# SECURITY CHALLENGES FOR DEMOCRATIC ELECTIONS

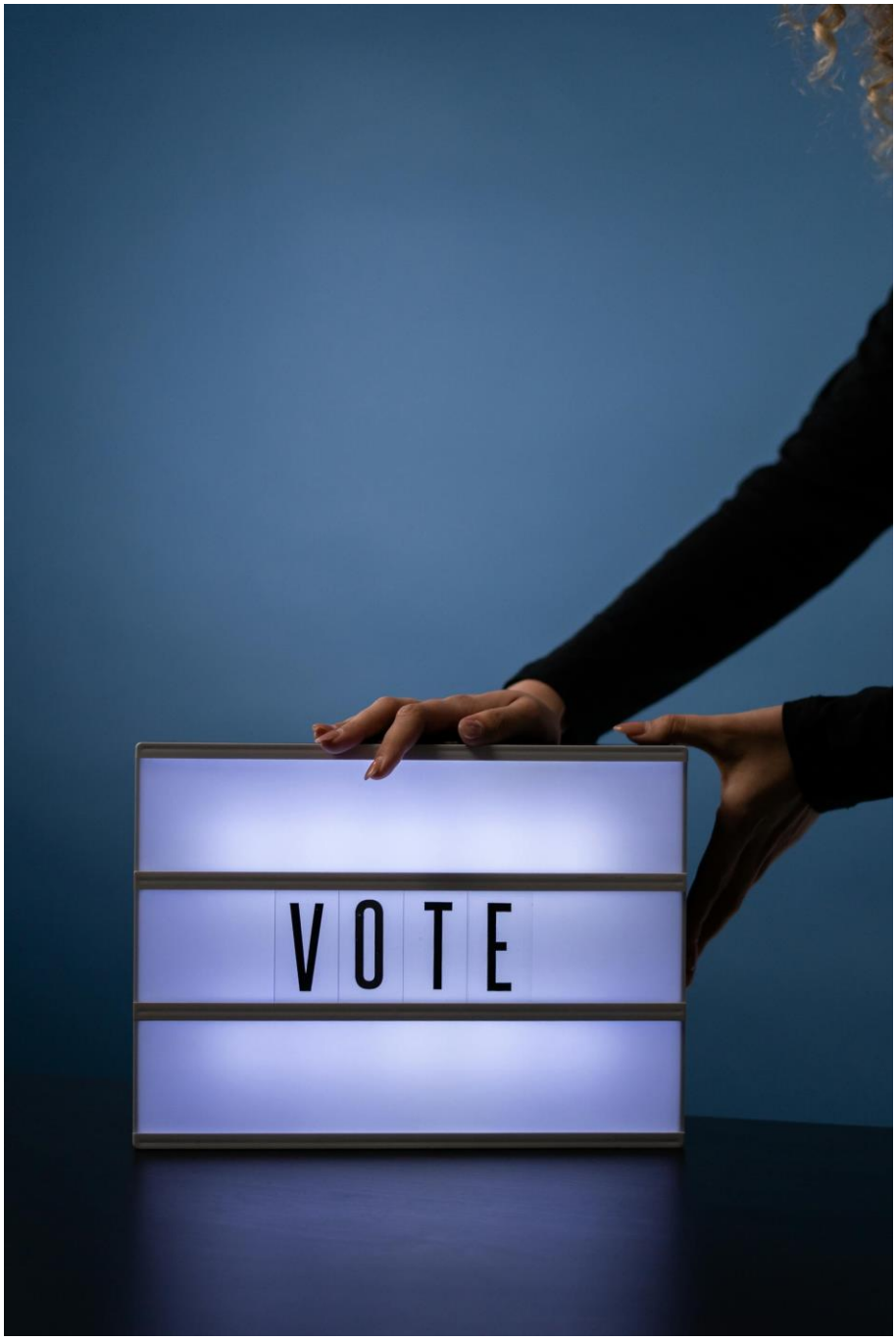


*Photo by cottonbro studio from Pexels*

On Wednesday, September 11, 2024, INCS-CoE held an on-line seminar on security challenges for democratic elections. Four speakers presented their ongoing research: Alan T. Sherman (UMBC, USA), Steve Schneider (Surrey, UK), David Lazer (Northeastern, USA), and Harumichi Yuasa (Meiji, Japan); see biographies at the end of this note These talks addressed significant and timely challenges involving voter coercion, verifiability, disinformation, and election law and policy.

*Alan T. Sherman* spoke about a solution to a long-standing challenge to the integrity of votes cast without the supervision of a voting booth: "*improper influence*," which he defined as any combination of vote buying and voter coercion. In comparison with previous proposals, the VoteXX system[1][2] is the first in the literature[3][4] to protect against a strong adversary who learns all the voter's keys---they call this property "*extreme coercion resistance*." When keys are coerced or stolen, each voter, or their trusted agents (which they call "*hedgehogs*"), may "*nullify*" (effectively cancel) their vote in a way that is unstoppable and irrevocable, and such that the nullification action is forever unattributable to that voter or their hedgehog(s). He demonstrated the security of the VoteXX system in the universal composability model. In comparison with previous proposals, VoteXX offers protection against even the strongest adversary who learns all keys. Other coercion-resistant protocols either do not address these attacks, place strong limitations on adversarial abilities, or rely on fully trusted parties to assist voters with their keys.

*Steve Schneider* spoke about Verifiable Voting in the Wild. Verifiability in Electronic Voting Systems is an approach to enabling checking of the election result independently of the system used to capture and process the votes. There have been numerous proposals in the literature for electronic voting systems designed to include verifiability, generally underpinned by cryptographic mechanisms. These typically enable voters to confirm that their vote has been captured as cast and enable observers (including the voters themselves) to verify that the votes have been counted and tallied correctly from the cast votes. The need to

[1] "VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections (extended abstract)," *Proceedings of E-VOTE-ID 2022*, University of Tartu Press (October 2022).
[2] "VoteXX: Extreme Coercion Resistance," https://eprint.iacr.org/2024/1354
[3] "VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections (extended abstract)," *Proceedings of E-VOTE-ID 2022*, University of Tartu Press (October 2022). https://eprint.iacr.org/2022/1212
[4] "VoteXX: Extreme Coercion Resistance," https://eprint.iacr.org/2024/1354

simultaneously ensure other requirements such as ballot privacy and coercion-resistance leads to voting ceremonies that can be intricate and place an additional burden on voters.
He described the trial deployment of two such systems in the wild: the vVote polling place system based around Pret a Voter; and the VMV (Verify My Vote) internet voting.
*David Lazer* evaluated the potential threats to the 2024 US election. The information environment has continued to rapidly change, and with those changes come new potential vulnerabilities to the integrity of the 2024 election. He examined lessons from the 2016 and 2020 elections, as well as some early findings regarding misinformation in the aftermath of the assassination attempt of Donald Trump.
*Harumichi Yuasa* addressed overseas voting reform in Japan. Overseas voting is an important system for guaranteeing the voting rights of citizens living abroad. However, in Japan, only postal voting or voting at an embassy is permitted. The COVID-19 pandemic has caused problems such as delays to postal voting and the inability to visit embassies due to lockdowns. A method has been proposed in which voters living abroad can vote via the internet using their My Number card. In addition, he introduced some of the problems in Japan related to elections and the internet.
The talks covered important topics such as coercion, verifiability, misinformation and secure, remote voting. Some of the key research challenges which emerged during the seminar Included:

1. The prevention of improper influence (coercion and voting selling),
2. Understanding the impact and mitigation of malware on untrusted machines,
3. The detection and prevention of denial-of-service attacks on the election system,
4. The challenge of maintaining usability in electronic voting systems as security protocols are introduced,
5. The need to address the structural vulnerabilities of social media platforms, which are the primary vectors for the spread of misinformation, and
6. Understanding the implications of Generative AI in the production of mis- and disinformation,
7. The development of tools which are user-friendly and engender trust.

More information about the individual presentations and the resulting research questions may be found on the INCS-CoE website (incs-coe.org) or by contacting the speakers. We encourage the community to start conversations which might lead to the solutions of some of these challenges.

## Speakers

### Prof Alan T. Sherman

Alan T. Sherman is a professor of computer science at the University of Maryland, Baltimore County (UMBC) in the CSEE Department. He is also associate director of UMBC's Cybersecurity Center and director of the UMBC Cyber Defense Lab. His main research interest is high-integrity voting systems. He has carried out research in election systems, formal-methods analysis of cryptographic protocols, algorithm design, cryptanalysis, theoretical foundations for cryptography, applications of cryptography, cloud forensics, and cybersecurity education. He is PI on two UMBC NSF-funded projects: EPIC---to study and improve how the US Navy and Army Military Academies teach cybersecurity, and SFS---to recruit and educate BS, MS, and PhD cybersecurity students to serve government. Previously, he served as PI on UMBC's NSF-funded CATS project (collaborative with the Universities of Illinois and Minnesota Duluth), which developed two concept inventories (CCI, CCA) for cybersecurity. Resulting work won best research paper at ACM SIGSCE 2023. Dr. Sherman is also a private consultant performing security analyses and serving as an expert witness. Sherman earned the PhD degree in computer science at MIT in 1987 studying under Ronald L. Rivest.

email: sherman@umbc.edu, https://www.csee.umbc.edu/people/faculty/alan-t-sherman/

### Prof Steve Schneider

Steve Schneider is a professor of Computer Science at the University of Surrey, UK, in the School of Computer Science and Electronic Engineering. He is Director of the Computer Science Research Centre in the School and was founding Director of the Surrey Centre for Cyber Security, an Academic Centre of Excellence in Cyber Security Research and Cyber Security Education recognised by the UK National Cyber Security Centre. A principal research interest is in Verifiable Electronic Voting Systems. He was one of the proposers (with Peter Y. A. Ryan and David Chaum) of the Pret a Voter voting system in 2005 and led its adaptation to a deployment (as vVote) in the 2014 Victorian State Election, Australia. He has also served as chair of the Working Group on Electronic Voting for the Institution of Engineering and Technology (IET). Other research interests include formal methods, concurrency theory, security verification, privacy, and digital identity. He obtained his PhD in Computer Science from Oxford University in 1989.

https://www.surrey.ac.uk/people/steve-schneider

## Prof David Lazer

**David Lazer** is University Distinguished Professor of Political Science and Computer Sciences, Northeastern University, faculty fellow at the Institute for Quantitative Social Science at Harvard, and elected fellow of the National Academy of Public Administration. He has published prominent work on computational social science, misinformation, democratic deliberation, collective intelligence, and algorithmic auditing, across a wide range of prominent journals such as Science, Nature, Proceedings of the National Academy of Science, and the American Political Science Review. His research has received extensive coverage in the media, including the New York Times, NPR, the Washington Post, and the Wall Street Journal. He is a co-leader and co-founder of the COVID States Project, one of the leading efforts to understand the social and political dimensions of the pandemic in the United States; as well as the National Internet Observatory. Dr. Lazer has served in multiple leadership and editorial positions, including on the Standing Committee on Advancing Science Communication for the National Academies, the International Society for Computational Social Science, the International Network for Social Network Analysis, Social Networks, Network Science, and Science.

## Prof Harumichi Yuasa

**Harumichi Yuasa** is Professor, Graduate School of Governance Studies, and Senior Staff to Office of the President, Meiji University. He is focusing on legal, administrative, and political aspects of internet and information society including protecting privacy and personal information, administrative information handling and disclosure, regulation of cyber security and defense activities, internet election campaign and e-voting. He is also serving as Committee Member, Cabinet, National Center of Incident readiness and Strategy for Cyber Security (NISC), Sub-Working Group for Research and Examination of Cyber Security-Related Laws and Regulations, Research Fellow, Ministry of Internal Affairs and Communications, Information and Communications Policy Research Institute, and Committee Member, Ministry of Internal Affairs and Communications, Standardization Study Group for Electoral List Management System, etc.