EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES • POLICY REVIEWS • OPINIONS

THE KOSSUSZKO INSTITUTE
The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments.

**EDITORIAL BOARD**

**Chief Editor:** Dr Joanna Świątkowska  
**CYBERSEC Programme Director and Senior Research Fellow of the Kosciuszko Institute, Poland**

**Honorary Member of the Board:** Dr James Lewis  
**Director and Senior Fellow of the Strategic Technologies Program, Center for Strategic and International Studies (CSIS), USA**

**Member of the Board:** Alexander Klimburg  
**Nonresident Senior Fellow, Cyber Statecraft Initiative, Atlantic Council; Affiliate, Belfer Center of Harvard Kennedy School, USA**

**Member of the Board:** Helena Raud  
**Member of the Board of the European Cybersecurity Initiative, Estonia**

**Member of the Board:** Keir Giles  
**Director of the Conflict Studies Research Centre (CSRC), UK**

**Editor Associate:** Izabela Albrycht  
**Chairperson of the Kosciuszko Institute, Poland**

**Executive Editor:** Karine Szotowski  
**Designer:** Paweł Wałkowiak | perceptika.pl

**Proofreading:** Justyna Kruk and Agata Ostrowska

**ISSN:** 2450-21113

**Disclaimer:** The views expressed in articles are the authors’ and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

© 2017 The Kosciuszko Institute  
All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.
The current issue of the European Cybersecurity Journal (ECJ) is being published during the 3rd edition of the European Cybersecurity Forum – CYBERSEC. The main motto of this year’s conference, ‘Dealing with Cyber Disruption’ reflects the key messages of the articles included in this ECJ.

Disruption is all about change – it can lead to destructive but also creative consequences. Modifications caused by digital technologies are exceptional, as they tend to significantly influence almost all aspects of our reality. Articles in the current issue of ECJ illustrate this conviction, thus providing readers with analyses of various disruptions caused by actions conducted in cyberspace.

We will have a chance to examine the constantly evolving threats landscape with a special focus on the recent ransomware attacks. We will also learn more about countermeasures that may be used to stop them. But digital technologies are not only about technical security of ICT systems. They are also about the changes that must occur within our traditional systems, including legal ones. One of the texts therefore provides us with a closer look at proposals aimed at increasing the effectiveness of the rules governing law enforcement access to digital evidence in a timely manner in order to prevent or investigate criminal and terrorist acts.

Another article focuses on one of the most burning problems that modern democracies face: cybersecurity of e-voting. This area requires increased attention from not only cybersecurity experts but also decision makers.

This issue of ECJ reveals a different nature of changes caused by the digital world, as cyberspace disturbs international relations and global peace and stability. Apart from investigating the problem, concrete initiatives aimed at reducing risk are provided in one of the articles dedicated to this issue as well as the interview conducted with H.E. Marina Kaljurand. Ensuring security in cyberspace requires strategies, relevant tools, and changes in terms of a qualified workforce. One article presented in this ECJ evaluates this need and calls for rapid and decisive action.

Finally, cyberspace has disturbed the traditional manner in which policies designed to face cyberthreats are created and implemented. Cyberspace has reshaped the status quo of main stakeholders and their power. Today, actions undertaken solely by state entities are insufficient. Multistakeholder engagement is needed and required. This approach will also be examined.

Even though a variety of approaches are covered in the current issue of ECJ, it is obvious that only a small piece of the landscape of changes has been analysed. We know very well that this is continuous process that needs to be repeated over time. We will do just that in subsequent issues of ECJ as well as through other editions of CYBERSEC.

Please join us in this journey.
CONTENTS

5 INTERVIEW
H. E. Marina Kaljurand

10 A MULTISTAKEHOLDER APPROACH TO CYBERSECURITY POLICY DEVELOPMENT
Lea Kaspar and Matthew Shears

15 GROWING THE NEXT GENERATION OF CYBER PROFESSIONALS
Brooke Griffith

20 INTERVIEW
Liis Vihul

22 DIGITAL SECURITY & DUE PROCESS: MODERNIZING CROSS-BORDER GOVERNMENT ACCESS STANDARDS FOR THE CLOUD ERA
Kent Walker

34 ALL ELECTIONS ARE HACKABLE: SCALABLE LESSONS FROM SECURE I-VOTING AND GLOBAL ELECTION HACKS
Liisa Past

48 WHAT CAN WE LEARN FROM WANNACRY AND NYETYA?
Lothar Renner

53 CYBERSPACE AND INTERNATIONAL RELATIONS: DIPLOMATIC INITIATIVES TO AVOID THE RISK OF ESCALATION IN THE CYBER ARENA
Luigi Martino
“There’s been a lot of claims that our election system is unhackable. That’s BS. Only a fool or liar would try to claim that their database or machine was unhackable,” said Jake Braun of DefCon 2017 hacker voting village where the participants successfully compromised a number of voting machines.

Like traditional paper ballots at a polling station, no electronic election technology is 100% secure 100% of the time. Just as with ensuring the uniformity, secrecy and integrity of the conventional voting process, a multitude of measures can be taken to prevent, detect, manage and mitigate risks of using election technology and, in particular, online voting. While the risks can be different from conventional paper ballots and thus require specific mitigation, they are not greater, as the Estonian experience has demonstrated through the past dozen years.

Electronic voting components are common in different election systems and can be defined as “use of electronic means to record, process, or tally votes.” Internet voting is one of these technologies. Here and...
henceforth the terms “I-voting” and “online voting” are used interchangeably to mean the process of recording votes remotely using internet-connected computers. Some literature refers to I-voting as “e-voting,” but unless in a direct quote, that term is generally avoided here to distinguish between use of electronic voting components (such as voting machines, electronic tallying etc.) and remote online voting.

**Background: Global Election Hacks**

Election technology has, in the past year, come to the focus because of increasing attempts, attributed to nation states or entities commanded by nation states, to influence elections and campaigns across the world. This “election hacking” denotes phenomena ranging from e-mail leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance or voting systems.

This “election hacking” denotes phenomena ranging from e-mail leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance or voting systems.

Often coupled with intense information operations, these cyber attacks on systems linked to campaigns and elections mean the adversary does not shy away from directly influencing the fundamental democratic processes of another nation. This has serious implications for liberal-democracies and how technology is used in the electoral process, what the security processes and standards should be and, perhaps most importantly, the political and legislative will to continue with and introduce new election technology initiatives across nations.

Through this adversarial strategy involving an intelligence-led and politically directed campaign, cyber attacks on elections are inherently integrated, combining, for example, cyber, influence, psychological, and information operations. Bill Priestap of the FBI’s Counterintelligence Division makes it clear that “Russia’s 2016 Presidential election influence effort was its boldest to date in the United States. Moscow employed a multi-faceted approach intended to undermine confidence in our democratic process. Russia’s activities included efforts to discredit Secretary Clinton and to publicly contrast her unfavorably with President Trump. This Russian effort included the weaponization of stolen cyber information, the use of Russia’s English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging”6.

The most prominent attacks on the US (2016) and French (2017) Presidential elections have most visibly targeted the campaigns and candidates. While there is no evidence that the vote recording or tallying might have been tampered with in the US7 or in other nations, such attacks do undermine the voter confidence and the legitimacy of an elected government by sowing doubt in political players and the body politic. This, in turn, helps to possibly delegitimize elected leaders, their decisions, and the government.

To meddle in the internal affairs of a nation or at least attempt to influence electoral behavior, the electoral process need not to be compromised at all in these hybrid scenarios. It is sufficient to attack, for example, prominent political players or widely used (government) e-services to raise questions regarding the reliance on electronic solutions and the social, political and economic institutions supporting such digital ways of life.

---


7 | Ibidem.
The efforts mounted during the 2016-2017 elections can also be groundwork for more advanced cyber attacks that could potentially impact electoral rolls or vote recording and tallying. Attempts to access state systems were identified in at least 21 US states in 2016 with data said to have been copied for mapping purposes or to plan future attacks. Compromised voter registration and campaign finance systems were later reported in at least 39 states with targets including election technology vendors. The effects are real – claims of tampering with election technology led Venezuela to political unrest in August 2017.

It should be noted, however, that domestic and foreign attempts to influence elections have not been brought about by election technology. Rather, election technology has become another domain in which voters exercise their rights and therefore for those who wish to suppress or interfere with those rights to further their goals.

With proper security, logs, verification, auditing and other safeguards, election technology allows for detecting irregularities – be it network traffic characteristic to a DDoS attack or tampering with votes or databases – and therefore mitigating their potentially devastating impact. In the Venezuelan case, a technology vendor published claims of tampering with the explanation that the election system is designed to be "tamper evident and self-reports any attempt to interfere with it. This means that the system is designed to protect the votes from any manipulation and to immediately identify and alert of such an attempt."

Given its fundamental role in the functioning of a representative democracy, election technology needs to be viewed in the wider context.

While the focus of this analysis is election technology itself, rather than the attacks, including cyber and information operations, against campaigns and political players, these cases need to be reviewed and serve to highlight that election technology cannot be viewed, analyzed and secured in isolation. Given its fundamental role in the functioning of a representative democracy, election technology needs to be viewed in the wider context. Risk assessment, as well as management decisions and steps taken to manage and mitigate risks related to election technology, need to take a holistic view and view the whole process with the understanding that the entirety of a liberal democratic process is viewed as an attack surface.

Such a comprehensive view or risk management is particularly important, as a politically motivated or state-backed attacker in cyberspace can generally take a longer-term perspective (a system may be compromised over an extended period of time) and maintain suitable resources for using a range of techniques and technologies. This allows the attacker to go undetected and employ an opportunistic and reactive strategy.

Combining that and the highly integrated nature of attacks against elections and campaigns, means that

a liberal democracy, if it is to succeed, needs to also take a holistic and comprehensive approach, encompassing strategic communication and democratic education as much as securing the technology. This, as demonstrated by multiple campaigns in 2016, includes improving the cyber hygiene, awareness, capacity building and operational security of political actors and candidates, allowing them to take a comprehensive approach that encompasses cyber security as well. While these factors will not be examined further here, they do need to be taken into account.

1. Remote Voting Technology Across the World

I-voting (or online voting) is fundamentally different from election technologies discussed so far. Estonia, the Netherlands, Canada and Australia have, among others, tested remote online voting. Many nations, most notably Germany and Switzerland, use a remote ballot system by mail. Online voting generally mimics such remote voting. While approaches vary, the commonalities are:

- Identification: Voters need to be identified to access the voting system. Estonia uses a secure digital identity (further elaborated below) while several nations have experimented with distributing credentials through mail, e-mail or SMS message, all distinctly less secure. Others have relied on identification through online banking, creating dependencies on a private sector service. Whatever the identification scheme (including no compulsory identification), it is both a live dependency as well as a possible attack vector of elections, digital or otherwise.

- Legal framework and political will: an election organizer has to ensure that the legal requirements for elections (secrecy, universality, integrity, security etc.) are met across the voting platforms, be it voting online, at the voting booth or having access to the ballot box otherwise. Several nations have put online voting, sometimes after a trial, on hold until courts or the legislator offer legal certainty, or political parties come to a consensus.

- Security: an election organizer has to ensure that the security requirements are met on par with voting at the polling place when implementing a remote voting solution.

None of these issues are unique to elections but rather environmental. Security, identification, and legal frameworks are required for all e-services and ways of casting a vote, therefore online voting benefits from – and fits into – a wider ecosystem.

2. Factors Facilitating I-voting Based on the Estonian Experience

Estonia was the first country to introduce I-voting in 2005 and has followed a unique path where the votes can be cast online during the early voting period. With the municipal elections of October 2017 being the ninth chance to vote online in a dozen years, the proportion of online voters has plateaued at a third (31.3% at the 2014 European Parliament elections and 30.5% at the 2015 parliamentary elections), a steady increase from 1.9% in the first-ever I-vote in 2005. In this time Estonia has "established a trust relationship" with voters.

2.1 I-voting Framework

§ 60 and § 156 of the Estonian Constitution dictates that elections are ‘general, uniform and direct’ with

While published during the Estonian 2017 election period, this paper is written before the municipal elections and therefore does not include data for the October 15, 2017 vote. The Estonian State Electoral Office is expected to have most up-to-date data available on www.valimised.ee/en.
voting being secret\textsuperscript{17} and all voting methods have to adhere to this standard. Early voting is no exception and the requirements are the same whether the voter is casting an absentee ballot at a designated pre-voting polling station, requesting a ballot box to their place of residence or i-voting\textsuperscript{18}.

I-voting opens for seven days (10th-4th day before election day) and mimics double-envelope (postal) voting “where the inner, privacy-providing envelope is replaced by encrypting the vote using the central system’s public key, and the outer authenticity and integrity layer is provided by signing the vote cryptogram with the voter’s ID card”\textsuperscript{19}. The votes are only opened and tallied once the personal information (digital signature or “outer envelope”) is removed\textsuperscript{20} and that happens on an “offline and air-gapped server”\textsuperscript{21}.

2.2 Security Measures by Design

Since introducing i-voting in 2005, Estonia has not seen a single significant technical or security incident influencing voting outcomes\textsuperscript{22}. In addition to the election procedures described above\textsuperscript{23}, the following principles have been followed:

- Reliance on existing ecosystem, including for identification and authentication of voters: Estonia relies fully on the state-backed secure digital identity (either ID-card or crypto-SIM-card-based) to identify voters online and allow them to digitally sign the electronic double envelope used to cast the Internet vote. This live dependency, explored further in the ecosystem subchapter of this paper, cannot be removed unless the voter identification requirement as such is removed. Additionally, Estonia relies on a digital population registry as one of the bases for all e-governance.

- Repeat voting: An i-voter can re-vote as many times as they would like and only the latest vote counts, with a paper ballot taking priority over online vote\textsuperscript{24}.

- Procedural controls “defining the main manual activities and practices that election officials engage in”\textsuperscript{25} are a core component of i-voting and documented in the election manual and security policy available (mostly in Estonian) on the elections website\textsuperscript{26}. Estonia relies heavily on these procedures focusing on data integrity between parts of the system, access control and mechanisms for dispute resolution and system continuity\textsuperscript{27}. Additionally, dispute resolution is designed to be fast, so as to not hinder the election process\textsuperscript{28}.


\textsuperscript{21} | Nurse, et al., op. cit., p.4.

\textsuperscript{22} | Author’s interviews, op. cit.


\textsuperscript{24} | Nurse, et al., op. cit. pp. 5-6.


\textsuperscript{26} | Nurse, et al., op. cit.

\textsuperscript{27} | Author’s interviews, op. cit.
• Constant feedback and improvement: While a more formalized lessons-learned structure would be desired, Estonian election organizers have shown flexibility and agility in constantly improving I-voting. The improvements have, amongst other input, been based on events and feedback, be it academic study, OSCE reports or heads-up from technology experts.

• Transparency measures have had a noteworthy impact on building confidence and trust in the I-voting system. This "aggressive openness" means that:

<table>
<thead>
<tr>
<th>Estonia publishes most of the I-voting documentation on the elections website (with the main exception being materials that expose vulnerabilities).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonia publishes the source code of the I-voting software on the open-source coding platform GitHub starting from 2013. As a security precaution, the uploaded repository is not used for further development but is the &quot;up-to-date code used in elections&quot;. The 2017 code is to be published after testing.</td>
</tr>
<tr>
<td>Estonia invites feedback from the technology community and Estonia’s volunteer Cyber Defense League in addition to formalized testing.</td>
</tr>
<tr>
<td>Estonia makes election procedures public and observable and parts of the system audited, all meeting standards similar to voting procedures at a polling station.</td>
</tr>
</tbody>
</table>

• Vote verification allows confirmation of whether “vote was cast as intended” and therefore enables detection when the computer had been compromised in a way that “changes the I-vote or blocks the I-voting”. Verification through separate devices (in Estonia’s case computer and smartphone) makes vote hijacking on a large scale more difficult.

• Estonia owns the software: Procured through a public tender, the Estonian election organizers own the I-voting software, allowing them to develop it as needed. The code base for Estonian I-voting is separate from the commercial products of the developer, thus mitigating the risk of another customer discovering, withholding and exploiting vulnerabilities.

• Testing: a public dummy demonstration is used as a functionality test about a month before Election Day. Security/penetration testing is to be carried out as new software is introduced.

• Traffic monitoring: CERT_EE, the body responsible for managing security incidents in the .ee domain, is engaged in the I-voting task force and monitors the network traffic to detect any anomalies, including possible DDoS attacks. Tools and ways to monitor logs are also constantly improved and developed.

While voting in a location outside of the polling station without the presence of polling workers does create risks, majority of the user-caused risks are not scalable and the procedures and safeguards described mitigate those risks. Additionally, the agencies involved put an effort into cyber hygiene awareness raising to remind voters of proper use of digital identity (for example: do not share your pin codes, use trusted computers).

Fundamentally, I-voting taking place in the pre-election period offers a time buffer that allows for reverting to universal paper vote on Voting Day should the remote voting not meet standards or incidents occur. While

28 | Nurse, et al., op. cit.
29 | Author’s interviews, op. cit.
30 | Nurse, et al., op. cit., p. 3.
31 | Author’s interviews, op. cit.
33 | I-voting on GitHub, op. cit.
34 | For more see www.kaitseliit.ee/en/cyber-unit.
35 | Author’s interviews, op. cit.
36 | Vassil, op. cit., p. 10.
38 | Nurse, et al., op. cit.
unlikely, the procedures (including availability of sufficient number of paper ballots and staffing at polling stations as well as legal procedures) are in place for such an eventuality. This also highlights that the reasonable way to approach I-voting is to see it as an option, allowing voters a diversity of choices, rather than the only way to collect votes.

2.3 Comprehensive Risk Assessment

In the past, the risk assessment of the I-voting systems had focused on the threats under the direct control of the election organizers (including technical risks stemming from the software). Given the changed threat landscape and adversary’s hybrid tactics, a more comprehensive risk assessment approach was introduced in 2017 to be able to mitigate risks arising from third parties and world politics as well as the lively digital ecosystem encompassing both Estonian e-governance solutions (including ID-card, population registry etc.) as well as third parties involved in the development and distribution of these solutions.

This is particularly important, as the legitimacy of the elections does not only depend on the technical execution of voting procedures. This approach also accounts for and suggests ways of mitigating risks arising from information/hybrid attacks, dependencies on the ecosystem, management issues, introducing new online voting software, the impact of a large group of first-time voters (for the first time, Estonia invites 16-18-year-olds to the polls) and other factors outside the direct control of the election organizers. The assessment includes dependencies on outside systems and services as well as ways to identify, manage and mitigate them, including approaches to transparent communication.

It is hoped that such a comprehensive approach, particularly as it was introduced early in the planning period, allows prioritization of tasks and resources according to their potential impact. The shared understanding of landscape brings parties involved to the same page in planning and management terms, thus allowing for better responses to eventualities as they arise.

2.4 Reliance on Existing Ecosystem

I-voting in Estonia is facilitated by a lively ecosystem on government e-services and a secure digital identity that all Estonians and residents carry.

The ID-card is the fundamental live dependency of I-voting, similar to identity documentation in voting at a polling station. The smart-card/chip-and-pin-based government-backed digitally usable identity document is supplemented by mobile-ID, a SIM-card based solution with equal guarantee. An additional electronic-use-only card is also available.

Digital ID identification/authentication is used to identify the voter online and allow them to cast and sign their vote. Card readers are widely available at a reasonable price. They are a standard feature on new computers and common in public and office workstations. The procedure of voter identification during I-voting is described in detail on the website of the Estonian elections.

Voter rolls, alike other personalized e-services are based on the Population Register, the uniform government database of primary personal data “such as the name, address and personal identification code” of citizens and legal residents. The register includes documents related to the Family Act and residence and is interlinked with and draws upon numerous government e-services.

Estonia’s legal framework is “designed to work seamlessly with the technological solutions of e-government.” A robust data exchange layer or “middle-ware system” (the “x-tee” or x-road) seeks to minimize repetitive data collection, improve interconnectedness of the state’s services.

---

39 Author’s interviews, op. cit.

40 Internet Voting in Estonia, op. cit.

41 Ibidem.

42 Republic of Estonia, Population Register from July 2017 on IT and Development Centre of the Ministry of the Interior.

43 Ibidem.

database and avoids the time-consuming dealing with paper data entry and verification. This digital public administration lays groundwork for all government e-services, I-voting included.

I-voting in Estonia is facilitated by a lively ecosystem on government e-services and a secure digital identity that all Estonians and residents carry.

The voter database therefore does not need to be prepared separately. Instead, the Population Register has an up-to-date database of those eligible to vote in particular elections and the “electronic lists of voters shall be sent to the State Electoral Office not later than by the thirteenth day before Election Day.” Providing the voter lists in good time before voting procedures also means there is no live reliance on the Population Register and problems with or attacks against the database will not influence I-voting.

These interconnected solutions create an ecosystem allowing I-voting, and it would be difficult to even conceptualize it without the described elements. At the same time, the reliance on these services creates a critical dependency for I-voting. In the case of the digital identity, the dependency is necessarily a real-time live one that can be mitigated but not overcome. Whatever model of identification and authentication voting uses becomes a critical dependency for the availability of voting.

2.5 I-voter Is an Average Voter

“For the first three elections multiple socio-demographic, attitudinal, and behavioral factors had a non-trivial association with being a first-time e-voter. However, from the fourth election onward, the importance of these factors gradually diminished, indicating the diffusion of e-voting among the Estonian electorate.”

In Estonia, the I-voter does not differ from the statistically average voter in almost any way and no socioeconomic factor (gender, income, education or nationality) predicts online voting. Even “computer literacy is no longer a clear driver of e-voting and thresholds set by modest skill level can over time be overcome with handily designed e-voting systems.”

Political preferences play no significant role in predicting participation in I-voting, meaning that, contrary to popular belief, no political party or their voter base is (dis)advantaged by I-voting. Once normalized, the only predictor of I-voting is the distance to a polling station, as the technological solution offsets the cost of voting. “The critical limit is a 30 minute round trip to the ballot station, anything above that makes e-voting already more probable than voting at the polling station.”

Most recent research based on Estonian data suggests I-voting “to be very “sticky”; a first time e-voter is very likely to stay e-voting in subsequent elections at consistently higher rates than a typical paper voter is to stay paper voting, or a non-voter to remain a non-voter.” As a result, the potential of I-voting in boosting turnout remains to be explored, with the potential clearly outlined.

---

49 | Vassil K., and Solvak M., (a), op. cit., p. 65.
50 | Vassil K., and Solvak M., (a), op. cit., p. 69.
3. Scalability and Best Practice

Estonia serves as a case study and potential testing ground for e-services and digital government solutions as “smaller countries with strong institutions can create high value as early adopters and create a demonstration effect for the world by assembling the right ecosystem.” This section looks at measures beyond the descriptions above to offer suggestions that would scale to larger societies seeking to protect election technology or introduce i-voting.

These measures focus on the social, legal and governance aspects and do need to be supplemented by both sound technical basis as well as a comprehensive risk management as described above. The Estonian strategy of transparency and publication of documentation serves a security purpose; supplementing risk assessment (including mapping of dependencies), clear procedures, testing and security by design. The Estonian approach is described above, with best practices outlined. Almost all the security precautions of i-voting are scalable to larger systems.

3.1 Start Small, Start Slow

The Estonian solution is particularly fitting in societies with few legacy systems and a lively ecosystem of (government) e-services, basic information infrastructure for secure electronic identity, and a national secure data exchange layer to facilitate communication between the systems listed above. As governments might move in that direction, their e-services cannot exist in isolation. In Estonia’s case, “the involvement of private banks was pivotal with regard to the success of the ID-card, both regarding societal awareness and the actual distribution of cards.” As the banks relied on the ID-card infrastructure to identify and authenticate their clients, it built trust and formed habits of using online services with the government-backed digital ID. For countries where such ecosystem is not as fully developed, focusing on a basic level of services and information infrastructure would be advisable before introducing i-voting.

I-voting in national elections is a monumental task and governments would be well advised to start small, either with non-binding polls, or with provincial elections.

Similarly, i-voting in national elections is a monumental task and governments would be well advised to start small, either with non-binding polls, or with provincial elections. This also offers potential for dispersed populations, whether nations with large diaspora or tribal elections in sparsely populated areas. A gradual approach allows for streamlining the process, and builds up trust at the heart of citizens’ willingness to adopt i-voting that forms habits.

A gradual process ensures that i-voting and other election innovation is built to supplement the paper ballot voting, not at its expense. The paper ballot is fundamental to elections and will remain an advisable backup because “paper gives election officials a way a deliver a correct results” in case of technology failures.

“Due to its slow take-off pace at the beginning,” governments adopting election technology should allow time to assess the progress and potential. The Estonian experience is most encouraging, as it took only three

55 | [CITATION Anu17 \l 1061].
elections for I-voting to fully diffuse. It is sometimes also hoped that I-voting would increase turnout by making voting easier. The Estonian experience reaffirms that while technology can enable political participation, it does not remove other barriers to participation. Thus governments are best advised to introduce technology hand-in-hand with other voter inclusiveness measures, not instead of them.

3.2 Comprehensive Approach and Stakeholderism

Given modern threats, including hybrid attacks against elections and the fundamentality of elections to citizens’ rights, election technology and I-voting benefit from a comprehensive and cross-government approach. The discussion of risk management above showed that, as the target of the attacks is the legitimacy of a democratic process, detection and mitigation has to draw on a comprehensive toolbox of measures far wider than just technical tools to defend the democratic process and its participants.

Simply put, the planning assumption needs to be that the adversary will make all or any attempts to delegitimize a democratic process and its participants. Therefore, election organizers need to accept and mitigate or prepare for risks that are outside their control, such as e-mail leaks or website defacements or attacks against vendors and work with all stakeholders and possible targets to mitigate those risks.

Given modern threats, including hybrid attacks against elections and the fundamentality of elections to citizens’ rights, election technology and I-voting benefit from a comprehensive and cross-government approach.

Secondly, functioning of elections cannot be up to only the elections organizers tasked with the technical execution. A multi-stakeholder approach, where all those involved in the electoral process have to be on board, means coordination and integrated (communication) management. In Estonia, for example, I-voting is managed by a task force that brings together the election organizer, the Information System Authority, the service providers I-voting relies on, and the software developer. Communication is managed by a team comprising of representatives of the election organizer, the government office and, in the case of I-voting, the Information System Authority.

Regardless of their particular approach, all governments and election authorities need to constantly monitor and account for the ever-changing threat landscape. Lawrence Norden, co-author of the "Securing Elections From Foreign Interference" report by New York University School of Law’s Brennan Center, said, "Threats are moving so much more quickly and I think that hasn’t really sunk in for a lot of people."

---

58 | Vassil K., and Solvak M. (a), op. cit., p. 57.
60 | Estonian National Electoral Committee, Riigi Teataja from June 2017 on Organization of I-voting (Elektroonilise hääletamise organisatsiooni kirjeldus).
Therefore there is a need to be well resourced, agile and flexible enough for systems and practices to be developed as new threats and attack vectors emerge.

In addition to functionality and security testing, outside critics and hackers can be embraced by election organizers to test election technology. For example, the Los Angeles County administrators took active interest in the DefCon hacking conference in July 2017 by planning to “invite the hackers to attack the proposed system as a test down the line – to ‘kick the tires’, as part of a wider effort to redesign the electronic elements of voting”.

These additional testers provide an extra pair of eyes, likely to discover or confirm vulnerabilities. As no testing methodology replicates another one, strength can play out in numbers. As security researcher T.J. Horner explained at DefCon, commercial testing might not be “as thorough or as public as the work” done at the hacker conference we did at the village. Therefore, it is important “to have a really broad range of people, a broad community, looking at this kind of technology if you have any hope of wanting to trust it to do something serious”.

3.3 Transparent Risk Management

Risks and vulnerabilities need to be openly addressed in public communication as the illusion of absolute security will undermine the election process as the first incident inevitably takes place. It often means communicating risks and vulnerabilities of technology, however theoretical, to an audience that is more accustomed to judging outcomes. In Estonia in 2017, a theoretical security vulnerability arising from the ID-card firmware became known to the Information System Authority about six weeks before the elections and just over a month before I-voting.

This vulnerability, while theoretical, impacted more than half of all ID cards in circulation. While I-voting is also possible using the state-backed but less common mobile-ID and digital-ID, the risk, if materialized would have an instantaneous effect on I-voting, given the live dependency on the digital identity scheme. In addition to mitigating the potential risks and fixing the vulnerability, the authorities involved opted for open and transparent proactive risk management strategy where civil service, decision makers, international partners, the media, and the public were informed of the vulnerability as well as the risks involved, the steps to overcome. This included a cross-government communication approach, cooperation between agencies, cooperation with the appropriate international agencies and corporations, etc.

3.4 Documentation and Procedures

While Estonia has established sufficient and fast dispute resolution and “crucial procedures are clearly documented”, “sustainability of existing security procedures, particularly with reference to knowledge definition and transfer is considered problematic. Furthermore, Estonia’s small committed staff means that those involved “already know what to do,” as an interviewee said, and “in some cases incidents and feedback reports appear to be addressed in a somewhat informal way,” thus creating a potential sustainability and replication issue.

These risks can be mitigated by added procedural formality and thorough documentation, including in organizational (including roles, cooperation formats) and technical details (including routines, configurations). Such lessons that are learned, including incident handling...
and other documentation would make the process less dependent on seasoned professionals and add clarity to planning, which would better allow for preparation for expectancies as well as the allocation of resources.

The same routines, to a great degree, mitigate human risks, including reliance on a single individual and the possibility of an insider threat. In the Estonian case, insider threats “may be unlikely given the relationships and professional trust”\(^7\), but it should not be overlooked. For larger nations, comprehensive documentation is useful in addition to advanced vetting of personnel and further security procedures.

### 3.5 Voter Education

The voter is generally viewed as “the most vulnerable link in the I-voting system”\(^7\), and Estonia has taken a number of measures have been taken to mitigate this. Voter education cannot focus on the particular technology (I-voting happening less than once a year does not incentivize specific leaning) but rather basic cyber hygiene.

Voter education cannot focus on the particular technology but rather basic cyber hygiene.

Awareness is a key factor in building trust in the system, therefore driving habit formation. In addition to the “significant amount of detail on the system online”\(^7\), wider voter education campaigns are needed. Uninformed voters will not adopt the I-voting technology or, as Cybernetica (the provider of Estonian I-voting software) highlights, voters’ lack of awareness of their responsibility for the safe conducting of the voting procedures\(^7\) contributes to risks in carrying out the election procedures.

Similar to any information system or network, the confidentiality, integrity and availability of election technology and data can only be assured if resources are available, including competent staff and sufficient funding. In many ways, therefore, voting technology is not unique and governments are empowered to make sure the process is secure, whether electronic or on paper.

However, given the fundamental importance of elections in a democracy, governments might wish to set clearer standards in wishing to ensure the security of electoral process. This can be done by implementing baseline security standards (including appropriate reporting and auditing) or designating elections, voting, or services

### 3.6 Legal framework

“Legislative efforts which typically follow technological developments are fundamental for the adoption and implementation\(^7\) of voting technology. As election technology is expanding an existing practice of exercising democratic rights into a new digital domain, the legislator and courts will need to test the constitutionality of election technology to prove that they meet the legal standards and requirements for free and fair elections. The language varies somewhat nation-to-nation, but any voting mechanism will need to meet the requirements of general, uniform and direct elections with the individual vote being secure. The organizer of the elections has to assure the voter’s freedom to cast their vote as preferred as well as transparency, accountability (including correct tallying with appropriate auditing, verification and observation processes in place) and public confidence in the elections.

However, given the fundamental importance of elections in a democracy, governments might wish to set clearer standards in wishing to ensure the security of electoral process. This can be done by implementing baseline security standards (including appropriate reporting and auditing) or designating elections, voting, or services

\(^7\) Nurse, et al., op. cit. p.6.
\(^7\) Nurse, et al., op. cit. p.7.
\(^7\) Nurse, et al., op. cit. p.9.
\(^7\) Heiberg S., and Willemson J., Modelling Attacks Against I-Voting (Elektroonilise hääletamise vastaste rünnete modeleerimine), Tallinn 2011.

\(^7\) Nurse, et al., op. cit., p.11.
elections rely upon (population databases, digital identity) and connection between these elements as critical information infrastructure or essential service. In some nations, local legislation might foresee other mechanism to mandate thorough security standards. Regardless of the approach, these measures are only effective if married to resources to properly implement them.

“Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law,” the former US Secretary of Homeland Security, Jeh Johnson, has argued. The definition of “election infrastructure” in this context is a comprehensive one: “storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.”

While such moves in the US have been met with some criticism as possible federal overreach, the DHS outlines that the move prioritizes federal efforts, makes security expertise and funding available, and improves communication and information-sharing between the stakeholders (including federal and state entities) on threats and vulnerabilities.

The US is by no means alone, even if national governments furnish critical infrastructure and essential services in a variety of ways. Among EU member countries, the transposition of the Directive on security of network and information systems (NIS Directive) might offer an opportunity to review the issue. While the directive focuses on the single market and does not list elections or voting as an essential service (for the list see Annex II, for definitions and identification Articles 4.5 of the directive), national governments have the freedom to furnish the transposition. The attacks on elections and related systems of 2016-2017 seem to have provided momentum for several European governments to consider it.

These steps might also carry symbolic value as these mechanisms highlight the sort of “benefits and protections” election technology enjoys. This means national governments can provide support and resources thus signaling the commitment and potentially contributing to deterrence against election meddling.

Conclusion

In conclusion, election technology, particularly I-voting, can be introduced and promoted with a comprehensive cross-government view with awareness of the complex threat landscape. It is shortsighted to view I-voting or any other election technology as a technical process, as it is a fundamental part of exercising democratic rights. Therefore, the protection and constant legitimization of the democratic process itself has to be at the center of election innovation. For example, new voting technology should not and need not be introduced at the cost of neglecting conventional paper ballots, and election technology cannot exist in isolation.

Estonia is a case study of a realistic, scalable ecosystem of e-services that fosters I-voting and could support election technology. The ecosystem needs to include a wealth of digital services from government and private sector to build trust and form habits. In particular, a government-backed secure digital identity, robust data exchange layer facilitating e-services, and a reliable population register all create conditions for I-voting.

78 | Ibidem.
Estonia is a case study of a realistic, scalable ecosystem of e-services that fosters e-voting and could support election technology. The ecosystem needs to include a wealth of digital services from government and private sector to build trust and form habits.

For a number of states grappling with declining turnouts at elections and with concomitant worries about the security of e-voting and governmental electronic services, the Estonian case provides a timely and useful study that attempts security-by-design whilst recognizing that residual risks will remain and needs careful checks and balances at micro and macro levels with attendant issues of scalability, including those of human-technical resources.

Acknowledgments

I would like to thank my colleagues at the Estonian Information System Authority, Kadri Kaska in particular, as well as Prit Vinkel and his team of the Estonian State Electoral Office and Dr Kristan Stoddart of Aberystwyth University. Your remarks have been invaluable. Similarly, the editors of this Journal have been most constructive and graceful during the writing process.
The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl