

# Policy Dimensions of Strengthening Election Cybersecurity

David P. Fidler

Indiana University Maurer School of Law

Council on Foreign Relations

October 18, 2017, Washington, D.C.

NASEM Committee on the Future of Voting

# Overview of remarks

- Extent of the policy failures in connection with the cybersecurity of election systems
- Need for a comprehensive, high-level political strategy to strengthen election cybersecurity
- Possible components of a comprehensive political strategy
- Examples of some specific policy options
- Challenges of designing and implementing a comprehensive strategy



# Policy failures on election cybersecurity

- Comprehensive failure to accord sufficient policy attention and political commitment to election cybersecurity
- Policy failure happened in three contexts in which cyber threats to election systems should be priorities
  - Administration of election systems → Cybersecurity risks
  - Cybersecurity → Election system vulnerabilities
  - Internet freedom → Cyber interference with core act of democracy and a fundamental right
- Why such comprehensive failure?
  - Functional: Capacity deficits to understand cyber threats to election systems and address them effectively → Local/State
  - Political: Calculation that other cyber threats were more urgent and serious (e.g., critical infrastructure protection; economic cyber espionage; cyber terrorism) → National
  - Philosophical: Complacency about the machinery of democracy in an increasingly dangerous digital world → International

# Comprehensive, high-level policy strategy (1): Objectives and levels of policy action

Strategic Objectives	Levels of Policy Action		
	Local/State	National	International
Protect (technological)			
↕			
Deter (political)			
↕			
Reassure (psychological)			

# Comprehensive, high-level policy strategy (1): Examples

Strategic Objectives	Levels of Policy Action		
	Local/State	National	International
Protect (technological)	<ul style="list-style-type: none"> <li>Secure voting machines and procedures</li> <li>Protected voter-registration systems</li> </ul>	<ul style="list-style-type: none"> <li>Guidelines/standards for election cybersecurity</li> <li>Financial resources for local/State systems</li> </ul>	<ul style="list-style-type: none"> <li>Information sharing</li> <li>Capacity building</li> <li>Joint R&amp;D</li> </ul>
 Deter (political)	<ul style="list-style-type: none"> <li>Deterrence by denial (strong, resilient defenses)</li> </ul>	<ul style="list-style-type: none"> <li>National security priority</li> <li>Sanctions (criminal, economic, political)</li> </ul>	<ul style="list-style-type: none"> <li>Collective action priority</li> <li>Common policies and solidarity on sanctions</li> </ul>
 Reassure (psychological)	<ul style="list-style-type: none"> <li>Pre-election testing</li> <li>Communication during election cycles</li> <li>Post-election verification</li> </ul>	<ul style="list-style-type: none"> <li>Visible support</li> <li>Assessment</li> <li>Leadership on improving resilience</li> </ul>	<ul style="list-style-type: none"> <li>Election monitoring</li> </ul>

# Comprehensive, high-level policy strategy (2): Tools of policy action

Levels of Policy Action	Tools of Policy Action		
	Actors	Processes	Norms
Local/State			
National			
International			

# Comprehensive, high-level policy strategy (2): Examples

Levels of Policy Action	Tools of Policy Action		
	Actors	Processes	Norms
Local/State	<ul style="list-style-type: none"> <li>• Governors</li> <li>• Secretaries of State</li> <li>• County/city officials</li> <li>• Election administrators</li> </ul>	<ul style="list-style-type: none"> <li>• Associations of governors, secretaries of state, and county/city officials</li> <li>• Specific cybersecurity initiatives</li> </ul>	<ul style="list-style-type: none"> <li>• Constitutional allocation of primary responsibility</li> </ul>
National	<ul style="list-style-type: none"> <li>• White House</li> <li>• DHS, State, NIST</li> <li>• Congress</li> <li>• Voting rights and other civil society groups</li> </ul>	<ul style="list-style-type: none"> <li>• Election Assistance Commission</li> <li>• Inter-agency processes</li> <li>• Federal-state cooperation mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>• Constitutional allocation of support responsibility</li> <li>• Criminalization of cyber interference</li> </ul>
International	<ul style="list-style-type: none"> <li>• Democratic states</li> <li>• International organizations</li> <li>• Civil society groups (e.g., election monitoring)</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber crime cooperation</li> <li>• Cyber threat information sharing mechanisms</li> <li>• Democracy promotion efforts</li> </ul>	<ul style="list-style-type: none"> <li>• Non-intervention</li> <li>• Human right to vote</li> <li>• Democracy promotion</li> </ul>

# Challenges for a comprehensive strategy on election cybersecurity

- Protect

- Sustainable → technologies and approaches (no HAVA 2.0)
- Proportionate → calibrate security with other goals (e.g., expand access to voting)
- Structural barriers → imperatives for significant federal government roles
  - Federalism → cooperation model as in disaster response, pandemic preparedness and response & counter-extremism
  - “Anarchical society” → US leadership among democracies

- Deter: “deterrence by denial” requires long-term commitment, without which protection can weaken and reassurance can fail

- Reassure

- Very bad political climate → allegations of “rigged” elections; investigation of campaign collusion with Russia; “fake news;” foreign information operations; divisive partisan politics; internet freedom in global trouble
- Raises the bar for what election cybersecurity has to achieve



# Contact information

David P. Fidler

Indiana University Maurer School of Law

211 S. Indiana Avenue

Bloomington, IN 47405

Tel: 812.855.6403

Email: [dfidler@indiana.edu](mailto:dfidler@indiana.edu)