ONLINE VOTING: REWARDS AND RISKS

Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

intel Security

ONLINE VOTING: REWARDS AND RISKS

by Peter Haynes
Sidebars and table by Jason Healey

In a world of near-infinite computing power, ubiquitous connectivity, cloud-based services, and big data, the fact that the vast majority of countries holds elections using paper ballots appears an anomaly.

Why are the same technologies that have revolutionized so many aspects of our daily lives not being used to improve the electoral process? Although the combination of primary, municipal, county, state, and government elections in the United States alone represents a vast data set, it pales beside the number of financial and other secure transactions that are processed online each day.

Viewed principally as a transaction, voting has some unique aspects. Financial transactions depend on creating a secure, reliable, and auditable end-to-end process that infallibly links, for example, buyer to seller. That entails creating strong, secure, and transparent identities for each party to the transaction. Online voting, by contrast, is predicated on privacy, anonymity, and freedom from outside influence or coercion—but also on the absolute auditability that is necessary to guarantee the principle of "one person, one vote" and to verify that each voter's intent is reflected in the election's outcome.

All these stringent requirements can largely be met with traditional paper voting or touch-screen direct-recording electronic (DRE) machines—even though these technologies are themselves far from perfect.[1] Paper-based voting can be manipulated easily in a number of ways, from ballot-stuffing to intimidation by corrupt officials, and offers poor security for both votes and voters (paper ballots are easily lost, stolen, or destroyed, and voters can be coerced on site).[2]

In theory, however, the types of online technologies that handle our financial transactions with remarkable reliability and security (notwithstanding high-profile breaches such as the Target credit-card theft) should also be able to revolutionize voting.

1 This publication references both e-voting and online voting. The authors use the term e-voting to refer to the use of electronic interfaces in the voting process (such as DRE) and online voting to refer to the entire process of voting over the Internet.
2 Sarah Birch, "Electoral Corruption," Institute for Democracy and Conflict Resolution, Briefing Paper (IDCR-BP-05/11), 2011.See http://www.idcr.org.uk/wp-content/uploads/2010/09/05_11.pdf.

REWARDS OF ONLINE VOTING: ESTONIA

In 2005, Estonia became the first country in the world to hold nationwide elections through an online voting system. Voters in these elections logged in by inserting their nationally issued ID cards into any personal computer with the voting application installed. The two-factor authentication process requires both the voter's ID smartcard and a PIN code in order to cast an encrypted and signed digital ballot.

To preserve anonymity during vote collection and processing, the outer layer of encryption that stores and protects the user's identity is removed before the "inner" encrypted vote reaches the election commission for counting.

As with any online system, there are potential problems, as suggested by a recent study[1] that found numerous potential vulnerabilities capable of disrupting the voting process. The system has apparently never faced a concerted attack from a hostile power, which could shake nearly any system.

It is worth noting that Estonia has fewer than a million voters, so the process may be difficult to scale to a national election in a large country. The Estonian system also depends on smart and secure citizen identity cards, which might not be accepted by all members of an electorate (especially in the United States).

So far, however, the system appears to have worked well in multiple local and general elections, with both the government and electorate satisfied with the benefits compared to the potential risks.

1 Drew Springall et al, "Security Analysis of the Estonian Internet Voting System," University of Michigan, November 2014, http://jhalderm.com/pub/papers/ivoting-ccs14.pdf.

Online voting has the obvious—though still largely unproven—potential to improve accessibility for the disabled and elderly; make long-distance voting far easier (important for military and other voters overseas); cut costs (paper ballots are costly to print, and the machines that count them inordinately expensive); and improve voter turnout. The latter would be especially true for reluctant younger voters if secure, remote voting via devices such as smartphones, tablets, and other electronic devices were possible.

Voting using smartphones or personal computers could also eliminate the possibility of influence by government officials or others who may abuse their supervisory roles at polling stations (though of course the system administrators who run the system would have to be highly trusted).[3] Remote voters also might take more time to make informed decisions than those in busy polling booths.

NOT SO NEW, BUT STILL NOVEL

Computing technology has been part of the electoral process for around half a century, with everything from punch cards to optical scanners used to tally votes. Corporations and other organizations have long used e-voting to elect officers and hold proxy elections. To date, countries as diverse as Australia, Brazil, Canada, Estonia, France, India, the Netherlands, the United Kingdom, the United States, and Venezuela have experimented with or implemented various forms of e-voting in primary, municipal, and national polls. Not all experiments have been successful, but several countries have replaced paper ballots at polling booths with DRE machines that can transmit polling data over a network to a central location or store it in local, removable memory (a printed record is usually available too).[4] Brazil's electoral system now uses DRE machines almost exclusively, and in its 2010 presidential election the result was declared a mere seventy-five minutes after the polls closed.[5]

Estonia has taken a different tack. Because all Estonians have a government "chip and PIN" e-ID card, online voting is now available to the country's electorate, and votes are encrypted for greater security.[6] Estonians can also vote more than once, from different devices and locations, over a thirty-day period—though only the final vote counts—giving voters the option to change their minds. They can also vote at a polling station on election day if they wish. Estonia has not, therefore, reduced paper costs. The Estonian system also enables individuals to verify their vote using a form of two-factor verification: in this case, two devices, such as a smartphone and a personal computer. Voters are unlikely to "sell" their vote because their e-ID cards are also tied to government services such as healthcare. According to Tarvi Martens, chairman of Estonia's Electronic Voting Committee, a quarter of the electorate votes online.[7]

REWARDS OF ONLINE VOTING: INDIA

India conducts the largest democratic elections in human history, and electronic voting machines are used at all polling stations—over 900,000 of them.

These e-voting machines have transformed Indian elections, saving money, helping illiterate people vote, and increasing vote-counting tenfold.

However, the existing machines run on 1980s technology in a country with over 900 million mobile phone subscribers, hundreds of millions of whom have smart identity cards with biometric data.

If India were to overcome its compelling security challenges and hold Estonian-style online elections (albeit with 1,200 times the population), it would mark digital democracy's true coming of age.

SECURITY CONCERNS STILL AN ISSUE

But for online voting in all its forms to take off, security will need to be vastly improved. When a hacker steals money online, the theft is easily discovered. Banks, online retailers, and other companies offering services over the Internet factor in some degree of loss as a cost of doing business online, and generally indemnify their customers against bad actors. Online voting poses a much tougher problem: lost votes are unacceptable. Online voting systems are complex, and any updates often must be separately recertified by election authorities. And unlike paper ballots, electronic votes cannot be "rolled back" or easily recounted. The twin goals of anonymity and verifiability within an online voting system are largely incompatible with current technologies. Russian state-sanctioned hackers, it should be recalled, brought almost all of Estonia's online activities to a halt in 2007 and might do so for online elections as well. Nobody knows whether the DRE machines or other proprietary voting systems in use elsewhere have already been hacked too.

3 In today's post-Snowden era, this concern is particularly pressing in ensuring the integrity of an election.
4 Critics of France's e-voting argue that the system still lacks proper security, is difficult to use, and is not worth the new cost. The United States has received similar recommendations that also include having a verifiable audit trail and the issuing of grants for developing secure cryptographic voting protocols. E-voting has been banned entirely by the Netherlands, Ireland, and Germany out of security and transparency concerns.
5 Daniel Castro, "Stop the Presses: How Paper Trails Fail to Secure e-Voting," Information Technology & Innovation Foundation, September 2007, See http://www.itif.org/files/evoting.pdf.
6 Daniel Castro, "Explaining International Leadership: Electronic Identification Systems," Information Technology & Innovation Foundation, September 2011, See http://www.itif.org/files/2011-e-id-report.pdf.
7 Charles Arthur, "Estonian e-voting shouldn't be used in European elections," Guardian, May 12, 2014. See http://www.theguardian.com/technology/2014/may/12/estonian-e-voting-security-warning-european-elections-research.

Alex Halderman, an assistant professor and security expert at the University of Michigan, has found holes in many existing online voting systems. In 2010, Dr. Halderman volunteered to test the integrity of an Internet voting system intended for use in Washington, DC. Within hours, his team accessed secret data on the system's server, including the key used to encrypt ballots; replaced votes that had been cast; linked voters' names to their votes; and forced the system's vote-confirmation screen to play his university's fight song. The team also found evidence that other hackers were trying to compromise the as-yet unused system. It was scrapped.[8]

PLENTY OF PROBLEMS, PLENTY OF POTENTIAL

But online voting is far from dead in the water. Many of the holes Dr. Halderman and his team discovered—such as minor programming errors or the use of default passwords—could be easily fixed, and the system could then be recertified by election officials.

Using the Internet is also much safer for some parts of the voting process, like registration, casting, and collecting votes (see graphic on p. 6-7). New techniques to improve the integrity, security, and anonymity of online voting systems are under development. For example, cryptographic features capable of verifying that votes have been recorded, counted, and declared accurately could be implemented *separately* from the computer hardware and software that is actually collecting those votes. Such an approach could be a game-changer, enabling anonymized verification of votes collected via diverse and comparatively insecure devices such as smartphones.

For the digital generation, unsupervised polling via mobile devices may be the "killer app" of e-voting. For that to become a reality, device security will still need to be strengthened. Biometrics (such as fingerprint scanning) and two-factor authentication (such as when a bank requires a customer to enter both a password and a code sent to his or her mobile phone) could help solve these issues.

Beyond enhanced security and auditability, greater public acceptance of and trust are also essential.

8 Alex Halderman et al., "Attacking the Washington, D.C. Internet Voting System," Conference on Financial Cryptography & Data Security, February 2012. See https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.

RISKS OF ONLINE VOTING: UKRAINE

In the midst of the internationally sensitive May 2014 Ukrainian presidential elections, there was a directed and sophisticated attack on electronic data systems allegedly intended to destroy the integrity of the count and create false results.

If the intrusion had not been detected, the tampered results would have shown a clear victory for an extremist far-right candidate, which may have led to further bloodshed, perhaps bolstering justifications for foreign intervention favoring Ukrainian rebel groups.

The Ukrainian election did not use e-voting but was a traditional election, demonstrating that electronic intrusions can potentially disrupt any vote-processing system.

Without very strong security, online voting offers even more opportunities for intrusions and tampering than traditional systems.

Most of today's voters understand the risks in paper-based polling, but familiarity and some degree of transparency—along with the knowledge that paper ballots can be recounted—has bolstered public trust in paper ballots. Online voting systems, by contrast, are viewed as opaque "black boxes" that can be manipulated in unseen ways. Improved verification, privacy, anonymity, and security protocols that work, along with voter education and the growing percentage of voters who have grown up with digital technology, will likely tilt the balance towards online voting—even if that shift initially manifests itself as a mix of online technologies and paper verification to reassure individuals that their vote has been cast and counted as they intended.

All this will take time. Broad adoption of most new technologies generally takes longer than technology optimists hope, but it will happen. Online voting's potential benefits in terms of reach, access, and participation have the power to revolutionize the democratic process around the world.

Peter Haynes is a nonresident senior fellow for the Strategic Foresight Initiative in the Atlantic Council's Brent Scowcroft Center on International Security. Jason Healey is director of the Cyber Statecraft Intiative in the Brent Scowcroft Center on International Security.

	REGISTRATION →	VOTER VERIFICATION →
Description	• Assures only authorized voters are allowed to exercise their vote. • In the United States, prospective voters must register several weeks beforehand, usually either by mail or at a government building.	• Ensures that on election day, each voter is who they say they are (identity and authentication) and are eligible to vote (authoriziation). • This might be done in paper-ballot elections by showing an ID card or verifying an address.
Rewards	Registering online is simpler for most people and especially: • Makes it easier for people with disabilities or living abroad; • Provides a more cost-efficient, transparent, and auditable process; and • Is expected by digital natives who do everything online.	While voting online, the verification must be built into the software. If done correctly, however, e-voting can: • Positively identify each person more accurately than even a government ID card and remain up to date; • Ensure only one vote is recorded for each person; and • Instantly identify and authorize voters in real time.
Risks	**Lower risks:** Attacks could target availability, confidentiality, or authentication of the system. • Distributed denial of service attacks (DDoS) can overload servers, preventing voters from registering. • Intruders could read personal information, submit false information, or even change info on voters.	**Lower risks:** Attacks here could particularly target availability and authentication of the system. • If separate servers are used for both verifying voters and counting votes, then the verification servers can be separately targeted for a DDoS. • Attackers could also take the place of legitimate voters through phishing attacks, tricking users into revealing their credentials.
Solutions	• To prevent DDoS, properly design networks and contract for more network bandwidth at critical times, such as just before registration deadlines. • Cryptography, secure software, and strong access control beyond passwords—including biometrics data such as fingerprints—can help keep intruders out of the system. • Nontechnical controls also help, such as mailing physical registration cards for people to confirm details.	• Basic and effective methods for electronic authentication are relatively cheap and easy to deploy. • The best solutions will use strong access control beyond passwords, such as biometrics or a smart card and personal PIN.

CASTING VOTES → COLLECTION & PROCESSING

• Ensures votes are accurate and anonymous. • Accuracy and anonymity can be relatively easy to guarantee in offline votes where verification happens separately from casting and in a controlled facility.	• Collecting local votes, centrally aggregating votes from other locations, and calculating the results. • Auditable records must be maintained throughout to assure the traceability of a voter's intent in case of a mistake or recount.
E-voting improves convenience by allowing voters to cast ballots online, sometimes from their own computer. These improvements: • Make it easier for people with disabilities or living abroad; • Provide a more cost-efficient, transparent, and auditable process with fewer chances for fraud; and • Possibly lead to higher voting turnout, especially among youth.	Online voting systems leverage the best advantages of computer technology to: • Use network connectivity to aggregate vote data from any distance; • Automatically and quickly tally votes; and • Easily display results in real time, if desired.
Very high risks: Attacks could target availability, confidentiality, or authentication of the system. • DDoS attacks can overload servers, preventing voting, especially if elections are held on a single day. • Attackers could potentially impersonate legitimate voters to cast false votes, or monitor network traffic to see how individuals voted.	**High risks:** DDoS attacks are possible to keep all voting locations from reporting, but the main threat is against integrity. • Intruders could potentially break into election servers and change previously cast votes.
• To beat DDoS, properly design networks and contract for more network bandwidth during voting day. • Cryptography, secure software, and strong access control beyond passwords such as biometrics are a must to ensure votes are not stolen. • For extra security, voters could use a preconfigured bootable USB or CD in their personal computer, guaranteed free of malicious software. • Nontechnical controls also help, such as voting over an extended time period.	• Cryptography; secure software, databases, and networks; and strong access control beyond passwords must protect election servers and the accounts of the users and especially systems administrators. • Other solutions, such as "tripwires" to see if any data has been changed, are also recommended.

ABOUT MCAFEE
McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

ABOUT THE ATLANTIC COUNCIL
The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor, Washington, DC 20005
(202) 778-4952, AtlanticCouncil.org