, interview, n.d.).

Russia's full-scale invasion of Ukraine

Several respondents noted that the Estonian government's cybersecurity response to Russia's full-scale invasion of Ukraine did not neatly align with the 24 February 2022 start of the invasion, but rather had been ongoing over the past decade as Russian aggression against Ukraine escalated. One respondent, a former senior cybersecurity specialist (interview, n.d.), indicated that Estonian officials had been playing close attention to Russian cyber-activity in Ukraine since 2014 (and perhaps even earlier, dating back to the Russian invasion of Georgia in 2008, about which the Estonian government wrote a lessons learned paper, which is still not publicly-available). Funding for enhancing cybersecurity mechanisms was allocated in January 2022; concerns around the security escalation in Ukraine and, ultimately, the full-scale invasion, made it easier to gain resources for cybersecurity initiatives (T. Peterkop, interview, April 3, 2023; Former MOD official, interview, n.d.). This increased funding is clearly outlined in official government messaging and announcements at the time (ERR, 2021; MOD, n.d.).

Several respondents expressed that cyberattacks faced by Estonian public and private sector entities in the immediate aftermath of 24 February were less, in both their frequency and severity, than they might have expected (National Situation Centre personnel, interview, n.d.; Former electoral official, interview, n.d.). As the war continued, cyberattacks did begin to earnestly target Estonia: these were mostly DDoS attacks, beginning with the NATO Locked Shields cybersecurity exercise in April 2022, and continuing throughout the year, as RIA's 2022 yearbook clearly shows (RIA, 2022). Multiple respondents expressed that the impacts of DDoS attacks felt less severe than cyberattacks in the past, including the 2007 cyberattacks, as the technology for mitigating DDoS attacks has improved over time, and the government has increased both its investment into cybersecurity and collaboration with the private sector (Former National Situation Centre official, interview, n.d.; Former senior MOD official, interview, n.d.).

While respondents indicated that cybersecurity mechanisms were already quite good at the onset of the 24 February full-scale invasion, they also outlined ways in which the Estonian government undertook a number of decisions in an attempt to further bolster cybersecurity. There was an exchange of technology between public institutions and critical infrastructure providers, and enhanced assistance provided by RIA (Former MOD official, interview, n.d.). A RIA official confirmed this process; since the onset of the full-scale invasion, RIA had crafted a three-layered approach to cybersecurity: the first layer involves the victim of a cyberattack turning first to RIA and its response teams for assistance; the second layer is RIA-supported (via resources and training) IT houses across the Estonian government, and the third layer is the Cyber Unit of the Estonian Defence League (L. Areng, interview, April 3, 2023).

Once again, there was a key focus on government messaging, especially in August 2022 as DDoS attacks reached their highest levels since 2007, as a Soviet-era tank was removed from public display in the border town of Narva, confirmed by RIA's 2022 yearbook (RIA, 2023). Announcing the cyberattack, Estonian CIO Luukas Ilves Tweeted: 'Yesterday, Estonia was subject to the most extensive cyber attacks it has faced since 2007. Attempted DDoS attacks targeted both public institutions and the private sector' (Ilves, 2022, n.p.). This Tweet was shared by high-profile Estonian government officials including President Alar Karis and Prime Minister Kaja Kallas. Multiple respondents acknowledge that this was, again, an instance of clear and transparent messaging about cyberattacks targeting Estonia; another noted that it represented an opportunity to "praise" the personnel responsible for responding to these cyberattacks.

Some respondents did, however, express concerns with this response, that the high-profile nature of this messaging could unintentionally place a target on Estonia for future cyberattacks, or be manipulated for purposes of Russian information warfare (Former MOD official, interview, n.d.; L. Areng, interview, April 3, 2023). The intrinsic linkage between information warfare and cyber operations by the Russian state – both before and since the start of the full-scale invasion – was pointed out by several respondents as an ongoing concern. Such a linkage between information warfare and cyber operations within Russian governmental doctrine is reflected in a great deal of literature (see for example, Etudo et al., 2023; Zelenkauskaite, 2022; Whyte, 2020). However, one respondent pointed out that crafting messaging around DDoS attacks is "safe" *vis-à-vis* other types of cyberattacks that may be more sophisticated, or potentially embarrassing or damaging to a country's reputation (Former National Situation Centre official, interview, n.d.). Therefore, it may have been less risky for Estonian government officials to publicly announce these DDoS attacks in August 2022, as this was deemed less damaging to either its reputation, nor technically to its digital governance's functionality.

External crises informing Estonia

Speaking with respondents also revealed that decision-making has not solely been shaped by Estonian crises, but has also been informed by crises that have occurred beyond its borders. One such example, outlined by multiple respondents, was the 2011 earthquake in Fukushima, in which the Japanese government lost a small amount of national data (T.H. Ilves, interview, March 14, 2023; T. Kotka, interview, March 28, 2023). With increased digitalisation and the move away from hard copies, one respondent emphasised how essential it became for information – and even legislation – that is stored solely digitally to be available in the event of disaster. While natural disasters, like the earthquake in Fukushima, are statistically quite infrequent in Estonia, respondents recognised the threat of occupation – as was seen in Crimea since 2014, but which Estonia also experienced during its occupation by the Soviet Union from the end of the Second World War until 1991 – whereby information could be destroyed or fundamentally altered. The same is also possible via cyberattacks. The result was the establishment of the first data embassy, located in Luxembourg, although the Estonian government began storing copies of information outside the country as early as 2005 in response to this threat (T. Kotka, interview, March 28, 2023).

Path dependencies across crises

This paper has treated the four selected crises as critical junctures, derived from historical institutionalist theory outlined previously, which can be used as markers from which path-dependent processes begin, and whereby outcomes, decisions, and processes result from those that came before them (Fioretos et al., 2016, p. 9). Indeed, it can be seen from the analysis above that the post-crisis responses and decision-making processes outlined by the interviewees gave rise to path-dependent processes in the Estonian context. The first is crisis communications responses, which originated with the 2007 cyberattacks, when officials carefully considered whether to go public with an acknowledgement of the DDoS attacks, a decision they did eventually undertake. Interviewees then asserted that subsequent communications strategies emerged from this initial decision: the 'radical transparency' approach to the eID crisis in 2017, and the acknowledgement of the largest DDoS cyberattacks on Estonia since 2007, publicly disseminated on the Estonian then-CIO's Twitter.

Secondly, new governance structures that emerged from the 2007 cyberattacks were directly related to crisis decision-making in subsequent cybersecurity crises. This included the elevation and empowerment of RIA in the aftermath of the 2007 cyberattacks prioritised this sophisticated technical expertise within the Estonian government; RIA played a lead role in the 2017 eID crisis and developing the patch to the ROCA vulnerability, while RIA auditing across the whole of Estonian government, aimed at ensuring cybersecurity compliance, was deployed throughout the COVID-19 pandemic and beyond. Furthermore, RIA's three-tier approach, offering cybersecurity services to the rest of government, was amped up following the start of the full-scale invasion. In addition to RIA, path dependencies from the establishment of the NATO CCDCoE in Tallinn following the 2007 cyberattacks could be seen with Estonian efforts to bring Ukraine into CCDCoE membership, with the purpose of exchanging cybersecurity and cyber defence expertise and knowledge following the start of the full-scale invasion. Finally, DDoS preparedness, resulting from overall improvements and investment in appropriate technology, can be traced from the 2007 cyberattacks. Subsequent disruptions from DDoS attacks throughout the COVID-19 pandemic and following the start of the full-scale invasion of Ukraine by Russia in 2022 were significantly minimised *vis-à-vis* what was experienced with the DDoS attacks in 2007. Thus, through these multiple instances, the critical junctures examined in this paper can be used to trace path-dependent processes in cybersecurity governance in the Estonian government over time.

Conclusions

Each of these events represents a distinct point and critical juncture in Estonia's history of cybersecurity and e-governance, each with their own unique and nuanced realities of the crisis at hand. However, there are commonalities that exist across these critical junctures that offer lessons in how a country, Estonia or beyond, can broach decision-making following cybersecurity crises, especially when those crises may potentially affect digitalised governmental provisions. Thus, there are three key overarching ways in which this paper's core research question – which asks how governments and their responsible bodies can respond in the aftermath of a crisis to bolster future cybersecurity, especially around digitalisation initiatives – has been addressed using the Estonian case.

Firstly, a common thread amongst Estonian government responses to cybersecurity crises is building on prior knowledge and experience, both inside of Estonia and internationally, by monitoring the cybersecurity threat landscape in other countries and their experiences with broaching crises as well. This is a continuous process, one which recognises that the cybersecurity landscape is not static, but ever-changing. Estonian government entities, in collaboration with the private sector, derived lessons from earlier cybersecurity crises, like the 2007 cyberattacks and 2017 eID crisis, and applied these learnings in future crises, including the COVID-19 pandemic and the Russian full-scale invasion of Ukraine, so that the impacts of cyberattacks were lessened. Furthermore, Estonian authorities monitored the threat landscape, looking at Japan after the 2011 Fukushima earthquake, or Ukraine since the 2014 annexation of Crimea, to learn from the experiences of other countries and bolster Estonian cybersecurity in response to such events. This indicates a constant process of observing and learning in times of both crisis and non-crisis, internally and looking to external examples. Indeed, a crisis is not a sole impetus for change and improvement to cybersecurity, but serves as a very strong driver.

Secondly, across these crises, the Estonian government has employed clear, coordinated messaging and transparency around times of crisis. Such an approach was initially derived from the 2007 cyberattacks, at the time quite unprecedented and as yet uncharted whether the government would acknowledge at all that the cyberattacks had taken place. Indeed, even today, the very acknowledgement of cyberattacks is often not guaranteed amongst many governments globally. However, the Estonian government of the time undertook the decision to acknowledge – to the general public and to other levels of governance (i.e., EU and NATO) – that they were experiencing DDoS cyberattacks, and this approach has subsequently

been taken during the eID crisis, throughout the COVID-19 pandemic, and following cyberattacks since the Russian full-scale invasion of Ukraine. This messaging has been coordinated by the responsible government entities, and taken place through channels such as press conferences or releases and government figures' social media, with the specific objective of informing the public of cyber crises in a clear, transparent, and easy-to-understand fashion.

Thirdly, while some new solutions indeed arose from these crises, in many cases, these crises acted as expeditors for other ideas that hadn't gone through prior. During the earliest days of the COVID-19 pandemic, for example, new solutions broached the move of education to a strictly online provision, but even 'new' provisions like online solutions for real estate transactions were derived from existing technologies from Estonian company Veriff, used in the e-Residency process, and repurposed for notarisation on real estate transactions. Additionally, the NATO-accredited CCDCoE in Tallinn had been proposed since 2004, but its establishment was likely expedited by the 2007 cyberattacks. Similarly, Ukrainian membership into the CCDCoE in 2023 and Estonian-Ukrainian cooperation on cybersecurity matters was expedited by the full-scale invasion in February 2022. This, therefore, shows the direct linkages between times of crisis and times of non-crisis, underscoring the need for creative responses to crisis in the moment, but also the need for innovation in times of non-crisis. New ideas and approaches, as well as simulations and exercises of the most unimaginable or worst-case scenarios, all contribute to increased preparedness for if, or more likely, when, the next crisis strikes.

Estonia represents a unique case in that it has fifteen years of cybersecurity history that can be examined, whereas most countries have not yet developed their cybersecurity processes over such a lengthy period of time. Therefore, as a mature case, Estonia has the benefit of learning and refining their approach over time. Drawing from this case, this paper makes both a theoretical and practical contribution to the existing body of scholarship. Theoretically, the novelty of this paper lies in the contribution to crisis management literature in the domain of cybersecurity, looking specifically at post-crisis management in a highly digitalised and mature case. The use of crises as critical junctures as sign-posts demarcating path-dependent processes in the Estonian cybersecurity governance process, especially examining these processes in the context of post-crisis management, is additionally novel in this regard. These findings have practical novelty for governments globally, who are currently undergoing digitalisation processes, and enacting cybersecurity mechanisms, at various stages and levels of governance.

Thus, this case offers lessons for other governments around 1) building upon prior

knowledge, internally and externally; 2) crafting communications strategies to be clear and transparent; and 3) allowing crises to serve as expeditors for new ideas, approaches, or policies in cybersecurity governance. Especially as many other governments have come to both the digitalisation and cybersecurity domain comparatively later than Estonia, there is immense benefit in observing such functions in Estonia, and tailoring responses aimed at bolstering cybersecurity to local intricacies in their own respective governance setting. For example, lessons could be derived for recent prominent examples of cybersecurity crises befalling digital governance in countries such as Costa Rica and Albania. The former declared a state of emergency in May 2022, as ransomware attacks originating from Russian cybercriminal group Conti held government websites ransom, initially targeting the country's Ministry of Finance but ultimately affecting 27 ministries (The Guardian, 2022; Murray and Srivastava, 2022; Datta and Acton, 2024, pp. 59-60). The latter suffered cyberattacks throughout July 2022, continuing into early 2023, and required assistance from Israel to reboot its e-governance structure that was taken offline by Iranian state actors (Taylor, 2023; Biberaj et al., 2022; Pavel, 2024, pp. 110-112). Now, as both governments grapple with the aftermath of said crises, similar to the post-crisis management period examined in this paper, there is an immense opportunity to adapt, bolster future cybersecurity mechanisms, and better equip them to navigate digitalisation and cybersecurity concerns into the future.

References

Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Granelli, F., Gravelines, J., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Pamment, J., Sari, A., Sazonov, V., Simons, G., & Terra, J. (2019). *Hybrid threats: 2007 cyber attacks on Estonia* (Hybrid Threats. A Strategic Communications Perspective). NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: The case of Estonia. *Political Science & Politics*, *42*(3), 497–505.

Areng, L. (2013). International cyber crisis managment and conflict resolution mechanisms. In K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (pp. 565–593). https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

Baezner, M. (2018). *Cyber and information warfare in the Ukrainian conflict* (Center for Security Studies (CSS)). ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

Bannister & Connolly. (2012). Defining e-governance. *E-Service Journal*, *8*(2), 3. https://doi.org/10.2979/eservicej.8.2.3

BBC News. (2007, May 17). *Estonia hit by Moscow cyber war*. BBC News. http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

Beltadze, G. (2017, September 12). *Toomas Hendrik Ilves: E-riigina tegutseb Eesti maailmaliigas, kriitikaks tuleb valmis olla [Estonia operates on the world stage as an e-state, we must be prepared for criticism]*. Arvamus Postimees. https://arvamus.postimees.ee/4240381/toomas-hendrik-ilves-e-riigina-tegutseb-eesti-maailmaliigas-kriitikaks-tuleb-valmis-olla

Biberaj, A., Sheme, E., Rakipi, A., Xhaferllari, S., Kushe, R., & Alinci, M. (2023). Cyber attack against e-Albania and its social, economic and strategic effects. *Journal of Corporate Governance, Insurance, and Risk Management*, *9*(2), 341–347. https://doi.org/10.56578/jcgirm090204

Boeke, S. (2017). National cyber crisis management: Different European approaches. *Governance*, *31*(2), 1–16.

Bogner, A., Littig, B., & Menz, W. (2009). *Interviewing experts*. Palgrave Macmillan.

Boin, A., T'Hart, P., Stern, E., & Sundelius, B. (2017). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.

Carmichael, L. (2021). Exploring Estonian e-government before, during, and beyond COVID-19. *New Zealand Journal of Research on Europe*, 7–51. https://dspace.ut.ee/server/api/core/bitstreams/7a9bbc5a-7785-44b9-beed-a392bfeb1a3e/content

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In M. Taddeo & L. Glorioso (Eds.), *Ethics and policies for cyber operations: A NATO Cooperative Cyber Defence Centre of Excellence initiative* (pp. 187–212).

Coombs, T. (2018). Crisis communication. In *The international encyclopedia of strategic communication* (1st ed., pp. 1–12). Wiley. https://onlinelibrary.wiley.com/doi/10.1002/9781119010722.iesc0054

Coombs, W. T., Holladay, S. J., & Tachkova, E. (2019). Crisis communication, risk communication, and issues management. In *Public relations theory: Application and understanding*. Wiley-Blackwell.

Cooperative Cyber Defence Centre of Excellence. (n.d.). *About us*. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/about-us/

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

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

D'Agostino, M. J., Schwester, R., Carrizale, T., & Melitsk, J. (2011). A study of e-government and e-governance: An empirical examination of municipal websites. *Public Administration Quarterly*, *35*(1).

Datta, P. M., & Acton, T. (2024). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*, *14*(1), 56–67. https://doi.org/10.1177/20438869221149042

EESTI. (2015, September 20). *Suurimal kodumaisel küberjulgeolekuõppusel lahendatakse simuleeritud küberintsidente [Simulated cyber incidents to be resolved at largest domestic cyber security exercise]*. ERR. https://www.err.ee/545744/suurimal-kodumaisel-kuberjulgeolekuoppusel-lahendatakse-simul

eeritud-kuberintsidente

Eesti Ekspress. (2020, April 15). *eKool langes küberrünnaku alla [eKool was the target of a cyberattack]*. Eesti Ekspress. https://ekspress.delfi.ee/artikkel/89554685/ekool-langes-kuberrunnaku-alla

Ehala, M. (2009). The Bronze Soldier: Identity threat and maintenance in Estonia. *Journal of Baltic Studies*, *40*(1), 139–158. https://doi.org/10.1080/01629770902722294

Ernsdorff, M., & Berbec, A. (2007). Estonia: The short road to e-government and e-democracy. In *E-government in Europe* (pp. 171–183).

ERR. (2021). Estonia directs additional €14.4 million to digital state upgrades in 2022. *ERR*. https://news.err.ee/1608361020/estonia-directs-additional-14-4-million-to-digital-state-upgrades-in-2022#:~:text=In%20order%20to%20reduce%20cybersecurity

Etudo, U., Whyte, C., Yoon, V., & Yaraghi, N. (2023). From Russia with fear: Fear appeals and the patterns of cyber-enabled influence operations. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad016

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2). https://doi.org/10.14763/2018.2.788

Fioretos, O., Falleti, T. G., & Sheingate, A. (2016). *Historical institutionalism in political science* (O. Fioretos, T. G. Falleti, & A. Sheingate, Eds.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199662814.013.1

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Hafner-Burton, E. M., Hughes, A., & Victor, D. G. (2012). The cognitive revolution and the political psychology of elite decision making. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1917037

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*, 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Härmand, K. (2021). Digitalisation before and after the Covid-19 crisis. *ERA Forum*, *22*(1), 39–50. https://doi.org/10.1007/s12027-021-00656-8

Herzog, S. (2017). Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity. *Georgetown Journal of International Affairs*, *18*(3), 67–78. https://doi.org/10.1353/gia.2017.0038

Ilves, L. (2022, August 18). *Yesterday, Estonia was subject to the most extensive cyber attacks*. X. https://twitter.com/luukasilves/status/1560105663933587458

Interpol. (2020, August 4). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Interpol. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*(2), 147–157. https://doi.org/10.1016/j.pubrev.2007.02.001

Jašina-Schäfer, A., & Cheskin, A. (2020). Horizontal citizenship in Estonia: Russian speakers in the borderland city of Narva. *Citizenship Studies*, *24*(1), 93–110. https://doi.org/10.1080/13621025.2019.1691150

Jin, Y., Coombs, W. T., Wang, Y., Van Der Meer, T. G. L. A., & Shivers, B. N. (2024). "READINESS": A

keystone concept beyond organizational crisis preparedness and resilience. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12546

Kaitseministeerium. (2022, January 20). *Government to invest additional 380 million euros in national security*. Kaitseministeerium. https://kaitseministeerium.ee/en/news/government-invest-additional-380-million-euros-national-security

Kerikmäe, T., Troitino, D. R., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica et Philosophiae Scientarium*, *7*(1), 71–80. https://doi.org/10.11590/abhps.2019.1.05

King, N., Horrocks, C., & Brooks, J. (2019). *Interviews in qualitative research* (2nd ed.). Sage Publications Ltd.

Kitsing, M. (2008). Explaining the e-government success in Estonia. *Proceedings of the 9th Annual International Digital Government Research Conference*.

Littig, B. (2009). Interviewing the elite – interviewing experts: Is there a difference? In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing experts* (pp. 98–113). Springer.

Mahoney, J., Mohamedali, K., & Nguyen, C. (2016). Causality and time in historical institutionalism. In O. Fioretos, T. G. Falleti, & A. Sheingate (Eds.), *The Oxford Handbook of Historical Institutionalism*. Oxford University Press. https://academic.oup.com/edited-volume/28116/chapter/212252196

Majandus- Ja Kommunikatsiooniministeerium. (2016, May 13). *Valitsus kiitis heaks küberintsidentide lahendamise plaani [Government approves cyber incident response plan]*. MKM. https://www.mkm.ee/uudised/valitsus-kiitis-heaks-kuberintsidentide-lahendamise-plaani

McBride, K. (2021, March 11). *Image of "digital Baltics" cracks under weight of pandemic*. New Eastern Europe. https://neweasterneurope.eu/2021/03/11/image-of-digital-baltics-cracks-under-weight-of-pandemic/

Murray, C., & Srivastava, M. (2022, July 9). *How Conti ransomware group crippled Costa Rica – then fell apart*. Financial Times. https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of Coppersmith's Attack: Practical factorization of widely used RSA moduli. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1631–1648. https://doi.org/10.1145/3133956.3133969

Østby, G., & Katt, B. (2019). Cyber crisis management roles – A municipality responsibility case study. *4th International Conference on Information Technology in Disaster Risk Reduction (ITDRR), Kyiv*.

Oviir, L. (2017, September 14). *Vastus Aivar Paule: ID-kaardi kriisikommunikatsiooniga tegelesid ässad [Response to Aivar Pau: ID-card crisis communication was handled by aces]*. Arvamus; Postimees. https://arvamus.postimees.ee/4244293/vastus-aivar-paule-id-kaardi-kriisikommunikatsiooniga-tegelesid-assad

Parsovs, A. (2020a). Estonian electronic identity card: Security flaws in key management. In *Usenix*. https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs

Parsovs, A. (2020b). Solving the Estonian ID card crisis: The legal issues. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3644664

Pau, A. (2017a, September 6). *Repliik: Ratas andis ID-kaardi jamaga turmtuld e-valimistele [Reply: Ratas threw a spanner in the works for e-voting with the ID card scandal*. Tehnika; Postimees. https://tehnika.postimees.ee/4234361/repliik-ratas-andis-id-kaardi-jamaga-turmtuld-e-valimistele

Pau, A. (2017b, September 14). *Repliik: Kriisikommunikatsioon mis tekitas kriisi [Reply: Crisis communication that created the crisis]*. Tehnika; Postimees. https://tehnika.postimees.ee/4243691/repliik-kriisikommunikatsioon-mis-tekitas-kriisi

Pavel, T. (2024). The Iranian cyberattacks in Albania: Actors, tactics, targets. *Dot.Pl*, *I*, 105–123. https://doi.org/10.60097/dotpl/196772

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *The Academy of Management Review*, *23*(1), 59. https://doi.org/10.2307/259099

Pernik, P. (2018). The early days of cyberattacks: The cases of Estonia, Georgia and Ukraine. In N. Popescu & S. Secrieru (Eds.), *Hack, leaks, and disruptions: Russian cyber strategies*. European Union Institute for Security Studies (EUISS.

Pierson, P., & Skocpol, T. (2002). Historical institutionalism in contemporary political science. In *Political Science: State of the Discipline* (pp. 693–721). W.W. Norton.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

RIA. (2018). *ROCA vulnerability and eID: Lessons learned*. https://www.ria.ee/en/media/742/download

RIA. (2021). *Cyber security in Estonia 2021*. https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2021.pdf

RIA. (2023). *Cyber security in Estonia 2023*. https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1), 211–222. https://doi.org/10.1016/j.dcan.2022.06.005

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*, 1–12. https://doi.org/10.1016/j.giq.2022.101781

Solms, B., & Solms, R. (2018). Cyber security and information security – what goes where? *Information and Computer Security*, *26*(1).

Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M., & Vassil, K. (2019). E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics*, *36*, 39–54. https://doi.org/10.1016/j.tele.2018.11.005

Stephany, F. (2020). It's not only size that matters: Determinants of Estonia's e-governance success. *Electronic Government*, *16*(3), 304–313. https://doi.org/10.1504/EG.2020.108501

Strauss, A., & Corbin, J. (1998). Coding for process. In *Basics of Qualitative Research* (pp. 163–178). Sage Publications.

Tasheva, I. (2021). Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View*, *20*(2), 140–149. https://doi.org/10.1177/17816858211059250

Taylor-Braçe, A. (2023, January 19). *Albanian PM: Country under daily cyberattacks*. Euractiv. https://www.euractiv.com/section/politics/news/albanian-pm-country-under-daily-cyberattacks/

The Guardian. (2022, May 12). *Costa Rica declares national emergency amid ransomware attacks*. The Guardian. https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ranso

mware-attacks

Turner, D. (2014). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2010.1178

University of Tartu. (2017). *Estonian code of conduct for research integrity*. https://ut.ee/sites/default/files/inline-files/code_of_conduct_for_research_integrity_eng_1.pdf

Urgessa, W. G. (2020). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. *Computer Law & Security Review*, *36*, 105368. https://doi.org/10.1016/j.clsr.2019.105368

Valimised. (2017, August 31). *Statistics about internet voting in Estonia*. Valimised. https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly*, *33*(3), 453–459. https://doi.org/10.1016/j.giq.2016.06.007

Von Soest, C. (2023). Why do we speak to experts? Reviving the strength of the expert interview method. *Perspectives on Politics*, *21*(1), 277–287. https://doi.org/10.1017/s1537592722001116

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa013

Zelenkauskaite, A. (2022). *Creating Chaos Online*. University of Michigan Press.

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies