CHAPTER II

Lessons from Estonia's National Cybersecurity Strategy: How to Succeed or Fail in Delivering Value

Kadri Kaska
Liis Rebane
Toomas Vaks

Introduction

Estonia has built its current level of cybersecurity maturity over the past 12 years by the continuous and systematic implementation of cybersecurity measures, supervision and collaboration; by relying on a decentralised governance model; guided by three national cybersecurity strategies, and verified through two national-level cyber crises in 2007 and 2017.

Estonia's digital ecosystem relies on the government-ensured secure digital identity and secure interagency data exchange environment. This approach has served as the enabler and amplifier of rapid digital innovation and ensured that cybersecurity is integrated into the very foundations of the digital society

Estonia's digital ecosystem relies on the government-ensured secure digital identity and secure interagency data exchange environment. This approach has served as the enabler and amplifier of rapid digital innovation and ensured that cybersecurity is integrated into the very foundations of the digital society. On the policy level, however, its decentralised cybersecurity governance model, in which stakeholders retain broad independence, has posed systemic challenges leading to weak coherence in strategic cybersecurity management and coordination, and ambiguous division of roles and responsibilities across organisations' overlapping mandates. Paradoxically, this lack of a centralised formal governance structure has simultaneously enabled an agile, flexible and integrated community, proven to serve as one of Estonia's greatest assets.

Lessons from Estonia's experience in building its cyber resilience alongside the development of the digital society, supported by national-level strategic planning, do not appear to be limited to Estonia. After giving an overview of Estonia's three national cybersecurity strategy periods, this chapter aims to draw some universally applicable lessons by discussing practical deliverables of cybersecurity strategies and the ways they offer to succeed or fail in creating real value.

1. Evolution of Estonia's National Cybersecurity Strategy

Estonia's first cybersecurity strategy, issued in May 2008, was driven by a manifest and well-recognised national need: lessons from the large-scale cyberattacks in the spring of 2007, when political tensions between Estonia and Russia spilled over into cyberspace and triggered weeks of coordinated cyber-attacks against Estonia's online presence – financial institutions, government agencies, news media and communications infrastructure.[1] The attacks brought about two important lessons for the Estonian state and society: (1) that targeting online assets can have a tangible impact on modern society's sense of normality, and (2) that, despite the onslaught, the country could maintain its functioning society and "the digital way of life" with the support of its existing fundamental technical, institutional and legal frameworks, and by connecting to international incident cooperation networks.[2] Following these lessons, the 2008 strategy was based on a firm recognition that national cybersecurity is a comprehensive task comprising public–private action, various domains, and technical, organisational and legal measures. The strategy focused on addressing resilience gaps by improving the cybersecurity of essential services, while institutionalising the experienced success of public–private collaboration and international cooperation.

The 2008 strategy was based on a firm recognition that national cybersecurity is a comprehensive task comprising public-private action, various domains, and technical, organisational and legal measures

The first strategy set the foundation for Estonia's overall cybersecurity model by: (1) improving infrastructure resilience, (2) allocating roles and responsibilities, (3) establishing the notion of a comprehensive national cybersecurity toolbox encompassing technology, legal framework, organisations and processes, and (4) placing a strong emphasis on international cooperation. Its successor, in 2014, set out to build further national detection and response capabilities; emphasised cybersecurity education and research as means for future-proofing society against cyber threats, addressed the national defence dimension of cybersecurity, and introduced a set of common principles to support a consistent cybersecurity approach across stakeholders and areas of responsibility.[3] The 2019 strategy, informed by the lessons of the 2017 ROCA (Return of the Coppersmith Attack) eID (electronic identity) vulnerability crisis, created mechanisms to stimulate the development of a strong, R&D-based cybersecurity enterprise sector, outlined objectives to fulfil Estonia's ambition in promoting the rule of law and norms of responsible state behaviour internationally,

Estonia's fourth national cybersecurity strategy is currently under development and is expected to merge the strategic planning of cybersecurity with the national digital agenda for the next decade

[1] Cyber Security Strategy Committee of Estonia, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en. For a more detailed account of and background to the events, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010), 18–23, https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

[2] Estonian Information System Authority, *Annual Cyber Security Assessment 2017* (Tallinn: Estonian Information System Authority, 2017), 4–5, https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

[3] Ministry of Economic Affairs and Communications of Estonia, *Cyber Security Strategy 2014-2017* (Tallinn: Ministry of Economic Affairs and Communications, 2014), https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

and substantiated the country's ambition towards a skilled society and workforce.[4]

Estonia's fourth national cybersecurity strategy is currently under development and is expected to merge the strategic planning of cybersecurity with the national digital agenda for the next decade. This step aims to complete establishing cybersecurity planning as a fully integrated part of the development of the digital society.[5]

2. Delivering Practical Outcomes?

Deriving from Estonia's experience over the past dozen years, five practical national cybersecurity strategy deliverables can be identified that have, to varying degrees of success, reinforced Estonia's development as a resilient digital society:

- a coherent and efficient **governance model** that is realistic with regard to available resources;
- a **strategic vision** and a set of fundamental principles ensuring long-term, value-driven development of national cybersecurity;
- a set of strategic objectives **along with an action pl**an for the strategy period, ensuring coordinated prioritisation and sustained progress in tackling increasing technological challenges and cyber threats;
- executing **national cybersecurity strategy planning as a process** that incorporates relevant actors across the whole cyber ecosystem, thereby strengthening the cybersecurity community by improving its interoperability and mutual calibration;
- making the strategy **accessible to international partners** by disclosing the proposed activities and underlying process, thereby offering a tool to support dialogue and collaboration with international counterparts.

While these deliverables correlate to some degree, each can be studied – and achieved – independently, as none is a strong prerequisite for the others. Each of these has its challenges, as the Estonian experience amply exemplifies. The following subsections describe the deliverables, discussing their impact, challenges, lessons learnt, and overall insight acquired from Estonia's three cybersecurity strategy documents and their implementation periods.

The 2018 review of the state of Estonia's cybersecurity affairs highlighted two key shortcomings: a lack of coherent leadership and a lack of ownership

2.1. A functional governance model

The 2018 review of the state of Estonia's cybersecurity affairs highlighted two key shortcomings: a lack of coherent leadership – where national cybersecurity resembled the sum of individual agencies' activities according to their own priorities more than a concerted whole – and a lack of ownership, with cybersecurity viewed as a complex technical matter that someone else should deal with. Consequently there was insufficient cross-agency situational awareness and information exchange, as well as fragmented, uneven and often wasteful cybersecurity management, despite general policy guidelines suggesting the consolidation of resources.[6] The 2021 draft strategy appears to come to similar conclusions, citing the challenge of ensuring adequate resources (primarily personnel) to effectively run a decentralised system in an increasingly complex environment, and ambiguity of responsibilities beyond broadly drawn roles.[7]

[4] See Estonian Information System Authority, "ROCA Vulnerability and eID: Lessons Learned," n.d., https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf; Ministry of Economic Affairs and Communications of Estonia, *Cybersecurity Strategy 2019-2022: Republic of Estonia* (Tallinn: Ministry of Economic Affairs and Communications, 2019), https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[5] The draft *Digital Society Development Plan 2030* was released for consultations with stakeholders in late autumn 2020. There is no publicly available version at the time of writing this chapter.

[6] Ministry of Economic Affairs and Communications of Estonia, *Cybersecurity Strategy 2019-2022,* Section 1.3.

[7] Draft *Digital Society Development Plan 2030.*

Clearly defined cybersecurity roles and accountability across the "whole of system" are generally recognised as fundamental for successful governance, and most national cybersecurity strategies devote a substantial amount of attention to this topic.[8] Actual national models vary; most adopt the approach of individual responsibility allocation with some cyber-specific coordination body aligning their (cyber) activities.[9] Estonia's reliance on a decentralised model, with stakeholders retaining their independence and the role of the lead body (the Ministry of Economic Affairs and Communications) as primus inter pares generally weak, has meant that achieving consistency of priorities, approach and resources across sectors has remained a persistent struggle. The National Cybersecurity Council, consisting of representatives of relevant ministries, is a policy planning and coordination format reflecting the same "sum of individual parts" approach, with individual ministries enjoying broad autonomy in their planning and working programmes.

The divergent interests of different agencies and ministries (the notorious "silo" approach) and difficulties in achieving central coordination have proven the main roadblocks to meeting strategic objectives

The divergent interests of different agencies and ministries (the notorious "silo" approach) and difficulties in achieving central coordination have proven the main roadblocks to meeting strategic objectives.[10] To complicate matters, the interplay between various agencies' cyber-specific and general roles has generally been poorly considered, although there has been some improvement in this regard with the growing importance of – and therefore attention to – cybersecurity.

"Cybersecurity governance as a sum of individual parts" approach admittedly has its benefits. It evolves organically as society's digitalisation grows, and does not require fundamental reorientation in the tasks or governance areas of government agencies

This "cybersecurity governance as a sum of individual parts" approach admittedly has its benefits. It evolves organically as society's digitalisation grows, and does not require fundamental reorientation in the tasks or governance areas of government agencies. The straightforward individual mandates imply an imaginary promise of effectiveness: objectives and priorities can be set within a single domain, allowing problems to be limited to their own constituency, where one is less dependent on external commitment and resources. It is context-aware and hence better equipped to respond to sector-specific needs. On the other hand, it tends to overlook interconnectedness and cascading dependences, and there is a risk of conflicting activities and competition over the same limited resources.

2.2. Long-term vision and fundamental principles

Successfully developing national cybersecurity is a continuous process and, ideally, strategic planning periods should consciously contribute to both a short-term and a long-term view. Today's success builds on the work and decisions of previous strategy periods, while the connection to earlier efforts is not necessarily evident. This means, however, that measuring the success of each strategy period is somewhat artificial: establishing success on the building blocks set during earlier time frames shows visible results of amplified compound gain, while setting building blocks that can only be "cashed in" as successes during

[8] Alexander Klimburg (ed.), *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 94–101, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf; International Telecommunication Union, World Bank, Commonwealth Secretariat,Commonwealth Telecommunications Organisation, and NATO Cooperative Cyber Defence Centre of Excellence, *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity* (Geneva: The International Telecommunication Union, 2018), 36, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[9] See the CCDCOE National Cybersecurity Organisation series, available at https://ccdcoe.org/library/publications/ and https://ccdcoe.org/library/strategy-and-governance/.

[10] Toomas Vaks, *Küberjulgeoleku strateegia mõju küberturvalisuse arengule Eestis 2008-2018* [The impact of cybersecurity strategy on the development of cybersecurity in Estonia in 2008–18] (Tallinn: Tallinna Tehnikaülikool, 2018), 52, https://digikogu.taltech.ee/en/Download/fb794e52-07fd-4b49-93cb-3be2c56d95c2.

Vision		
2008–2013	**2014–2017**	**2019–2022**
Reduced vulnerabilities of cyberspace in the nation as a whole[11]	Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society	Estonia is the most resilient digital society
Fundamental principles		
2008–2013[12]	**2014–2017**	**2019–2022**
Cybersecurity action plans should be integrated into the routine processes of national security planning	Cybersecurity is an integral part of national security, supporting the functioning of the state and society, the competitiveness of the economy and innovation	We consider the protection and promotion of fundamental rights and freedoms as being as important in cyberspace as in the physical environment
Cybersecurity should be pursued through the coordinated efforts of all concerned stakeholders, of the public and private sectors as well as of civil society	Cybersecurity is ensured in a coordinated manner through cooperation between the public, private and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace	We see cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis for Estonia's socioeconomic growth. Security must support innovation and vice versa
Effective cooperation between the public and private sectors should be advanced for the protection of critical information infrastructure	Cybersecurity is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources	We recognise the security assurance of cryptographic solutions to be of unique importance for Estonia as it is the foundation of our digital ecosystem
Every information system owner should be aware of his or her responsibilities in the prudent use of information systems and should also take the necessary security measures to manage identified risks	Cybersecurity starts with individual responsibility for safe use of ICT tools	We consider transparency and public trust to be fundamental for a digital society. We therefore commit to adhere of the principle of open communication
A general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered	A top priority in ensuring cybersecurity is to anticipate and prevent potential threats and respond effectively to threats that materialise	
Estonia should cooperate closely with international organisations and other countries to increase cybersecurity globally	Cybersecurity is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence	
Proper attention should be paid to the protection of human rights, personal data and identity	Cybersecurity is ensured by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information and identity	
The development and administration of IT solutions for the provision of public services should be brought into compliance with relevant frameworks and policies to ensure the continuity and recovery plans of their information systems	Cybersecurity is supported by intensive and internationally competitive research and development	

Table 1. Vision and fundamental principles of Estonian national cybersecurity strategies

[11] 'Vision' is not explicitly defined in the 2008 strategy and has been extracted from the text.

[12] Some detail has been omitted from a few entries without altering the meaning in order to keep the compact format of the overview table.

future strategy windows, without offering immediate benefit, is not reflected in this measurement.

Estonia's cybersecurity vision has consistently focused on protecting the digital society as a whole, while the fundamental principles have carried the idea of protecting and promoting fundamental rights in cyberspace, and Estonia's openness and contribution in international developments

The strategy's vision and fundamental principles should serve as soft balancing mechanisms to shift the focus away from optimising for short-term progress at the expense of building long-term success – which occurs when effort is concentrated on picking tactical victories, possible thanks to earlier investments, and leaving no resources for setting a path for a successful future (such as education, R&D and international contributions towards shaping the global digital environment).

Each of Estonia's three cyber strategy documents to date has outlined the overall strategic vision and a set of fundamental principles to embody the underlying value system for strategic planning. The vision and fundamental principles for each strategy period are summarised in Table 1.

Throughout all strategy periods, Estonia's cybersecurity vision has consistently focused on protecting the digital society as a whole, while the fundamental principles have carried, in various forms, the idea of protecting and promoting fundamental rights in cyberspace, and Estonia's openness and contribution in international developments. Both the vision and principles focus on building long-term value and contribute to Estonia's success that has enabled accomplishments in international alliances and cooperation formats, building e-services on a secure digital identity framework, and relying on the relatively high maturity of critical information infrastructure.

A consistent vision and fundamental principles support long-term strategic alignment and build-up of compound value in both domestic and international collaboration. The long-term ambition should be balanced with an agile openness to make adjustments at the highest level of strategic planning. While each change needs to be well-motivated, and the top-most vision and principles are less suited for experimenting with frequent changes than lower-level goals and action plans, several reasons may justify change:

- when suggested by an increased maturity level – yesterday's vision could be today's baseline;
- in the event of external technological developments or changes in the overall threat landscape;
- when justified by lessons learned;
- when the existing vision or fundamental principles are unfit for their purpose as an alignment and communication tool for stakeholders and the target audience.

A universal strategic planning challenge, irrespective of the country or sector, is the risk of limiting the significance of a strategy document to a nice piece of writing that contains all the right principles and ambitions but has very little practical effect

As its cybersecurity strategic planning has evolved, Estonia's vision and fundamental principles have followed these ideas – the needs and maturity were clearly very different in 2008 and 2019. For example, an aspect introduced only in 2019 was the security assurance of cryptographic solutions – mainly building on the case of the 2017 ROCA eID vulnerability crisis, which highlighted Estonia's digital ID as the cornerstone of its entire digital ecosystem.[13]

[13] Estonian Information System Authority, "ROCA Vulnerability and eID."

2.3. Actionable and realistic strategic objectives

A universal strategic planning challenge, irrespective of the country or sector, is the risk of limiting the significance of a strategy document to a nice piece of writing that contains all the right principles and ambitions but has very little practical effect. The main causes for this include:

- a mismatch with the action plan, where the completion of a planned set of actions does not adequately contribute to reaching the corresponding strategic goal;
- resource planning is weakly linked with the strategy process – a challenge intensified for domains with a decentralised governance model (Estonia's cyber-security governance throughout all three strategy periods is a good example);
- insufficient connection and integration with other national strategic planning documents – stand-alone efforts within an isolated cybersecurity strategy lead to weak results. With cybersecurity becoming an integral part of all fields of governance and policy planning at national level, this challenge will grow over time.

Two further underlying aspects can markedly reduce the practical applicability of a strategy: a lack of prioritisation and an insufficient or misleading performance measurement framework, which will be described in more detail below.

Indeed, Estonia's cybersecurity strategy practice has struggled with all of the above.[14] Expert interviews conducted in 2018 regarding Estonia's key cybersecurity strategy challenges cited failures in resource planning (recognising cybersecurity as a priority but failing to match this with resource allocation); a lack of connection with overall national strategic planning, where the Cybersecurity Strategy was treated as an isolated document with stakeholders failing to recognise responsibilities as theirs; plus interagency rivalries.[15]

2.3.1. A collective letter to Santa Claus – or, everything is important!

Nearly all strategic planning processes, irrespective of the field or nation, have limitations set by available human and financial resources. This is especially true for Estonia as a very small country, meaning that setting clear priorities is of defining importance.

Cybersecurity planning induces a strong initial intuition that everything is important, often amplified by stakeholders who each argue from the perspective of their own most burning issues

Cybersecurity planning induces a strong initial intuition that everything is important, often amplified by stakeholders who each argue from the perspective of their own most burning issues. As a result, unclear priorities – wanting it all and wanting it now – emerge, subsequently facing resource constraints. Ideally, the strategy process is designed so that this mismatch is identified and addressed during development. However, as this is an extremely difficult discussion – which of all the very important things shall we not do during the next strategy period? – this step is often dismissed, leading to a vague strategy and arbitrary prioritisation.

This has been among the hardest trials for Estonia's cybersecurity planning during all strategy periods. The new, 2021, draft strategy will attempt to address this shortcoming of its predecessors, prioritising the strengthening of (1) core infrastructure and (2) incident prevention and response capabilities, instead of trying to boil the ocean.[16]

[14] Piret Pernik concluded in a 2013 review that: there were insufficient links between strategic objectives and measures on the one hand and budgeting and resources on the other; there was a lack of coherence between the cybersecurity strategy and agencies' mandates and actual activities, and between the cybersecurity strategy and key state documents and government development plans; and the strategy duplicated other development plans. See Piret Pernik, *Küberjulgeoleku strateegia 2008–2013 analüüs* [Analysis of the cybersecurity strategy 2008–13] (Tallinn: Rahvusvaheline Kaitseuuringute Keskus, 2013), 5–6.

[15] Vaks, *Küberjulgeoleku strateegia mõju*, 29–30.

[16] Draft *Digital Society Development Plan 2030.*

2.3.2. Struggling with metrics

It is widely acknowledged that an actionable national cybersecurity strategy must be paired with quantifiable goals. According to the leading academic authorities in quality management studies, H. James Harrington and Thomas McNellis, "measurement is the first step that leads to control, and, eventually, to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."[17] However, attaching measurable quantities to strategic goals may turn out to be the most challenging task in strategic planning. A metrics system can fail for several reasons: the design of the metrics may be misaligned with strategic priorities or insufficient to address them; or there may be underlying data quality issues, overly ambiguous metrics, or insufficient monitoring, reporting and follow-up. The fact that cybersecurity is a discipline undergoing intense development does not make the task easier: what constitutes an adequate maturity level remains a moving target.

Failures, in turn, transfer to overall weaknesses in strategic planning and efficient governance. Poor data quality and misaligned or inadequate design of the metrics system may lead to communicating arbitrary information or miscommunication of the status quo to decision-makers. This in turn can lead to reactive escalation and disproportionate attention to specific facets of the security landscape, while ignoring the remainder of the spectrum. Aspects that are not measured – due, for example, to lack of data or measurement maturity – may become increasingly neglected and, as inadequately aligned metrics, can encourage a false sense of security regarding success or failure.

Estonia has seen many of these shortcomings in its strategic planning periods, from a lack of metrics and irrelevant metrics to insufficient attention and monitoring. A desire for comprehensive progress monitoring led to the inclusion of performance indicators in the 2014 strategy, even if analysis preceding their formulation was scant and the indicators themselves often appeared token in nature rather than substantial. Of course, such challenges were hardly unique; according to the Global Cybersecurity Index (GCI) 2017, a mere 21% of countries globally included some form of performance metrics in their cybersecurity strategy, while the indicator had significantly improved to 47% by time of the subsequent report.[18] It can be expected that the capacity and maturity for cybersecurity performance monitoring will improve along with the increasing maturity of the discipline as a whole.

Viewing cybersecurity strategy as a process, rather than simply an outcome document, strengthens connections between the government agencies involved, and also with non-government stakeholders that represent an essential pillar of national cybersecurity

Estonia has seen many shortcomings in its strategic planning periods, from a lack of metrics and irrelevant metrics to insufficient attention and monitoring

2.4. National strategy as a process, not just a document

Estonia has, from the onset, followed the principle of inclusiveness in the strategy development process, recognising the need to engage a wide range of stakeholders in both the strategy planning and implementation

[17] H. James Harrington and Thomas McNellis, "Mobilizing the Right Lean Metrics for Success," *Quality Digest,* May 2006, https://www.qualitydigest.com/may06/articles/02_article.shtml.

[18] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva: ITU-D, 2017), 27–37, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf; International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2018* (Geneva: ITU-D, 2018), 18. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

phases.[19] This has to do with Estonia's established approach to public policy and administration, in which those impacted by a policy choice must be given a chance to voice their views, but also recognising the role of private-sector stakeholders as providers of essential services, and their unique knowledge and expertise.[20] Viewing cybersecurity strategy as a process, rather than simply an outcome document, strengthens connections between the government agencies involved, and also with non-government stakeholders that represent an essential pillar of national cybersecurity.

Bringing together all stakeholders and enabling interconnected dialogue on strategic directions and collaboration tools may in the end be more impactful than concluding an eloquent, academically sound document. In terms of producing sustained effect, a meaningful, engaged process has proved a deliverable in its own right: the process of producing Estonia's first cybersecurity strategy in 2008 was considered among its most important achievements as it brought together state institutions and strengthened the government's cooperation with private companies and educational institutions.[21] Experts interviewed for a 2018 study viewed the strategy preparation and implementation process as having strengthened Estonia's cybersecurity posture, as the effort created both a structure to address cyber issues and a platform for recognising key problems and identifying solutions in a concerted manner. There was an almost unanimous view that the process and outcome alike were key factors in achieving a systematic approach and gaining broad public and political recognition for cybersecurity as a matter of public and national security.[22] In addition, the strategy process helps uphold a broader public interest in finding solutions to the sector's challenges – which stimulates developments even beyond the objectives and measures directly addressed in the strategy text itself. [23]

Pursuing intense stakeholder involvement as a priority comes at a cost: it makes the document relatively expensive to produce and the process is lengthy and potentially chaotic. At the same time, academic quality might be lost compared to having a few strategic planning consultants putting the document together without "messy" discussions. One may be tempted to consider procuring a strategy from planning experts or copying from leading strategies around the world. However, the effort put into intense stakeholder management brings proportionate value in terms of community commitment. Despite the time and resource intensity of the preparation and implementation of strategies, it enables systematic management of the developments and is hence expedient from the point of view of the state, presumably not only in Estonia but also in other countries.[24]

The effort put into intense stakeholder management brings proportionate value in terms of community commitment

2.5. The strategy as a tool for international collaboration

The publication of cybersecurity strategies plays an important role in declaring national priorities and explaining them to stakeholders and partners, thereby defining and legitimising the presence and purposes of the public administration in this domain.[25] Beyond publishing them for the awareness of its domestic stakeholders, Estonia has tried to make all three of its cybersecurity strategy documents accessible online to a broad international audience, translating them into English. This provides a meaningful disclosure of the planned activities and a reasonable level of understanding of the underlying process.

[19] *Inclusiveness* is recognised as one of the nine overarching principles of strategic cybersecurity, acknowledging that the strategy should be developed with the active participation of all relevant stakeholders and should address their needs and responsibilities. See International Telecommunication Union et al, *Guide to Developing a National Cybersecurity Strategy,* 31.

[20] Pursuant to the Administrative Procedure Act, § 40. See Riigikogu, "Administrative Procedure Act," *Riigi Teataja* (State Gazette), RT I 2001, 58, 354 (27 March 2019) (translation), https://www.riigiteataja.ee/en/eli/527032019002/consolide. Similar provisions exist in sectoral acts, e.g. regulation of the telecommunications market, spatial planning.

[21] Pernik, *Küberjulgeoleku strateegia,* 29.

[22] Vaks, *Küberjulgeoleku strateegia mõju*, 49.

[23] Ibid., 53.

[24] Ibid.

[25] Ibid., 49.

The sharing of information by states on their national cybersecurity strategies is recognised as one of the confidence-building measures defined by the Organisation for Security and Cooperation in Europe (OSCE) in 2016.[26]

Such international transparency makes the strategy document a useful tool in communication with international counterparts for identifying the collaborative potential of dialogue partners, supporting global capacity-building efforts and, not least, upholding a country's standing as a trusted, open and valuable partner. Estonia considers its reputation as a capable partner and a clear voice in the international arena as an asset supporting the exchange of information and knowledge with strategic partners, thereby strengthening its strategic objectives and values.[27]

Conclusions

Studies confirm that both Estonia's cybersecurity strategies and the strategy development process as a whole have had a tangible, positive impact on Estonia's cybersecurity capacity development. Both cybersecurity as an outcome and the strategic planning process have been pursued as nationwide, multi-stakeholder processes in which the private sector and other stakeholders have been engaged.[28]

Estonia's successes and failures in developing and implementing national cybersecurity strategies point to several universally applicable aspects. Based on this experience, we have chosen to highlight the five most relevant deliverables, along with related challenges:

- **Defining a successful governance model.** The decentralised governance model pursued by Estonia has its benefits and challenges. While organisations' broad autonomy stimulates partnerships, the consistency of actions and efficient use of resources are difficult, requiring particular attention to the division of responsibilities, coordination, and mechanisms for decision-making;

- **Providing long-term vision and fundamental principles** to guide value-driven strategic development that remains consistent across strategy periods, yet is open to revision and adjustment where justified;

- **Setting actionable and realistic strategic objectives**, along with a comprehensive system of metrics that help to understand, control and improve performance, and ensuring the necessary focus and prioritisation;

- **Investing in cybersecurity strategy as a process** in order to ensure close involvement of stakeholder groups and a strong community, and resisting the temptation to merely settle for a presentable document;

- **Communicating national priorities** to international stakeholders and partners.

It is hoped that such candid discussion of the successes and failures of the national cybersecurity strategic planning experience will have practical educational value for those analysing their own success in implementing cybersecurity strategy and defining its future objectives and priorities, and revising the viability of long-term vision and principles.

There are undoubtedly many differences between Japan and Estonia: size, demographics and population density, economic structure, public administration and policy tradition, and history. Yet in terms of both the reliance of society on digital infrastructure, the significance of cybersecurity for societal resilience, and the vital importance of rules-based cyberspace and effective international cooperation and information sharing, they have plenty in common. Japan has been a prime dialogue partner for Estonia in the Asia-Pacific region, and the mutual sharing of information and lessons learned in the area of cybersecurity has benefited both parties. Given the value of such exchanges, we hope this chapter will contribute to their continuation on the strategic planning level, strengthening the cyber resilience of both countries.

[26] Organisation for Security and Co-operation in Europe (OSCE), "Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," *PC Journal*, No. 1092, 10 March 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf.

[27] Ministry of Economic Affairs and Communications, *Cybersecurity Strategy 2019-2022,* Section 1.3 and Objective 3.

[28] Vaks, *Küberjulgeoleku strateegia mõju*, 53.