IISE ANNUAL CONFERENCE & EXPO 2024

Securing Democracy: Threat Mitigations in Mail Voting Processes

Vanessa Gregorio[1], Natalie M. Scala[1], **Josh Dehlinger**[2]

[1]*Department of Business Analytics & Technology Management*
[2]*Department of Computer & Information Sciences*
Towson University

About Us

- Empowering Secure Elections Research Lab at Towson University
  - Non-partisan, interdisciplinary research lab focused understanding the risks to election processes and developing mitigations to the cyber, physical, and insider risks that can arise
  - Partnered with Maryland Boards of Elections to develop targeted, poll worker training modules to develop awareness of threats in elections processes and equipment
  - 2020 U.S. Elections Assistance Commission Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology
  - Analyzed risks to mail-based voting processes, updated the EAC's attack tree, and were the first to develop a relative risk assessment for U.S. elections (Scala et al., 2022)
    - Demonstrated that mail-based voting increases voter access and disincentivizes attacks from adversaries

Motivation

How do we ensure their votes count as they intended?

How do we ensure elections are secure?

Focus: Polling Places

Not part of the discourse

Still integral to the voting process

Motivation

- Pivot to mail voting during the 2020 Primary & General Elections as a result of COVID-19
  - Spread of misinformation about election integrity
  - No evidence of widespread election fraud
- Necessity to identify and mitigate actual risks in mail voting
  - Lack of existing research
  - Lack of poll worker training
  - Implications for democracy

Context

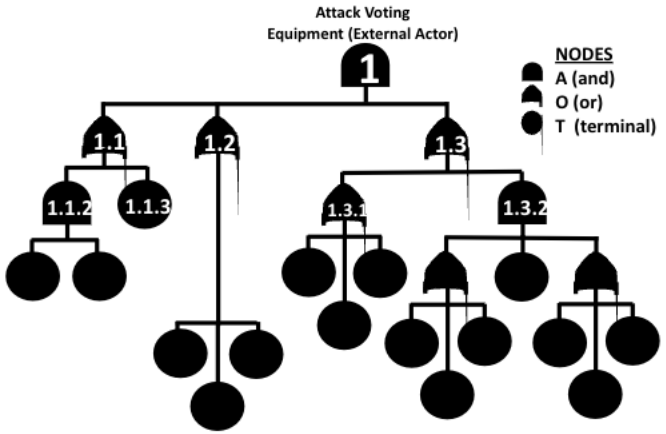
Inventories of vulnerabilities and known incidents

Human as trusted insider threat not considered

Socio-technical, critical infrastructure systems need a threat analysis case to demonstrate their fit for purpose

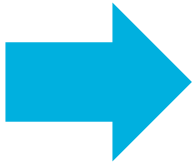
Conducting Risk Analyses

- Minimize number and impact of negative consequences
- Utilize a combination of reactive, proactive, and predictive approaches
- Defense in depth strategy
  - Threat tree analysis
  - Delphi method
  - Allocate resources based on risks of most concern

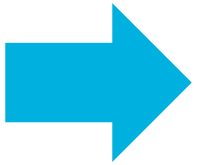


Conducting Risk Analyses

Build a comprehensive list of threats first



Map mitigations to threats they can counteract



Continuous review after finalizing

Features of Mail Voting that Must Be Accounted For

- Most threats are from insiders who try to genuinely participate in elections, not external malicious actors
- No in-person interactions between voters and poll workers
- Process lasts over a period of time
- Voting procedures are not federalized
  - If mistakes are made, the ballot cure process varies across all states
  - Threats will differ for each district, so mitigations must be tailored to their unique needs

Our Approach

Systems approach needed to develop threat model and analysis [Price et al., 2019]

- Cyber, physical and insider threats

Risk model framework to assess threats and countermeasures [Locraft et al., 2019; Scala et al., 2020]

- Extensive research to identify vulnerabilities

Systemic Threats

First academic team to define threats systemically in elections

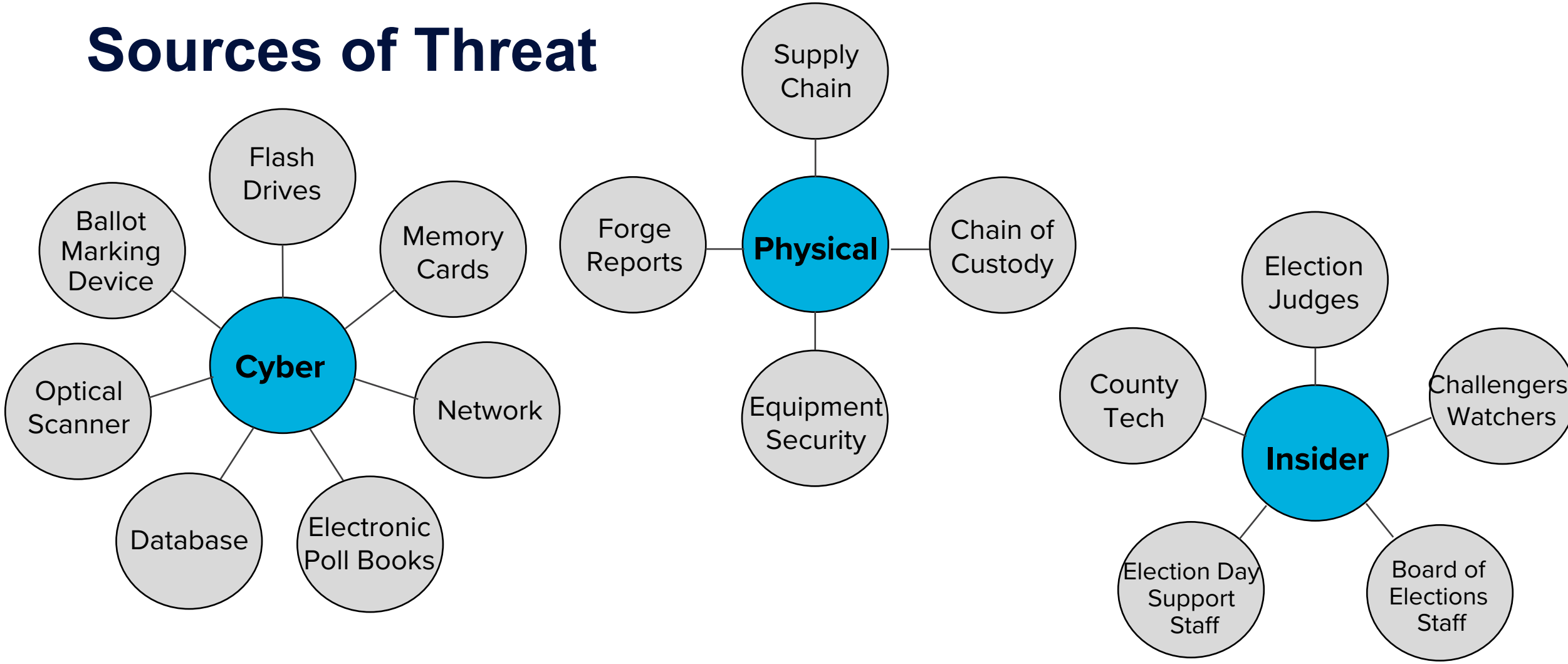
Framing extends beyond elections

Cyber
- Digital machines and media
- Regardless of Internet connection

Physical
- Tampering with or disrupting equipment

Insider
- Adversaries and insiders
- Simple, honest mistakes
- Deliberate actions with ill-harm effects

Sources of Threat



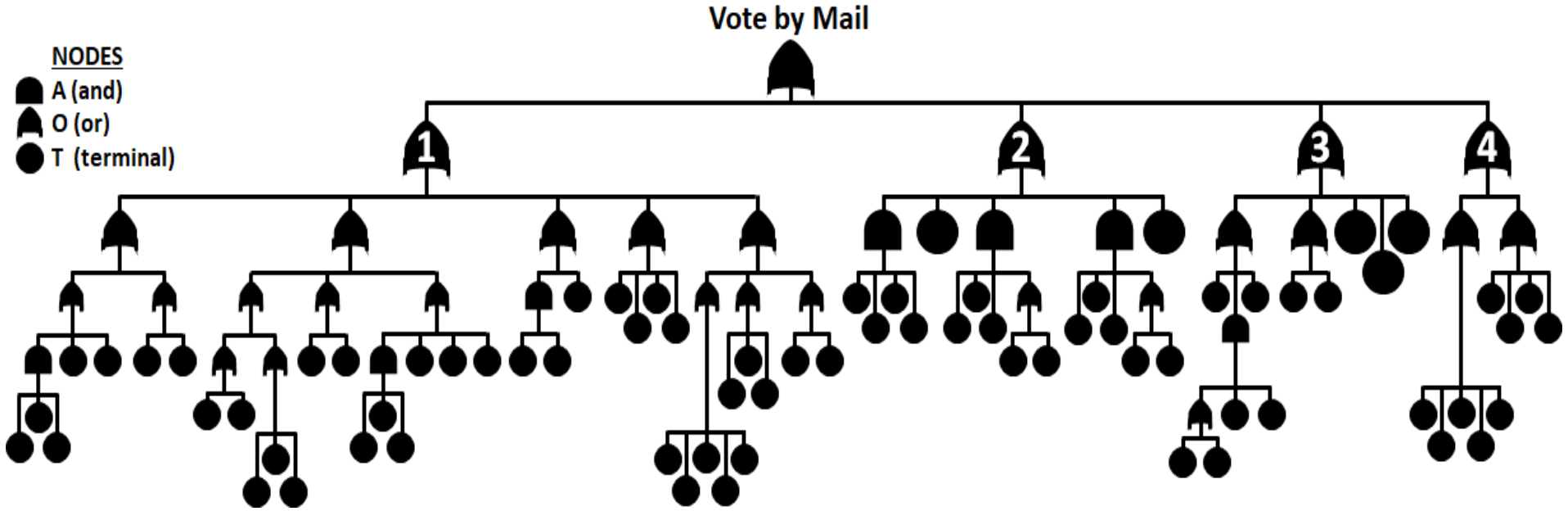
Attack Trees and Risk Analysis

- Attack tree is inventory of risks
  - Does not identify strength or likelihood
  - Threats and scenarios: Systemic sources
- Decompose complex actions into hierarchical levels
- Graphic representation of security problem
- EAC data: Much has changed

Previous Research on Mail Voting Threats & Mitigations

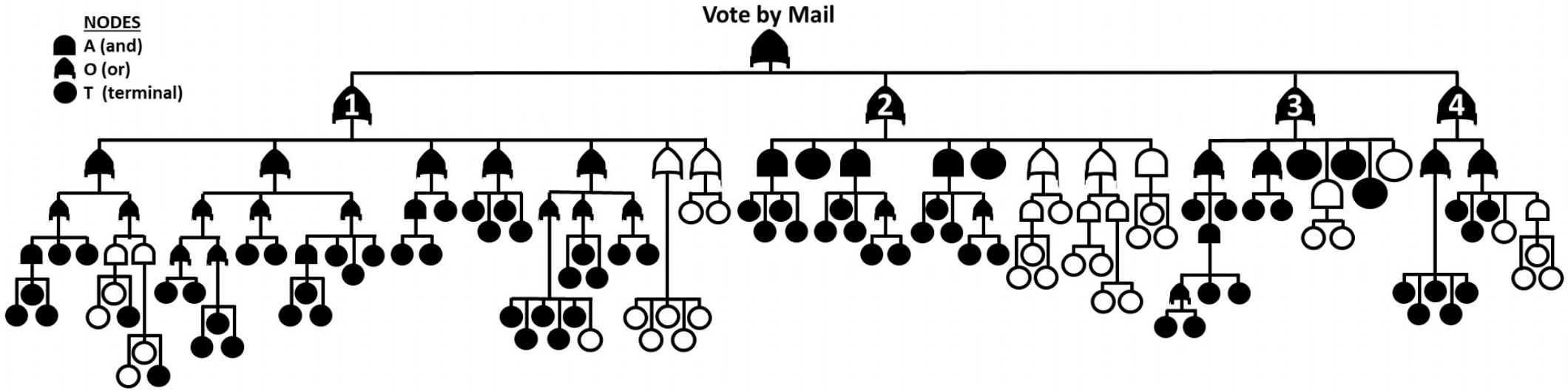
- Election Operations Assessment (EAC, 2009): attack trees for voting processes, including mail voting
- Scala et al. (2021): mail voting process maps
- Scala et al. (2022): updated mail voting attack tree from EAC (2009) & calculated risk
- Haseltin et al. (2021) began formalizing list of mitigations for mail voting threats outlined in EAC (2009) and Scala et al. (2022)

Vote by Mail Attack Tree (EAC, 2009)



- Threat scenarios
  - Insider = 32
  - External = 16
  - Voter error = 9
  - Total = 57

Updated Attack Tree



- 30 new threats
- Threat scenarios
  - Insider = 40
  - External = 23
  - Voter error = 10

Strength or Likelihood of Threat

Consider utility on three dimensions

- Attack cost (AC) u_1
- Technical difficulty (TD) u_2
- Discovering difficulty (DD) u_3

Terminal nodes

Criteria adapted from Du and Zhu (2013)

Attack Cost (AC)		Technical Difficulty (TD)		Discovering Difficulty (DD)	
Grade	**Standard**	**Grade**	**Standard**	**Grade**	**Standard**
5	Severe consequences likely	5	Extremely difficult	1	Extremely difficult
4	High consequences likely	4	Difficult	2	Difficult
3	Moderate consequences likely	3	Moderate	3	Moderate
2	Mild consequences likely	2	Simple	4	Simple
1	Little to no consequences likely	1	Very simple	5	Very simple

Updating Previous Research

- Our research builds off of [Haseltin et al., 2021], which:
  - Created a list of mitigations for time-based, insider, and cybersecurity threats, and
  - Mapped these mitigations to insider threats in the updated mail voting attack tree
- Our work…
  - Adds four new threats to [Haseltin et al., 2021]'s list
  - Maps mitigations to all threats in the updated mail voting attack tree

Mail Voting Threat Mitigations

Mail Voting Threat Mitigation List			
M1: Encourage voter registration in local districts	M2: Verify the mailing address and contact information	M3: Send a notification via text, email, or voice alert via BallotTrax/BallotScout	M4: Replacement ballot package request
M5: Notify voter to send the ballot back before the deadline	M6: In-person absentee voting	M7: Drop the ballot at drop boxes	M8: Monitor election staff misbehavior
M9: Provide sufficient and comprehensive election staff training	M10: Video monitoring	M11: Ballot design	M12: Enhanced IT resources
M13: Storage security	M14: Equipment security	M15: Voter roll upkeep	M16: Enhance voter education

No shading: adapted from [Carmen's paper]

Shading: new mitigations

Mail Voting Threat Mitigations

Mitigation	Description	Threats
M11: Ballot design	Mail ballots with clear and easily understandable instructions and design will ensure that voters are able to correctly complete their mail ballot package. Multiple formats should be available to accommodate voters with disabilities or voters who speak/understand other languages than English.	• Mail ballot has confusing, misleading, or incorrect instructions • Mail ballot has confusing, misleading, or incorrect design • Voter completes mail ballot package incorrectly or does not vote because of poor instructions or design

Key Takeaways

- Socio-technical, critical infrastructure systems are at risk to cyber, physical, and insider threats and need threat analysis cases to demonstrate their fit for purpose
- Understanding threats enables for effective development and analysis of mitigations

IISE ANNUAL CONFERENCE & EXPO 2024

Dr. Josh Dehlinger
jdehlinger@towson.edu

Remember to complete your evaluation for this session within the app!

iise.org/annual #IISEANNUAL2024