HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 3 (2023)

The Digitization of Democracy in Practice: Comparing Internet Voting in Estonia and the U.S.

Alice Shen[1] and Yingqiu Kwang[#]

[1]The university of British Colombia
[#]Advisor

ABSTRACT

In the recent development of electronic government and electronic democracy, Internet voting has sparked intense academic debates and attracted various experimentations among nation-states. This paper overviews major theoretical discussions over the topic and compares literature on the evolution of Internet voting practices in two countries: Estonia and the United States. We argue that the diffusion and sustainability of the Internet voting system in national politics is not the sole outcome of technological innovation. Instead, it relies upon a comprehensive institutional building of digital infrastructure that maintains public trust in the digital transformation and charters the government action in response to security risks.

Introduction

Since the turn of the new millennium, the exponential growth of technological innovation has galvanized society in many unprecedented ways. Internet's increasing prevalence in the information age has profoundly reshaped the global market and altered business and work. Social connectivity has become more accessible and complex, bringing an array of improvements in our daily lives, from communication to socialization and shopping to business. More than that, the emergence of digitization has further displayed the power to transform the norms of conventional politics. Over the past two decades, a growing number of countries have been modernizing their governments and services by integrating new technologies into various aspects of the governance process. In North America, for instance, online opinion polls have replaced traditional phone surveys for collecting the evolving expectations of citizens and businesses. Within the European Union (E.U.), governments have welcomed interest groups' submission of letters online in response to policy consultations in different policy contexts. Recent social movements in the Middle East, North Africa, and Hong Kong have also shown the influence of the Internet in social mobilization.

Perhaps the most innovative yet controversial development in this global move toward electronic government (and electronic democracy) is Internet voting. Internet voting, also denoted as i-voting or remote voting, is a digitized voting system where the voters can vote remotely at private sites through an Internet-enabled computer or other electronic media (Warkentin et al., 2018). Arguably the future mode of political participation (U.S. Vote Foundation, 2015), Internet voting moves beyond other commonly defined electronic voting methods, such as using stand-alone electronic voting machines, voting kiosks, or simply using the Internet for transmitting and tabulating electoral results.

Over the past twenty years, voting remotely over the Internet has drawn a remarkable degree of attention worldwide from scholars, politicians, and the public at large. Multiple prospects have been proposed on how the future may unfold. On one extreme, cyber enthusiasts hail Internet voting as the 'magic ballot (Germann and Serdült, 2017)'. By reducing the physical costs of voting and lowering participating hurdles, voting online will make the process more accessible and convenient, thus enticing more people - especially young people - to participate (Gronke et al., 2008; Gibson, 2005). It will also help to protect against electoral fraud (Schryen, 2004). The outcome of Internet voting, therefore, is expected to reverse the trend of increasing turnout decline, a major source of grave concerns shared among almost every advanced democracy today. On the other extreme, however, the cybersecurity community, fearful of

technology failures and security problems, counterargues that mixing the Internet and voting is always a horrendous idea (Parks, 2019). The ease of hacking personal computers and the servers of electoral committees and the weak encryption of electronic votes during Internet voting make it challenging to ensure ballot integrity and maintain voter privacy. Furthermore, scholars are concerned about the fairness of online voting and raise questions about calculations of expected electoral gains and losses for specific political factors (Hall, 2015; Mendez, 2010).

In everyday politics, the potential benefits and harms of Internet voting have attracted a variety of responses from nation-states. While most of the polities continue to vote offline, several countries across Europe and North America have experimented with Internet voting, aiming to cut the costs of elections, reduce voting mistakes, and increase voter turnout. Even for those pioneers, however, their experimentation varies significantly, not just in the scope and the performance but also in their reactions to existing security problems. Whereas most projects were discontinued after the actual (and perceived) threats of cyberattacks, i-voting continues to be practiced in several corners of the world.

Our aim in this paper is to focus on the practice of Internet voting in two countries: Estonia and the United States. With a population of 1.3 million, Estonia is the only country in the E.U. that offers citizens the option of universal Internet voting. Since 2005, the government has continued this practice for over ten years despite the international community's growing concerns about security risks. While the United States was the first country in the world to trial voting online during the 2000 Arizona Democratic Primaries, today's practice remains limited to a few U.S. states. And most of these projects have also eventually been discontinued because of security problems.

By navigating through the literature that analyzes and compares the experimentation and evolution of Internet voting in both countries, we argue that to better understand the applicability and endurability of Internet voting across national politics, we must take into consideration the significance of the state's historical institutional building of digital infrastructure. Not only is it a crucial factor that determines the diffusion and performance of online voting in a country, but it also helps to shape the state's perception of security risks and thus formulate its own course of action in response to these threats. In Estonia, the concerted national effort to build a digital state has resulted in the normalization and routinization of digital transactions among its citizens, which has greatly facilitated the uptake and diffusion of online voting. Meanwhile, the presence of the digital state has also contributed to citizens' high trust in digital government. Amidst growing security concerns, the Estonian government has focused on fostering a holistic system of cybersecurity and trust to anticipate and mitigate risks rather than abandoning the technology. The United States, by contrast, felt behind in constructing such institutional infrastructure. Consequently, America's decentralized political system has led to the application of online voting in limited scope. After Russia interfered with the U.S. Presidential elections in 2016, mainstream press reports and political commentators quickly shifted to emphasize security vulnerabilities in the remote voting environment. It has also led to the suspension of multiple internet voting pilot programs.

The rest of the article is organized into four sections. The first section thoroughly explores the existing literature on online voting and offers a thematic overview of four critical debates on the topic. The second and third sections examine the experimentation and evolution of online voting in Estonia and the United States, respectively. For each country, we first delineate the history of the online voting system and investigate the benefits realized on electoral turnout, its systematic vulnerability to cybersecurity risks, and government policies in response. This analysis is followed by a discussion of the institutional development of digital infrastructure, emphasizing how it determines the diffusion of online voting and the different perceptions of security problems in both states. We conclude by summarizing our comparative analysis and discussing its significant implications for the future prospects of Internet voting.

Key Theoretical Debates over Internet Voting

In the literature on electronic democracy and electoral studies in political science, Internet voting is a highly contested topic. This section overviews relevant scholarships and organizes the discussion around the following four crucial theoretical debates:

- online voting and its influence on turnout
- its vulnerability to security risks
- its contribution to the basis of democracy
- its applicability across different national contexts

Internet Voting and Electoral Turnout

For Internet voting optimists, their primary argument is that i-voting constitutes 'the ultimate in convenience voting reforms (Alvarez, Hall, and Trechsel, 2009; Powell et al., 2012),' which can work as a remedy to low and decreasing electoral participation rates. First and foremost, Internet voting is both cost- and time-saving. Inspired by the rational choice approach, standard theories of electoral turnout often contend that the probability of an individual's turnout in elections is partly a function of the costs implied in voting (Riker and Ordeschook, 1968). Empirical research by File (2018) and Gomez, Hansford, and Krause (2007) also suggests that any obstacles in the voting process, ranging from distance and transportation to polling stations to terrain and bad weather conditions, may cost voters more time and money and decrease voter participation. Making voting online, in this regard, makes the trip to the polling station redundant. The unprecedented agility it brings to the voting process can be considerably cost- and time-saving for citizens. According to Germann and Serdült (2017), Internet voting also implies an extended voting deadline. Compared to postal voting, by which voters have to send off their voting materials several days before Election Day to ensure their ballots are counted on time, Internet votes are delivered immediately. They can thus be submitted closer to Election Day. It may also save voters the expenditure required and efforts implied in postal voting, such as organizing a postage stamp.

Second, Internet voting increases accessibility. In addition to the obstacles mentioned above, citizens, especially voters with health issues and disabilities, suffer from reduced mobility to travel to their polling stations on Election Day and cast their votes. Digital voting technologies can empower these socially excluded groups to overcome such participation hurdles and, thus, increase voter confidence and their willingness to participate in elections. Meanwhile, Internet voting can also benefit people who live in remote areas and attract those temporarily located out of their home country. Therefore, it is exceptionally compatible with modern mobile lifestyles comprising travel, migration, and transnationalism. Furthermore, Internet voting can be especially appealing to young people. As pointed out by Gibson (2005) and Vassil and Weber (2011), traditional paper-and-pencil forms of voting are increasingly seen as outdated, especially among the wired younger generation. Following this line of thinking, moving elections online is expected to raise the attractiveness of voting and create a positive turnout effect.

Finally, Internet voting can have a transformative effect on election administration. With online voting, there will be a reduced need for the government to deploy and operate the physical polling infrastructure and to equip the voters with essential hardware (Goodman and Spicer, 2019). Less personnel will be required to perform absentee voting and counting. As a result, Internet voting can reduce costs to electoral authorities. Additionally, digital technologies in voting can make the tallying, tabulation, and delivery of election results faster and more accurate (Goodman, Pammett, and DeBardeleben, 2010). The voting software can also identify unconsciously produced invalid votes, which helps reduce possible ballot errors and other general inefficiencies.

However, opponents of Internet voting criticize that while digital technologies may initiate better electoral participation, the expectation of a massive turnout is often exaggerated and has yet to be materialized (Bochsler, 2010; Goodman, 2014). An argument by Berinsky (2005) notes that digital technologies can act as an additional barrier to already disadvantaged groups. In practice, many people would find it difficult and resistant to use the new technology, thus nullifying any promises presented in theory. Norris (2005) and Sciarini et al. (2013) also compare the advantages of i-voting and postal voting, concluding that the extra convenience Internet voting can offer is minimal and may not be big enough to entice additional voters to the polls. In the study of 59 British local entities in the context of the 2003 English local elections, Norris (2005) finds that postal ballots were highly effective at boosting turnout in British localities while i-voting proved less successful. Even in the cases of highly effective pilot i-voting projects, Gibson

(2005) finds that curiosity and high levels of media attention play crucial roles in driving up electoral participation in the initial phase when Internet voting was introduced. Such effects, however, appear unlikely to persist in the longer run. Internet voting may not have a prolonged impact on electoral turnout.

More importantly, citizens' decision to electoral participation is subject to far more complex factors. Political disaffection and disillusionment, for instance, is an outstanding issue. The disengaged and alienated citizenry often lacks interest in engaging in politics and is particularly resistant to any changes (Vassil et al., 2016; Yamamoto and Kushin, 2014). Meanwhile, public confidence in the legitimacy of elections is equally crucial in determining people's incentives to participate. Risks of third-party manipulation in transmitting ballots via the Internet could raise concerns about the integrity of elections, which, in an extreme scenario, could even decrease turnout (Birch, 2010; Gerber et al., 2013; Norris, 2014). Created as a convenient voting method, Internet voting may appeal to those electorates who have abstained due to inconveniences and apparent mobility problems. However, as concluded by Sharma (2020), it cannot act as a 'technological' fix to in-depth political and socioeconomic issues beyond technological reasons.

The complex relationship between Internet voting and electoral participation has been manifested in several existing empirical studies that present mixed empirical results about the nexus in multiple national contexts. For example, in the Brazilian budget referendum and the 2000 Arizona Democratic Primaries, Spada et al. (2015) and Solop (2001) draw similarly optimistic conclusions that the i-voting experiment significantly increased turnout. However, this effect was not observed by Segaard, Baldersheim, and Saglie (2013) in the context of Norwegian local elections. Even for the single-case electoral research of Switzerland, conclusions still vary from study to study. Whereas Serdült and Trechsel (2006) illustrates that Internet-voting increased turnout in the Swiss canton of Zurich, Sciarini et al. (2013) and Germann and Serdült's (2017) study of the Genevan i-voting trials draw contradictory conclusions that Internet voting did not affect actual electoral turnout rates over a long time span.

Internet Voting and Security Risks

The extant scholarship also differs dramatically in their perceptions of cybersecurity risks underlying the i-voting process. Concerns about privacy and integrity typically top the list of counterarguments to electronic voting in general and Internet voting in particular (for example, Scott, 2020; Vicens, 2019). For those studies, the risks primarily come from the relaxation of control of the immediate voting environment. Moving elections online implies that the election authorities can now only provide voters with a secure voting solution but not control the environment for them. Citizens are granted the discretion to implement the solution in their preferred manner. In the eyes of cybersecurity experts like Jefferson, et al. (2004b) and Wolchok, et al. (2012), such an electoral setting leads to many severe problems. Attackers can find ways to take over the voter's computer and shut down the network with viruses or worms. They can also deny voters access to polls and fool individuals into believing they are receiving legitimate data when this is not the case (spoofing) (Awad and Leiss, 2011). In any of these circumstances, voter disenfranchisement becomes a viable threat to the legitimacy of elections. More than that, the risks also take place on the client side. There seems to be a consensus that Internet voting schemes offer little or no protection against vote coercion, vote buying/selling, vote tempering, and voter (mis)identification. Voter privacy may also be breached when their activities may be monitored and recorded during the electoral process.

However, these concerns are not unique to Internet voting. As illustrated in Krimmer, Duenas-Cid and Krivonosova (2022), traditional voting may also result in service denials when Voters are denied easy access to polls and when polling places are opening late, closing early, and running out of ballots. Traditional voting can also be highly insecure. Problems such as vote buying/selling, voter coercion, vote tampering, and voter identification also exist in mail-in balloting. Absentee ballots mailed could also be stolen in the process (Krimmer and Volkmer, 2005). Grounded in the notion that no practical system in the world is risk-free, scholars who retain high hopes for the digitalization of elections tend to accept the trade-offs between desirable properties of electoral systems such as security, accessibility, accuracy, verifiability, anonymity, transparency, and cost-effectiveness (Willemson, 2018).

To better proceed with Internet voting, a stream of literature focuses on drafting and establishing critical principles required for secure electronic voting using the Internet (Alvarez and Hall, 2008; Kavakli, Gritzails and Christos, 2007). High-level security and privacy requirements should be published early in development. Helm (2021) proposes a comprehensive Internet-based system approach incorporating voter registration, voting process, and counting. There have also been international efforts to define standards for Internet-enabled elections. The Council of Europe published recommendations in 2004 and 2017, along with procedural safeguards, to set operational and technical standards on accessibility, interoperability, system operation, security, audit, and certification caused by the i-voting process (Council of Europe, 2004 & 2017).

Several other research turns to technological innovations, exploring how the advancement of digital techniques can better deal with security risks and find ways to enhance trust in and strengthen electorate's commitment to Internet voting. Wang et al. (2015) and Zissis and Lekkas (2011), for instance, suggests a cloud computing architecture to identify vulnerabilities and secure electronic government services. Wang et al. (2017) overviews different cryptographic tools in the design of modern i-voting systems. Studies by Kshetri and Voas (2018) and Abba et al. (2017) explore the possibility of constructing a more secure online voting system by applying blockchain-enabled technologies.

Internet Voting and the Basis of Democracy

The right to vote is essential to a well-functioning democracy. The United Nation Universal Declaration of Human Rights explicitly states that the right to take part in the conduct of public affairs, including the right to vote and to stand for election, is at the core of democratic governance. In the Code of Good Practices in Electoral Matters, the European Commission for Democracy further elaborates on five main principles of electoral law that underpin the basis of democracy: that are, universal, equal, free, secret, and direct suffrage (Garrone, 2005). As the arrival of Internet voting often involves innovative manners different from the traditional ways of voting, whether moving elections online is a boom or loom for democracy has also become a new focus of academic debate.

On the one hand, Internet voting plays a crucial role to equal participation. When voting is made possible from all computers, elections become more accessible to people with limited mobility. It also enables the participation of voters who leave their usual place of residence for a particular time. More than that, Germann (2021) argues that online voting is especially beneficial for effective participation by reducing accidental residual votes. Unlike some voters who intentionally skip some races and spoil their ballots as a form of protest (Solvak and Vassil, 2015), electorates are also prone to make accidental mistakes in the process, leading to the invalidation of their votes. Accidental residual votes may occur when voters uncertain about electoral rules end up voting for more candidates than are allowed or when they fail to mark ballots in a sufficiently clear way (Carman, Mitchell, and Johns, 2008). Trivial as it may seem, Dahl (1989) stresses that it is likely to reinforce well-known inequalities in representation stemming from unequal participation. In this regard, being able to identify these unconsciously produced mistakes, Internet voting should make it more likely that votes enter the final count and, thus, increase effective participation.

Kies and Kriesi 's (2005) research also appraises Internet voting's contribution to facilitating voter freedom. With abundant sources of information available online, Internet voting may help reduce the dissemination of untruthful and biased propaganda favoring specific individuals or organizations. Voters, as a result, enjoy more freedom to form their own electoral opinions. Meanwhile, online voting further helps voters express their opinions more freely by shielding them from the pressures and influences of others, especially from their parents and seniors (Internet Policy Institute, 2001).

On the other hand, however, Internet voting can also bring detrimental harm to some of the democratic principles. Pratchett et al.'s (2005) critics, for example, cast doubt on achieving universal access to private computers. It is no secret that Internet diffusion rates vary significantly across nation-states. Even in the most developed societies, many people are unfamiliar with new technologies, and some have never used a computer (Auer and Mendez, 2005). Suppose universal access to digital technologies is unlikely ever to be achieved. In that case, some voters without

access to a computer at home and/or at their workplace may be deprived of their voting rights. By implication, the introduction of Internet voting would run counter to the principle of universal suffrage. Similarly, when the security and reliability of online voting are not ensured, vote disenfranchisement may happen, rendering the free expression of voters' opinions no longer possible (Garrone, 2005). As an outcome, both principles of universal and free/effective suffrage will be violated.

Following a social network perspective, Unt, Solvak, and Vassil (2017) worries that moving elections online may also bear the risk of turning voting rituals into yet another isolated, individual action on par with other trifle things people do online. Without reduced exposure to political discussions and engaging in the collective exercise of democratic participation, Internet voting may endanger the social nature of voting and possibly reduce the crucial sense of social responsibility and civic duty.

Internet Voting and Implementation Across Nation-states

At the turn of the twenty-first century, Internet voting was first trialed in the 2000 Arizona Democratic Primaries. In 2002, i-voting experiments were officially adopted in the United Kingdom and quickly expanded to several countries worldwide, including at least Australia, Estonia, Canada, Norway, and Switzerland. In recent years, the great hopes for the digitization of elections have also attracted a few more countries to follow suit. Scotland, for instance, has opened a public consultation on electronic voting, internet voting, and other advanced voting technologies. India has tested alternative online voting systems for non-resident Indians and disabled voters (Anooja, 2016). Lithuania also plans to roll out i-voting systems for overseas electorates (LRT English, 2020).

The implementation of Internet-voting experiments, however, differs significantly from country to country. In Table 1 below, we classify the i-voting practices of these pioneering nation-states into four distinct types. Countries first conducted Internet voting in different scopes. In some countries like Canada, Australia, France, Brazil, and Switzerland, those experiments were limited in scope, typically occurring in local and regional settings. The Netherlands, by contrast, introduced online voting at the Dutch 2006 national parliamentary election, where both stand-alone electronic voting machines nationwide and Internet voting for citizens living abroad were employed (Schryen and Rich, 2009). Estonia is the first country worldwide to offer citizens the option of legally binding, universal Internet voting without any preconditions.

Table 1. Variation of Internet Voting Practices Across Countries

	Suspension after Security Problems	**Continuation after Security Problems**
Nation-wide Internet Voting	Netherland	Estonia
Local/Regional Internet Voting	Canada, Australia, France, Norway	Switzerland

Countries also responded to security concerns of Internet voting with varying strategies. In Ireland and Germany, both governments introduced electronic voting machines in the early 2000s, but concerns about their susceptibility to security risks quickly prevented them from putting these devices into practice. Several countries also chose to abandon experimentation with i-voting after the first few trials. For example, Norway trialed Internet voting in 2011 and 2013 but eventually discontinued these efforts due to mounting public concerns about the system's security. Similarly, France was an early adopter of Internet voting in legislative elections for overseas territories. However, immediately after the 2016 U.S. Presidential elections, where evidence suggested Russia's intervention with political campaigns, France declared that electronic voting would not be allowed in its 2017 Presidential election and has stopped the practice of Internet voting ever since. On the contrary, amidst increasing cybersecurity concerns across the international community, countries like Switzerland and Estonia still allow the continuation of Internet voting in their national electoral systems.

As illustrated in Table 1, Estonia and the United States represent two drastically different paths toward electronic government and digital democracy. In the sections below, we explore in more detail the implementation and evolution of Internet voting systems in these two countries.

Internet Voting in Estonia

In 2005, Estonia adopted a nationwide remote voting system. So far, the country has experienced a total of eight Internet-enabled voting practices for local, national, and European elections. The Estonian National Electoral Committee hosts a website where citizens can cast their binding ballots. Eligible voters must use their electronic I.D. card, a compulsory identification system for all Estonian residents, and a PIN code to identify themselves to enter the system for casting their votes (Heiberg, Parsovs, and Willemson, 2015).

Impacts on Electoral Turnout

Historical analyses of Internet voting in Estonia illustrate a striking trend: Since its inception, the digital electoral system has attracted substantial growth in online votes. In the 2005 local elections, only 9,317 residents voted over the Internet, comprising a mere 1.9 percent of all votes received. However, the share of Internet votes increased almost 15 times in succeeding elections, reaching 30.5 percent in the 2015 national elections (Vassil et al., 2016). In 2019, i-votes during the Riigikogu elections constituted 43.8 percent of all votes. In the European Parliament elections held in May 2019, the share reached 46.7 percent. Ehin et al. (2022) predict that a continuation of this trend would lead to the majority of votes cast electronically in the 2023 general elections.

Nevertheless, a definitive conclusion has yet to be drawn on the impact of Internet voting on electoral turnout in Estonia. Trechsel and Vassil (2010), for example, report significant effects of Internet voting that increased turnout by 2.6 percent in the 2009 local elections. However, Bochsler's (2010) study counterargues that the increase in turnout was, in fact, associated with other political and socioeconomic variables. Internet voting, as a result, was found to have no effect. The expected impact of a massive turnout, according to Solvak and Vassil (2017), seems to be a misplaced hope. The main effect of Internet voting is not an increase but the stabilization of turnout at 63 to 64 percent in national elections in Estonia.

Impacts on Democratic Principles

In addition to the substantial growth in Internet voting, there has been a transformation in the demographic distribution of those electronic voters. Trechsel and Vassil (2010) observe small but significant demographic biases in these early i-voting trials in Estonia. First-time Internet voters in the country were likely to be ethnic Estonians, college-educated, wealthy, and early middle-aged (aged 35-45). Ethnic Russians, by contrast, appeared less enthusiastic about this new digital technology. However, since the 2015 national election, such biases have reportedly disappeared. Even computer literacy, which used to be a strong predictor of i-voting, no longer mattered. It means people with poor computer skills were as likely to vote online as their counterparts who excelled in digital technologies.

These empirical results have led Solvak and Vassil (2016) to believe that Internet voting in Estonia has successfully spread from a small and resourceful elite group to reach a broad mass of the less privileged population. By implication, the rapid process of i-voting diffusion within the country contributes to universal and equal democratic participation.

However, several studies warn of a new divide caused by the practice of Internet voting in Estonia. More particularly, The Center Party, the main left-wing party in the country, reportedly received three to four times fewer votes online than offline in the past three parliamentary elections. Centrist voters appeared less committed to online

voting than their counterparts from other parties, especially the liberal Reform Party. Internet voting, in this case, can distort election results, particularly in close elections. As concluded by Lust (2015), i-voting practices in Estonia are becoming more politically biased. Even worse, Kitsing (2011) points out that the availability of innovative platforms for online political participation has yet to engage the public in the legislative process. Estonians are still unwilling to express their views about new laws in the government portal. Online democratic participation, therefore, remains largely unimproved.

Security Risks and Government Responses

The vulnerability of its Internet voting system is not new to Estonians. In April 2007, just two years after its first i-voting experiments, the country suffered a massive cyberattack that suddenly swamped the government and crucial bank and media websites with traffic. Consequently, bank machines stopped working, and crucial internet infrastructure ground to a halt. Meanwhile, the complicated relationship between Tallinn and the Kremlin exposes Estonia to possible cyberattacks from Russia. The most recent security scandal occurred in 2017 when Infineon, a multinational enterprise producing the Estonian ID card chip, was disclosed with a severe security vulnerability that affected around 800,000 Estonian ID cards and millions of cards used worldwide.

Rather than backing away from this new digital innovation, the Estonian government has chosen to maintain the system and strive to become a world pioneer in Internet voting. In addition to refining its digital technique for several years, the country has further incorporated the aim to build a secure voting platform as part of its more profound national campaign to achieve the digital transformation of society. For example, the Estonian Information System Authority (RIA) was established in 2011 to administer the country's information systems. This government agency is not just a cybersecurity governor but is also responsible for the core e-government systems (Fillion, 2020). In 2014, Estonia also became the first country in the world to launch e-Residency, a transnational digital identity that anyone in the world can apply for (Microsoft, 2017). Despite the cybersecurity concerns, online voting stays more ‘sticky’ than conventional voting among Estonian residents. Solvak and Vassil (2017) find that about 80 percent of Internet voters will continue to vote online in the next two elections. In comparison, about 60 percent of conventional voters will continue to vote in person at the polling station.

Institutional Building of Digital Infrastructure

Estonia's striking success in implementing - and sustaining - Internet voting nationwide has attracted the world's attention to look for its secret recipe. There seems to be a consensus that the introduction and successful development of Internet voting must be viewed in the context of a broader state-led effort to build one of the world's most advanced systems of e-governance.

Estonia's institutional building of a digital state primarily involves an early adoption and fast penetration of the Internet and computerization. Immediately after restoring independence from Soviet domination in 1991, the Estonian government took a bold step to embrace digital technology. Under the 'Tiger Leap Program,' launched in 1996, all Estonian schools were provided with computer classrooms and connected to the Internet. Computer science became a required subject to raise citizens' digital awareness. Businesses and local governments also built public-private partnerships to make wireless Internet available in public places free of charge. Public libraries soon became internet hubs, enabling older people to access government services online (Roonemaa, 2017). The government further endeavored to move many public services online. In the 2000s, Estonian residents could file taxes, register a business, and apply for social benefits remotely on the Internet. Most Estonians also embraced the development of information technologies as a national priority. Following the collapse of Communism, Estonian citizens took pride in the formation of a digital state as a way to distinguish the country from other post-Communist societies (Kitsing, 2011).

Consequently, these pioneering policies have significantly improved digital competencies, capabilities, and attitudes among Estonia's residents. Statistics show that today, 79 percent of Estonians are frequent Internet users, more than in any other East European country (Lust, 2018). The share of households with an Internet connection in the country has increased from 37 percent in 2005 to 90 percent in 2020. Mobile broadband penetration is also among the highest in the world, standing at 158 subscriptions per 100 inhabitants in 2020 (OECD, 2023). These achievements have undoubtedly laid a solid foundation for the fast diffusion of Internet voting in the country.

Perhaps the most crucial institution built for the Etonian digital society was the issuance of the national I.D. card in 2002. The Estonian ID card is a state-issued identity document mandatory for Estonian and E.U. citizens residing permanently in Estonia. This digital I.D. also replaced many other I.D. cards, from bank cards to health insurance cards, and can authenticate a person's identity and sign documents online (Alvarez, Hall, and Treschel, 2009). I.D. cards' capacity to strongly bind digital and physical identities has allowed the Estonian government to completely rethink and transform public services.

Before the introduction of Internet voting in 2005, Estonia also endeavored to establish comprehensive legal and regulatory institutions that facilitate the digitization process. It is commonly known that legislation change can be a slow process: alongside the time required for drafting and editing, it also requires reaching difficult - sometimes impossible - political agreements. This is especially challenging for Internet voting. As illustrated by Ehin et al. (2022), as legislation is often prescriptive with paper-based procedures in mind, internet voting cannot be easily integrated into existing legislation.

The legal framework first established multiple laws to build and protect digital citizenship in Estonia. For instance, the 1999 Identity Documents Act includes detailed provisions for digital I.D. cards. The 2000 Digital Signatures Act regulates the use of legally binding digital signatures. The Population Register Act and the Personal Data Protection Act regulate the use of data containing information on all citizens and residents of Estonia (Ehin et al., 2022). In 2002, the parliament then passed a series of electoral acts, including the Riigikogu Election Act, the Local Government Council Election Act, and the Referendum Act. These legislations introduced the possibility of i-voting in local, national, and European elections and referenda, along with detailed clauses on vote counting, including cancellation of multiple votes. In this context, implementing Internet voting seemed like a natural extension of the existing electronic government services.

Public Trust of Internet Voting

Finally, the institutional innovations of a digital state have enabled a high level of trust among Estonian voters. Unified theories of acceptance and use of technology have identified trust as a major precondition for technology adoption and use (Carter and Bélanger, 2005; Carter and Campbell, 2011). Especially for digital technologies for electoral systems, proposals for Internet voting systems are often based on the assumption that voters' computers provide a trusted computing platform. Regardless of the remote voting methodology, the public must trust the electoral process enough to accept the results. In everyday politics, political parties play a crucial role in shaping the attitude of voters toward Internet voting. Ehin and Solvak (2021) illustrate that due to the complexity of the systems in question, most voters cannot form independent opinions on the system's trustworthiness. Therefore, they are likely to rely on signals from trusted political parties to shape their trust/distrust of the i-voting system.

With over 40 percent of the population casting their votes online, Estonia today has built a solid foundation of trust in the digitized electoral system. Solvak and Vassil's (2016) longitudinal study of Estonian Internet voters from 2005 to 2019 finds that while there are some fluctuations across time and the type of election, the share of voters who trust i-voting hovers around 70 percent. A survey also confirms that on a scale of 0-10 measuring their trust in Internet voting, over 60 percent of Estonian voters pick values between 6 and 10. Moreover, Internet voting in Estonia has also enjoyed persisting political support. In history, three left parties - the Center Party, the People's Union, and its successor, the Conservative People's Party - challenged the legality of online voting in Estonian and European

courts (Lust, 2018). Nonetheless, party-based opposition has gradually waned over time. Instead, they have taken turns in shouldering the responsibilities of the government (Ehin and Solvak, 2021).

High usage rates and trust among the electorate suggest that Internet voting is longer considered an experiment in Estonia. Instead, it has become a routinized practice essential to the regular framework for conducting elections. As a result, the normalization and entrenchment of Internet voting make it difficult for any political actor to advocate discontinuation. With a range of domestic actors now deeply vested in the continued performance of the digital system, the political and reputational costs of abandoning i-voting would be very high, extending far beyond the realm of election administration.

More importantly, the high level of trust in Internet voting has also reformulated the government's perception of potential security risks. In the face of cyber-interference attempts, the discussion dominating Estonian politics today is not about whether or not to use technology in elections but how to facilitate structural and cultural changes to foster a holistic climate of cybersecurity and trust (Fillion, 2020). In addition to anticipating and mitigating risks, the government and electoral authorities have been committed to improving, developing, and updating the technological, legal, and organizational aspects of the Internet voting system. Consequently, Estonia's high trust in the digital government survived a series of cybersecurity crises. After the most recent I.D. card scandal in 2017, Estonian authorities resolved the crisis by developing a software update to bypass the vulnerability without replacing the affected cards. A 2020 survey by Raag (2020) shows that 82 percent of residents still trust Estonian e-governance and digital services; among working-age respondents, the figure even stands at 88 percent.

Internet Voting in the United States

Public awareness of Internet voting in America significantly grew after the fiasco of the U.S. presidential election in 2000. Many voters from Florida failed to punch the voting card cleanly, a form of voting whereby voters punch holes in voting cards with a ballot marking device. Such vulnerability to human errors might have swayed the 2000 election to Bush. In addition, many voters misunderstood the rules and simultaneously voted for a presidential and a vice presidential candidate in U.S. elections. In this context, Internet voting was quickly trialed in the context of a binding election in 2000 for the Arizona Democratic Primaries. In 2002, Washington passed the Help America Vote Act (HAVA), investing billions of federal and state tax dollars in updating older voting technologies. The outcome was the Secure Electronic Registration and Voting Experiment project (SERVE) launched in 2004. Under the supervision of the Department of Defense, SERVE was designed to facilitate registration and voting over the Internet.

Internet Voting in a Limited Scope

However, America's i-voting experiments remain within a small scope. The 2004 SERVE system, for instance, was only trialed among residents in seven states (Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington) who agreed to participate. Additionally, it was restricted to overseas voters and military personnel. At present, 25 states are allowing ballots to be returned via email or a web portal. These pilot programs remain open only to overseas residents, military service members, and voters with disabilities. No nationwide Internet-enabled elections have taken place. These experiments so far have also been small. Electronic votes in the state pilot programs represented less than 0.2 percent of the total ballots cast in 2020.

Decentralized State in Digital Infrastructure Building

Compared to the concerted national building of the digital state of Estonia, America's capacity to construct a nationwide digital society has been largely decentralized. Fillion (2020) delineates that U.S. states pursue completely different paths toward the digital revolution. While some places have launched experiments to revolutionize ways of voting,

others still struggle to make sure old, computerized machines are working, with slow progress made. Absent centralized coordination efforts at the top, socioeconomic status has also become a great deal of influence over the accessibility - thus diffusion - of Internet voting in the United States. Among others, age, level of education, and socioeconomic status may affect a voter's computer access, therefore leading to unequal electoral participation.

Furthermore, the decentralized political system in the United States also makes it difficult for the country to establish the required legal framework similar to the General Data Protection Regulation (GDPR) in Europe. The lack of legal institutions for Internet voting will negatively affect the potential likelihood of building trust in American society. Teffer (2017), therefore, believes that America's fear of big government is what makes widespread I-voting unlikely anytime soon.

Emphasis on Security Risks

Like Estonia's digitized electoral system, Internet voting experiments in the United States also suffer criticism about their security vulnerabilities. Jefferson, et al. (2004), for example, warn that the 2004 SERVE system of its security failures both on the server and the user side. In West Virginia, the rollout of a blockchain-based mobile voting app, Voatz, to deployed and overseas military personnel also experiences similar criticism. A group of MIT researchers pinpoints that not only is this electoral software susceptible to hackers' altering, stopping, or exposing how an individual user has voted. Its use of a third-party vendor for voter identification and verification also poses potential privacy issues for users (Parks, 2019; Abazorius, 2020). Rutgers Law School professors and students also challenge an app-based ballot system launched in New Jersey for its 33 local elections (Kiefer, 2020). Of note, our discussion here is about the technological infrastructure of online voting. It is not about the political disputes over the 2020 election and the false claims that were made.

However, what is unique to the United States is that the lack of trust and usage of Internet voting in American society have quickly driven up the public's doubts and reluctance to embrace digital technologies, especially when encountering cybersecurity risks. The memories of Russia's aggressive interference in the 2016 presidential election have become a watershed. The confidential materials were released to the public, indicating the Kremlin's apparent attempts to influence the outcome of the U.S. presidential election by hacking the Democratic National Committee's system in 2016. In response, mainstream press reports and political commentators in the country quickly turned to emphasize the threat of how malicious foreign actors can use information and communications technologies to undermine America's democratic processes. Sanger, Perlroth and Barnes (2021) reported that the White House was essentially caught off guard when Russia successfully launched the widespread attack now believed to have affected upward of 250 federal agencies and businesses. The Kremlin's success without hacking election infrastructure further reveals the weaknesses of protection measures in the United States against global interference (Stone, 2020). Even worse, as Brattberg and Maurer (2018) highlight, the cyber-attack was paired with a disinformation campaign.

Compared to Estonia and many other i-voting pioneers, the United States appears more susceptible to a worst-case scenario in cybersecurity attacks. While although cyber threats are there in Estonia, no hacking of its electoral process is known to the public. The scandal has more or less blown over. However, Foer (2020) expresses deep concerns about many terrifying possibilities that might happen with Internet voting in the context of the United States. A hostile group - Russia, Iran, QAnonn - could overwhelm the vote-casting portal at the last minute. Due to the lack of public trust in the digital electoral system, any (perceived) security threat would most likely ignite an endless legal battle in the country and erode what little confidence is left in the democracy (Mestel, 2022). Following these cautionary narratives, many states have put the brakes on their previous experimentation with Internet voting.

Conclusion

Recently, there has been a new surge of interest in Internet voting. The latest advances in artificial intelligence and related innovations are expanding the frontiers of the digital revolution and global mobility. The outbreak of the global pandemic has further triggered the need to move voting online as senior citizens, the strongest voting bloc in advanced democracies (United States Census Bureau, 2017), are found most vulnerable to contracting fatal diseases in crowded environments. Enthusiasm for Internet voting has started to boom in nondemocratic regimes. In 2014, the Moscow city government introduced a web-based voting system, the Active Citizen platform, allowing citizens to participate in local decision-making (Schlaufer, 2020).

Our analysis of Internet voting practices in Estonia and the United States in this paper shows that great hopes for the digitization of electoral systems often met various realities in national politics. Estonia has been exceptionally successful in the realm of electronic government and democracy: it does not just offer citizens the possibility of pan-national Internet voting in binding elections. Internet voting has also become normalized and entrenched in the country over the years, which has survived multiple security crises. The United States, by contrast, falls significantly behind in the diffusion of online voting in society. Most of these i-voting pilot programs were limited in scope and have eventually been discontinued due to security concerns. Our comparative overviews of literature on the implementation and evolution of digital electoral innovations in both countries offer two significant implications for the prospects for the future of Internet voting.

First, the implementation and diffusion of the Internet voting system often involve a complicated process of institutional building rather than just embracing the advent of digital technologies. Estonia's remarkable achievements in remote voting rely upon an advanced national digital infrastructure that takes on a long-term obligation to refine the technology, build legal frameworks and defend the system against cybersecurity attacks (Alvarez, Hall, and Trechsel, 2009). More importantly, the presence of the digital state also helps to confer strong digital identities upon their citizens that consolidate the voters' willingness and ability to use the Internet to cast ballots.

Building such a comprehensive system of digital governance takes time and patience. Policymakers, therefore, should not expect immediate results following the introduction of new voting technologies but to realize online voting as an advanced service instead of a quick fix to existing problems. The diffusion of the Internet voting system also entails administrative, legal, and policy innovations in different political and economic contexts (Krivonosova, 2022). By implication, countries ~~with~~ decentralized institutional governance structure, as observed in the United States, are expected to experience challenges when deploying remote Internet voting on a large scale.

Second, evidence in both Estonia and the United States shows that security concerns exist everywhere; developing secure electronic authentication systems is a priority for governments worldwide. However, public trust is perhaps the most essential precondition for the endurability of Internet voting amidst mounting security concerns. Estonia's story further illustrates that trust does not solely come from the advanced features of digital technologies used for an Internet voting application. Instead, it emerges from the normalization, institutionalization, and routinization of particular practices in the context of broader socio-technological systems. On the contrary, the case of the United States concludes that Internet voting is unlikely to develop beyond the experimental stage of small-scale pilots without public confidence in the digital capabilities of the state and society. Even worse, the expected benefits of Internet voting will likely be overshadowed by the fear of security and technological failures.

To the extreme, we argue that introducing Internet voting in a low-trust context will bring more harm than good to the basis of democracy. In societies exhibiting significant socioeconomic divides and ethnic and religious disparities, introducing Internet voting may lead to new political biases. Without robust democratic institutions, Internet voting in countries undergoing regime transitions may turn out largely unreliable and illegitimate. Small changes in the vote shares of parties could lead to significant differences in the distribution of seats in legislatures, leading to lengthy legal and political battles over the outcomes of elections (Lust, 2018). Internet voting may also be manipulated as an arsenal for authoritarian regimes to harass opposition parties, bribe and coerce voters, and miscount votes

(Freedom House, 2017). Policymakers should carefully assess potential risks and difficulties before introducing and sustaining Internet voting.

References

Abazorius, A. (2020) 'MIT researchers identify security vulnerabilities in voting app.' Available at: https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 (Accessed: 6 May 2023).

Abba, A.L. et al. (2017) 'Security analysis of current voting systems.' [Conference presentation]. Electrical and computing technologies and applications (ICECTA), pp.1-6.

Alvarez, R.M. and Hall, T.E. (2008) 'Building secure and transparent elections through standard operating procedures.' *Public Administration Review,* 68(5): pp.828-838.

Alvarez, R.M., Hall, T.E. and Trechsel, A. (2009) 'Internet voting in Comparative Perspective: The case of Estonia.' *PS: Political Science & Politics,* 42(3): pp.497-505.

Anooja, A. (2016) 'Internet voting system and digital India.' *International Journal of Emerging Trends & Technology in Computer Science,* 5(1): 62-64.

Auer, A. and Mendez, M. (2005) 'Introducing e-voting for the European Parliament elections.' in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting).* London: Routledge, pp.124-143.

Awad, M. and Leiss, E.L. (2011) 'Internet voting in the USA: Analysis and commentary.' *Transforming Government: People. Process and Policy,* 5(1): pp.45-55.

Berinsky, A.J. (2005) 'The perverse consequences of electoral reform in the United States.' *American Politics Research,* 33(4): pp.471-491.

Birch, S. (2010) 'Perceptions of electoral fairness and voter turnout.' *Comparative Political Studies,* 43(12): pp.1601-1622.

Bochsler, D. (2010) 'Can Internet voting increase political Participation? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections.' [Conference presentation]. The 'Internet and Voting' Conference. 3-4 June. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1456827 (Accessed: 6 May 2023).

Brattberg, E. and Maurer, T. (2018) 'Russian election interference: Europe's counter to fake news and cyber attacks.' Washington, DC: Carnegie Endowment for International Peace.

Carman, C., Mitchell, J. and Johns, R. (2008) 'The unfortunate natural experiment in ballot design: The Scottish Parliamentary elections of 2007.' *Electoral Studies.* 27(3): pp.442-459.

Carter, L. and Bélanger, F. (2005) 'The utilization of e-government services: Citizen trust, innovation and acceptance factors.' *Information System Journal,* 15(1): pp.5-25.

Carter, L. and Campbell, R. (2011) 'The impact of trust and relative advantage on Internet voting diffusion.' *Journal of Theoretical and Applied Electronic Commerce Research.* 6(3): pp.28-42.

Council of Europe. (2004) 'Legal, operational and technical standards for e-voting.' Available at: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf (Accessed: 6 May 2023)

Council of Europe. (2017) 'Recommendation CM/Rec(2017)51of the Committee of Ministers to member States on standards for e-voting.' Available at: https://rm.coe.int/0900001680726f6f (Accessed: 6 May 2023).

Dahl, R.A. (1989) *Democracy and Its Critics.* New Haven: Yale University Press.

Ehin, P. et al. (2022) 'Internet voting in Estonia 2005-2019: Evidence from eleven elections.' *Government Information Quarterly,* 39(4): 101718.

Ehin, P. and Solvak, M. (2021) 'Party cues and trust in remote Internet voting: Data from Estonia 2005-2019', in Krimmer, R. et al. (eds.) *Electronic Voting*. Berlin, Germany: Springer, pp.75-90.

File, T. (2018) 'Characteristics of voters in the Presidential Election of 2016', Washington, DC: U.S. Census Bureau. Available at: https://www.census.gov/content/dam/Census/library/publications/2018/demo/P20-582.pdf (Accessed: 6 May 2023).

Fillion, S. (2020) 'If Estonia figured out online voting 15 years ago, why can't the U.S.?' Available at: https://www.forbes.com/sites/stephaniefillion/2020/08/24/if-estonia-figured-out-online-voting-15-years-ago-why-cant-the-us/?sh=235d30f315ab (Accessed: 6 May 2023).

Foer, F. (2020) 'Russiagate was not a hoax', *The Atlantic,* 19 August. Available at: https://www.theatlantic.com/ideas/archive/2020/08/russiagate-wasnt-a-hoax/615373/ (Accessed: 6 May 2023).

Freedom House. (2017) 'Populists and autocrats: The dual threat to global democracy.' Available at: https://freedomhouse.org/report/freedom-world/2017/populists-and-autocrats-dual-threat-global-democracy (Accessed: 6 May 2023).

Garrone, P. (2005) 'Fundamental and political rights in electronic elections.' in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting)*. London: Routledge, pp.111-123.

Gerber, A.S. et al. (2013) 'Do perceptions of ballot secrecy influence turnout? Results from a field experiment.' *American Journal of Political Science,* 57(3): pp.537-551.

Germann, M. (2021) 'Making votes count with Internet voting.' *Political Behavior,* 43: pp.1511-1533.

Germann, M. and Serdült, U. (2017) 'Internet voting and turnout: Evidence from Switzerland.' *Electoral Studies,* 47: pp.1-12.

Gibson, R.K. (2005) 'Internet voting and the European Parliament elections', in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting)*. London: Routledge, pp.29-59.

Gomez, B.T., Hansford, T.G. and Krause, G.A. (2007) 'The Republicans Should Pray for Rain: Weather, Turnout, and Voting in U.S. Presidential Elections.' *The Journal of Politics,* 69(3): pp.649-663.

Goodman, N.J. (2014) 'Internet voting in a local election in Canada,' in B. Grofman, A.H. Trechsel and M. Franklin (eds.) *The Internet and Democracy in Global Perspective.* Berlin, Germany: Springer, pp. 7-24.

Goodman, N.J., Pammett, J.H., and DeBardeleben, J. (2010) 'A comparative assessment of electronic voting'. Available at: https://www.elections.ca/res/rec/tech/ivote/comp/ivote_e.pdf (Accessed: 6 May 2023).

Goodman, N.J. and Spicer, Z. (2019) 'Administering elections in a digital age: Online voting in Ontario municipalities.' *Canadian Public Administration,* 62(3): pp.369-392.

Gronke, P. et al. (2008) 'Convenience voting.' *Annual Review of Political Science,* 11: pp.437-455.

Hall, T. (2015) 'Internet voting: The state of the debate', in S. Coleman and D. Freelon (eds.) *Handbook of Digital Politics.* Cheltenham, UK: Edward Elgar, pp.103-117.

Heiberg, S., Parsovs, A., & Willemson, J. (2015). 'Log Analysis of Estonian Internet Voting 2013-2014.' IACR Cryptol. Available at: https://eprint.iacr.org/2015/1211.pdf (Accessed: 6 May 2023).

Helm, J.E. (2021) 'Distributed Internet voting architecture: A thin client approach to Internet voting.' *Journal of Information Technology,* 36(2): pp.128-153.

Internet Policy Institute. (2001) '*Report of the national workshop on Internet voting: Issues and research agenda*'. Available at: https://dl.acm.org/doi/pdf/10.5555/1123075.1123096 (Accessed: 6 May 2023).

Jefferson, D. et al. (2004) 'Analyzing Internet voting security: An extensive assessment of a proposed Internet-based voting system.' *Communications of the ACM,* 47(19): pp.59-64.

Kavakli, E., Gritzalis, S., and Christos, K. (2007) 'Protecting privacy in system design: The electronic voting case.' *Transforming Government: People, Process and Policy,* 1(4): pp.307-332.

Kiefer, E. (2020) "NY halts 'Internet voting' experiment after court challenge." Available at: https://patch.com/new-jersey/newarknj/nj-halts-internet-voting-experiment-after-court-challenge (Accessed: 6 May 2023).

Kies, R. and Kriesi, H. (2005) 'Internet voting and opinion formation.' in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting).* London: Routledge, pp.147-165.

Kitsing, M. (2011) 'Online participation in Estonia: Active voting, low engagement.' *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance,* pp.20-26.

Krimmer, R., Duenas-Cid, D. and Krivonosova, I. (2020) 'Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly?' *Public Money & Management,* 41: pp.8-10.

Krimmer, R. and Volkamer, M. (2005) 'Bits or paper? Comparing remote electronic voting to postal voting.' Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b675ceb003b719aaa5bff885347162cb84c4f76d (Accessed: 6 May 2023).

Krivonosova, I. (2022) 'The forgotten election administrator of Internet voting: Lessons from Estonia.' *Policy Studies,* 43: pp.1254-1276.

Kshetri, N. and Voas, J. (2018) 'Blockchain-Enabled E-Voting.' *IEEE Software*, 35(4): pp. 95-99.

LRT English. (2020) 'Lithuanian government backs online voting, but with caveats.' Available at: https://www.lrt.lt/en/news-in-english/19/1190786/lithuanian-government-backs-online-voting-but-with-caveats (Accessed: 6 May 2023).

Lust, A. (2015) 'Online voting: Boon or bane for democracy?' *Information Policy,* 20(4): pp.313-323.

Lust, A. (2018) 'I-vote, therefore I am? Internet voting in Switzerland and Estonia.' *SAIS Review of International Affairs,* 38(1): pp.65-79.

Mendez, F. (2010) 'Elections and the internet: On the difficulties of 'upgrading' elections in the digital era.' *Journal of Representative Democracy,* 46(4): pp.459-469.

Mestel, S. (2022) 'American democracy isn't ready for this: Lessons from the iVote meltdown.' *The Atlantic,* 20 May. Available at: https://www.theatlantic.com/ideas/archive/2022/05/american-democracy-isnt-ready-online-voting/629927/ (Accessed: 6 May 2023).

Microsoft. (2017). 'From Submarines to Cyber: Estonia's Innovation Journey.' Available at: https://blogs.microsoft.com/eupolicy/2017/11/29/submarines-cyber-estonias-innovation-journey/ (Accessed: 6 May 2023).

Norris, P. (2005) 'E-voting as the magic ballot for European Parliamentary elections?' in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting)*. London: Routledge, pp.60-90.

Norris, P. (2014) *Why Electoral Integrity Matters.* Cambridge: Cambridge University Press.

OCED. (2023) 'OECD broadband statistics update.' Available at: https://www.oecd.org/digital/broadband-statistics-update.htm (Accessed: 6 May 2023).

Parks, M. (2019) 'In 2020, some Americans will vote on their phones. Is that the future?' Available at: https://www.npr.org/2019/11/07/776403310/in-2020-some-americans-will-vote-on-their-phones-is-that-the-future (Accessed: 6 May 2023).

Powell, A. et al. (2012) 'E-voting intent: A comparison of young and elderly voters.' *Government Information Quarterly,* 29(3): pp.361-372.

Pratchett, L. et al. (2005) 'Balancing security and simplicity in e-voting.' in F. Mendez and A.H. Trechsel (ed.) *The European Union and E-Voting (Electronic Voting)*. London: Routledge, pp.166-184.

Raag, T. (2020) 'Eesti digiriik naudib nii kohalike elanike kui e-residentide toetust.' Available at: https://pealinn.ee/2020/06/04/eesti-digiriik-naudib-nii-kohalike-elanike-kui-e-residentide-toetust/ (Accessed: 6 May 2023).

Riker, W. and Ordeshook, P. (1968). 'A Theory of the Calculus of Voting.' *American Political Science Review*, 62(1), pp.25-42.

Roonemaa, M. (2017) 'Global lessons from Estonia's tech-savvy government.' Available at: https://en.unesco.org/courier/2017-april-june/global-lessons-estonia-s-tech-savvy-government (Accessed: 6 May 2023).

Sanger, D.E., Perlroth, N., and Barnes. J.E. (2021) 'As Understanding of Russian Hacking Grows, So Does Alarm', *The New York Times,* 3 January. Available at: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html (Accessed: 6 May 2023).

Segaard, S.B., Baldersheim, H., & Saglie, J. (2013) 'The Norwegian trial with internet voting: results and challenges.' Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=4658860 (Accessed: 6 May 2023).

Schlaufer, C. (2020) 'Why do nondemocratic regimes promote e-participation? The case of Moscow's active citizen online voting platform.' *Governance,* 34(3): pp.821-836.

Schryen, G. (2004) 'Security aspects of Internet voting.' *Proceedings of the 37th Annual Hawaii International Conference on System Science*. Hawaii, USA, pp.1-9.

Schryen, G. and Rich, E. (2009) 'Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland.' *IEEE Transactions on Information Forensics and Security*, 4(4): pp.729-744.

Sciarini, P. et al. (2013) 'Etude du vote par internet dans le canton de Genève.' Available at: https://cdc-ge.ch/wp-content/uploads/2022/06/evotingrapportunige0.pdf (Accessed: 6 May 2023).

Scott, T. (2020) 'Why electronic voting is still a bad idea.' Available at: https://www.markpack.org.uk/160622/why-electronic-voting-is-still-a-bad-idea-tom-scott/ (Accessed: 6 May 2023).

Serdült, U. and Trechsel, A.H. (2006). 'Ergänzende Dokumentation: Umfrage bei Stimmberechtigten der Zürcher Gemeinden Bertschikon, Bülach und Schlieren anlässlich des Pilot-versuchs zum Vote électronique vom 27. November 2005.' Bern: Bundeskanzlei. Available at: https://www.zora.uzh.ch/id/eprint/135593/ (Accessed: 6 May 2023).

Sharma, S. (2020) 'Can't change my political disaffection! The role of political disaffection, trust, and resistance to change in internet voting.' *Digital Policy, Regulation and Governance,* 22(2): pp.71-91.

Solop, F. (2001). 'Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election.' *PS: Political Science & Politics, 34*(2), pp.289-293.

Solvak, M. and Vassil, K. (2015) 'Indifference or indignation? Explaining purposive vote spoiling in elections.' *Journal of Elections, Public Opinion and Parties,* 25(4): pp.463-481.

Solvak, M. and Vassil, K. (2016) *E-voting in Estonia: Technological diffusion and other developments over ten years (2005-2015)*. Johan Skytte Institute of Political Studies, University of Tartu.

Solvak, M. and Vassil, K. (2017) 'Could Internt voting halt declining electoral turnout? New evidence that E-voting is habit forming.' *Policy & Internet,* 10(1): pp.4-21.

Spada, P. et al. (2015) 'Effects of the Internet on participation: Study of a public policy referendum in Brazil.' *Journal of Information Technology & Politics,* 13: pp.187-207.

Stone, P. (2020) 'Cyber attacks and electronic voting errors threaten 2020 outcome, experts warn', *The Guardian*, 2 January. Available at: https://www.theguardian.com/us-news/2020/jan/02/elections-2020-cyber-attacks-democrats-experts (Accessed: 6 May 2023)

Teffer, P. (2017) 'Build trust before you introduce e-voting, says Estonian president.' Available at: https://euobserver.com/digital/138394 (Accessed: 6 May 2023).

Trechsel, A.H. and Vassil, K. (2010) 'Internet voting in Estonia: a comparative analysis of four elections since 2005: report for the Council of Europe.' Strasbourg, France: Council of Europe.

United States Census Bureau. (2017) 'Voting in America: A look at the 2016 Presidential election.' Available at: https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html (Accessed 6 May 2023).

Unt, T., Solvak, M. and Vassil K. (2017) 'Does Internet voting make elections less social? Group voting patterns in Estonian e-voting log files (2013-2015).' *PLoS One*, 12(5): pp.1-13.

U.S. Vote Foundation. (2015) 'The future of voting: end-to-end verifiable Internet voting: Specification and feasibility study.' Available at: https://www.usvotefoundation.org/E2E-VIV (Accessed: 6 May 2023).

Vassil, K. and Weber, T. (2011) 'A bottleneck model of e-voting: Why technology fails to boost turnout.' *New Media & Society,* 13(8): pp.1336-1354.

Vassil, K. et al. (2016) 'The diffusion of Internet voting: Usage patterns of Internet voting in Estonia between 2005 and 2015.' *Government Information Quarterly,* 33(3): pp.453-459.

Vicens, A.J. (2019) 'Online voting is a really, really bad idea.' Available at: https://www.motherjones.com/politics/2019/11/online-voting-problems/ (Accessed: 6 May 2023).

Wang, B. et al. (2015) 'DDos attack protection in the era of cloud computing and software-defined networking.' *Computer Networks,* 81: pp.308-319.

Wang, K. et al. (2017) 'A review of contemporary e-voting: Requirements, technology, systems and usability.' *Data Science and Pattern Recognition*, 1: pp.31-47.

Warkentin, M. et al. (2018) 'Social identify and trust in Internet-based voting adoption.' *Government Information Quarterly,* 35(2): pp.195-209.

Willemson, J. (2018) 'Bits or paper: which should get to carry your vote?' *Journal of Information Security and Applications,* 38: pp.124-131.

Wolchok S. et al. (2012) 'Attacking the Washington DC Internet voting system', in A.D. Keromytis (ed.) *Financial Cryptography and Data Security 16th International Conference*. Kralendijk, Bonaire: Springer, pp. 114–128.

Yamatomo, M. and Kushin, M.J. (2014) 'More harm than good? Online media use and political disaffection among college students in the 2008 election.' *Journal of Computer-Mediated Communication,* 19(3): pp.430-445.

Zissis, D. and Lekkas, D. (2011) 'Securing e-government and e-voting with an open cloud computing architecture.' *Government Information Quarterly,* 28(2): pp.239-251.