

ELECTIONS, CYBERWARFARE, AND THE FUTURE OF AMERICAN DEMOCRACY: WILL YOUR VOTE BE DISARMED?



WEBINAR **SEPTEMBER 30, 2020**

MODERATOR

Rick Rolf

Previously served as senior foreign policy adviser, chief campaign strategist, and spokesman for the late Senator Mark O. Hatfield

PANELISTS

Douglas W. Jones

Associate Professor of Computer Science at the University of Iowa

Matthew Bishop

Professor of Computer Science at UC Davis

Stephanie Singer

Research Assistant Professor at PSU, Previously served on the Philadelphia Board of Elections

Phil Kiesling

Founder and chair of the Vote at Home Institute, previously Oregon Secretary of State

Biról Yesilada

Director of the Mark O. Hatfield School of Government and Professor of Political Science and International Studies at Portland State University

[VIEW RECORDING](#)

Resources

• VerifiedVoting: <https://verifiedvoting.org> for information on election security, hardware in use at your local precinct, and more.

PRESENTED BY THE MARK O. HATFIELD NSA/DHS NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBER RESEARCH

KEY POINTS

- An informed citizenry is our democracy's greatest defense against "influence operations" to delegitimize our election process.
- We limit the threats to elections security by properly funding our election offices.
- Election results are officially certified by each state, not the media and not politicians.
- Disinformation and chaos will likely accompany election day and the weeks afterward.
- The best defense we have against the results being questioned is a large margin of victory.
- You mitigate risk by hand-marking a paper ballot, if that is possible (such as with vote-by-mail).
- Postal equipment and voting machines are all vulnerable to malware attacks. Logic and accuracy tests should be administered regularly.
- We need to make election systems that are resistant to carelessness (that also limits bad actors who often will hide behind the guise of carelessness).
- Apocalyptic journalism is not helpful to democracy. Journalists should instead be focused on spreading information about the safeguards that are in place to protect our elections.
- Cybersecurity concerns aren't just about hacking into polling machines or voter databases; it's also about social media campaigns to discourage participation in the election. You don't need to steal a vote that has never been cast.

What can you do?

- Vote. The power of your vote is not just the outcome of individual races. High voter turnout legitimizes the democratic process.
- Observe your local election process--find out when counts happen, how they are processed, etc. Volunteer to be an observer of the election count in your district.
- Get involved in local government by watching your local city or county council meetings.
- Drop ballot at your local election office or an official ballot drop box if you don't trust the post office.
- Vote. The real threat is voter suppression. Force your vote to be taken, don't give it away.