Quantitative Threat Modeling and Risk Assessment in the Socio-Technical Critical Infrastructure Systems

Dr. Natalie M. Scala and **Dr. Josh Dehlinger**

SoS Virtual Institute (VI) Mid Year Meeting

July 2024

Berkely, CA

EMPOWERING SECURE ELECTIONS

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)

What about the Typical American?

How do we ensure their votes have integrity?

Who are the People at a Polling Place?

Poll workers

Insiders!

Voters

Why We Are Here

- Senate Intelligence Committee (2019): Election systems in all 50 states targeted in 2016
- Robert S. Mueller, III (2019): Interference ongoing
- Director of National Intelligence (2020): Iran and Russia obtained US voter registration information
- Election infrastructure designated as national critical infrastructure (2017)
- Election infrastructure are socio-technical systems administered by trusted insiders

Context and Motivation

EMPOWERING SECURE ELECTIONS

- 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

Case Study

- Precinct Count Optical Scanners (PCOS) used in ~70% of US
- Previous threat assessment by Elections Assistance Commission (EAC) in 2009
- Administered by poll workers (i.e., temporary, seasonal, trusted insiders)

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
- Adapting approaches used in software safety analysis and establishing safety cases

Research Agenda

EMPOWERING SECURE ELECTIONS

Model the relative risks of adversaries and trusted insiders exploiting threat scenarios in developed attack trees, using critical infrastructure precinct count optical scanner (PCOS), in-person voting machines as a case study.

Year 1 ongoing effort (outcomes 1–3)

Outcomes	*Year 1*	*Year 2*	*Year 3*
1. A comprehensive, updated attack tree and mitigation analysis for critical infrastructure equipment and processes	√		
2. A scenario analysis to categorize threat scenarios as cyber, physical, or insider with an adversarial or insider source	√		
3. A risk assessment of threat scenarios on the updated attack tree that considers insider / adversarial attack costs and technical difficulties as well as information assurance assessments of the difficulties to discover an attack	√	√	
4. The identification of risks of most concern within the process across temporal phases		√	
5. An impact analysis of suggested policy implications and security mitigations (e.g., adversarial implications, human behavior interdictions) and their ability to reduce cyber, physical, and insider risks			√
6. The dissemination of the threat and mitigation analyses results		√	√
7. An assessment of the systematic threat and mitigation analysis approach's utility for use in national critical infrastructure socio-technical systems and processes, and recommendations for the adoption of the approach at the national level		√	√

Outcome 1 – Attack/Threat Tree

Goal - *A comprehensive, updated attack tree and mitigation analysis for critical infrastructure equipment and processes.*

Approach - Bi-directional analyses focusing on developing an updated threat tree, using adapted SFMEA/SFMECA for validation/completeness, as a basis to develop threat scenarios.

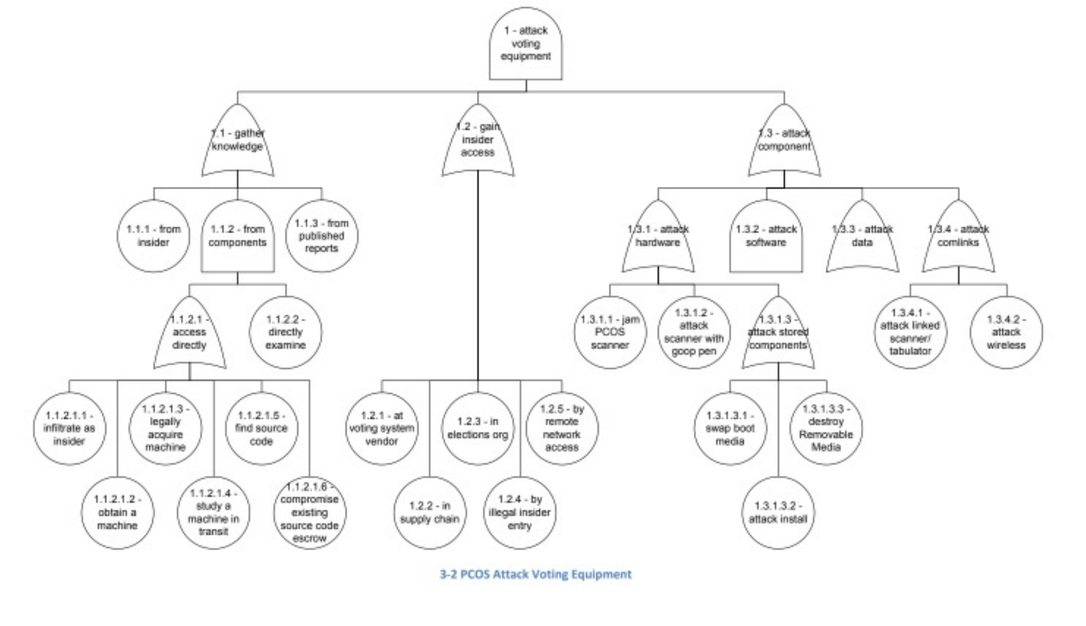
1. Identify/update new threats not found in existing EAC (2009) PCOS threat tree
2. Validate threat completeness with SFMEA/SFMECA
3. Develop updated attack tree

Status – Complete

Attack Trees and Risk Analysis

EMPOWERING SECURE ELECTIONS

- Attack tree is inventory of risks
  - Does not identify strength or likelihood
  - Threats and scenarios: systemic sources
- Decompose complex actions into hierarchical levels
  - A top-down, forward analysis approach that goes from security incident (i.e., hazards) to the underlying contributing threats (i.e., failure modes)
- Graphic representation of security problem
- EAC data: Much has changed



Partial EAC PCOS Threat Tree (2009)

Investigating Attack Tree Revisions

Needs

- Threats to critical infrastructure
- Adaptive adversary

Validation

- Bi-Directional Analysis using adapted SFMEA/SFMECA
- Boards of Elections
  - Maryland counties
- Comparison to BMD threat analysis

Sources of data

- Mainstream, non-partisan news articles
- Bipartisan or non-political think tanks
- Academic centers
- Voter instruction sheets
- State-created documentation
- Poll worker training manuals

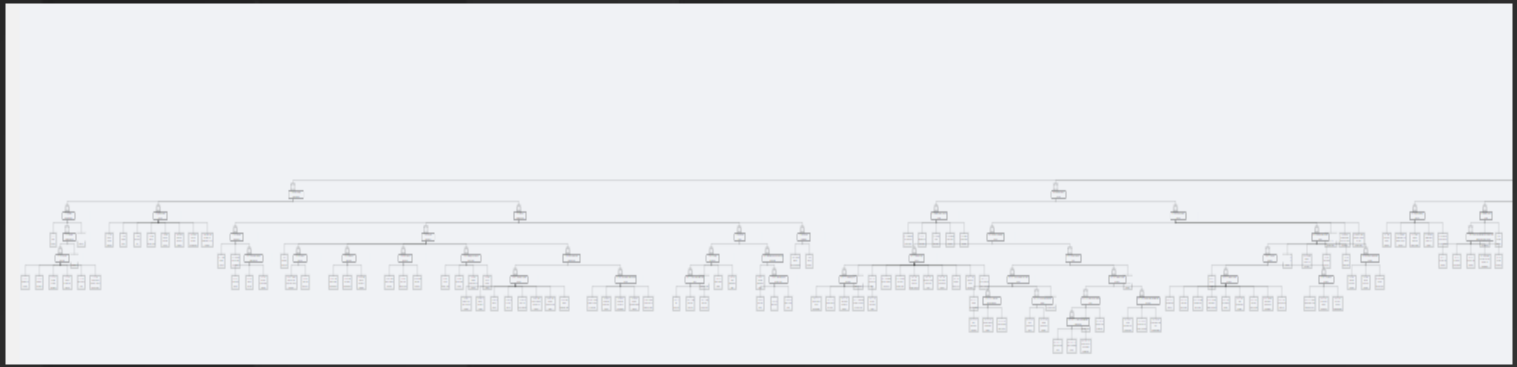
Software Failure Modes, Effects and Criticality Analysis

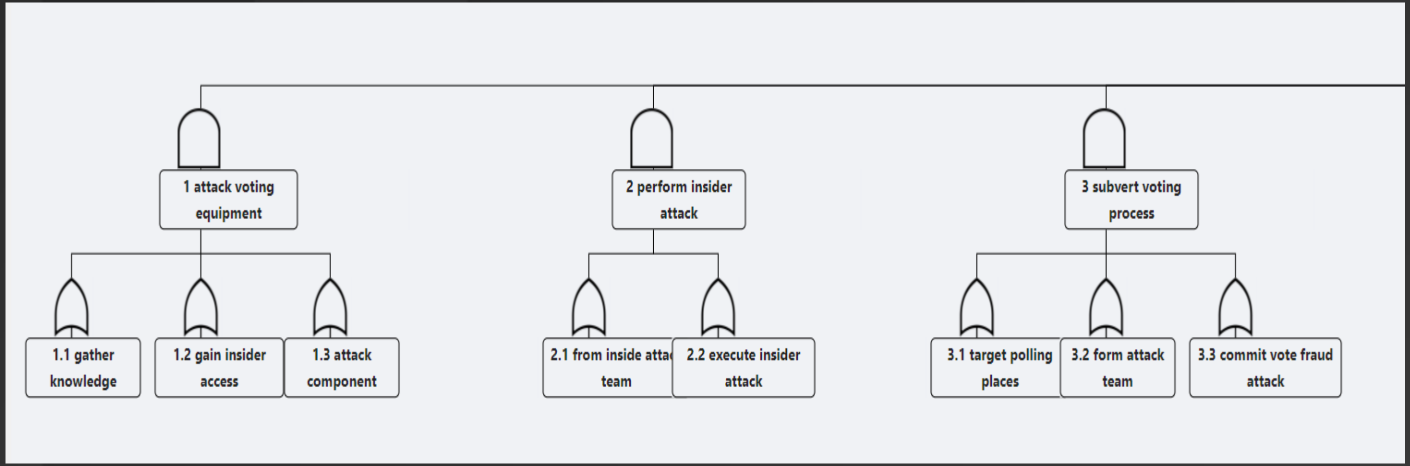
- A bottom-up, forward analysis to identify and address potential problems, or failures and their resulting effects on the system
- Performed independently and in parallel to threat tree analysis, is bi-directional in that it combines a forward analysis (from failure modes to effects) with a backward analysis (from hazards to contributing causes)
- Used to discover potential threats of in-person voting using PCOS machine to complete/validate the threat tree

Potential Failure Mode	Potential Effects of Failure	S	Potential Causes of Failure	O	D
	Misrepresent voter intent	Critical	Data entry error	A moderate probability of occurrence	Good detectability
	Voter confusion and disruption	Important	Inconsistent proofreading	A moderate probability of occurrence	Good detectability
Ballot printing error	Legal and Administrative challenge	Critical	Lack of transparency	An occasional probability of occurrence	Good detectability
	Misrepresent voter intent	Critical	Data entry error	A moderate probability of occurrence	Good detectability
		Critical	Technical Malfunction in Voting Machines	An occasional probability of occurrence	Good detectability
		Critical	Human Error in Data Entry	A moderate probability of occurrence	High degree of detectability
Ballot reading error	Miscounted votes	Critical	Cybersecurity Attacks on Voting Systems	An unlikely probability of occurrence	Likely to detect
	Voter confusion and disruption	Critical	Electrical outage	An occasional probability of occurrence	Fair detectability
		Critical	Communication Breakdown	A moderate probability of occurrence	Good detectability
	Loss of Voter Confidence (Doubts ab	Critical	Inadequate Contingency Planning (Lack of backup sys	An occasional probability of occurrence	Fair detectability
		Important	Server Failures	A moderate probability of occurrence	High degree of detectability
	Data Integrity Issues	Important	Cybersecurity Attack	A remote probability of occurrence	Likely to detect
		Important	Equipment Malfunctions	An occasional probability of occurrence	Good detectability
Infrastructure outage	Extended Voting Periods	Important	Insufficient Staffing	A moderate probability of occurrence	Fair detectability
	Voter does not influence the election	Disastrous	Calibration error	A remote probability of occurrence	Fair detectability
Machine does not count vote	Dissatisfied voters	Important	Unreplacable parts	A remote probability of occurrence	Fair detectability
		Important	Technical Glitches in User Interface	An occasional probability of occurrence	Good detectability
	Dissatisfied voters	Important	Unclear Instructions on Machine Use:	A moderate probability of occurrence	Fair detectability
		Important	Machine Calibration Issues	An occasional probability of occurrence	Good detectability
		Important	Limited Number of Voting Machines	A high probability of occurrence	High degree of detectability
Voters have difficulties using machine	Increased Waiting Times	Important	User Error in Operating Machines	A moderate probability of occurrence	Fair detectability
	Dissatisfied voters	Critical	Poor Planning/Troubleshooting	A moderate probability of occurrence	High degree of detectability
		Critical	Systematic Backup Failure	A moderate probability of occurrence	Fair detectability
		Critical	Unanticipated Technical Glitches	An occasional probability of occurrence	Good detectability
	Data Loss	Critical	Human Error in Backup Management	A moderate probability of occurrence	Good detectability
		Important	Hardware Failures without Redundancy	A high probability of occurrence	Low or no detectability
		Important	Insufficient Contingency Planning	An occasional probability of occurrence	Fair detectability
No backups in case of failure	Extended Downtime	Important	Software Incompatibility Issues (Incompatibility issues	A moderate probability of occurrence	Fair detectability
	Voter confusion and disruption	Critical	Poor Planning/Troubleshooting	A moderate probability of occurrence	High degree of detectability
		Important	Insufficient Ballot Stock at Polling Stations	A moderate probability of occurrence	Fair detectability
		Important	Inefficient Ballot Distribution Process:	An occasional probability of occurrence	Good detectability
	Longer Waiting Times	Important	Unexpected Surges in Voter Turnout	An occasional probability of occurrence	Fair detectability

Partial New PCOS SFMECA

Updated PCOS Threat Tree





- 5 new subtrees
- New threats
  - Insider = 14
  - Physical = 21
  - Cyber = 4

  Total = 49

Outcome 2 – Threat Scenario Analysis

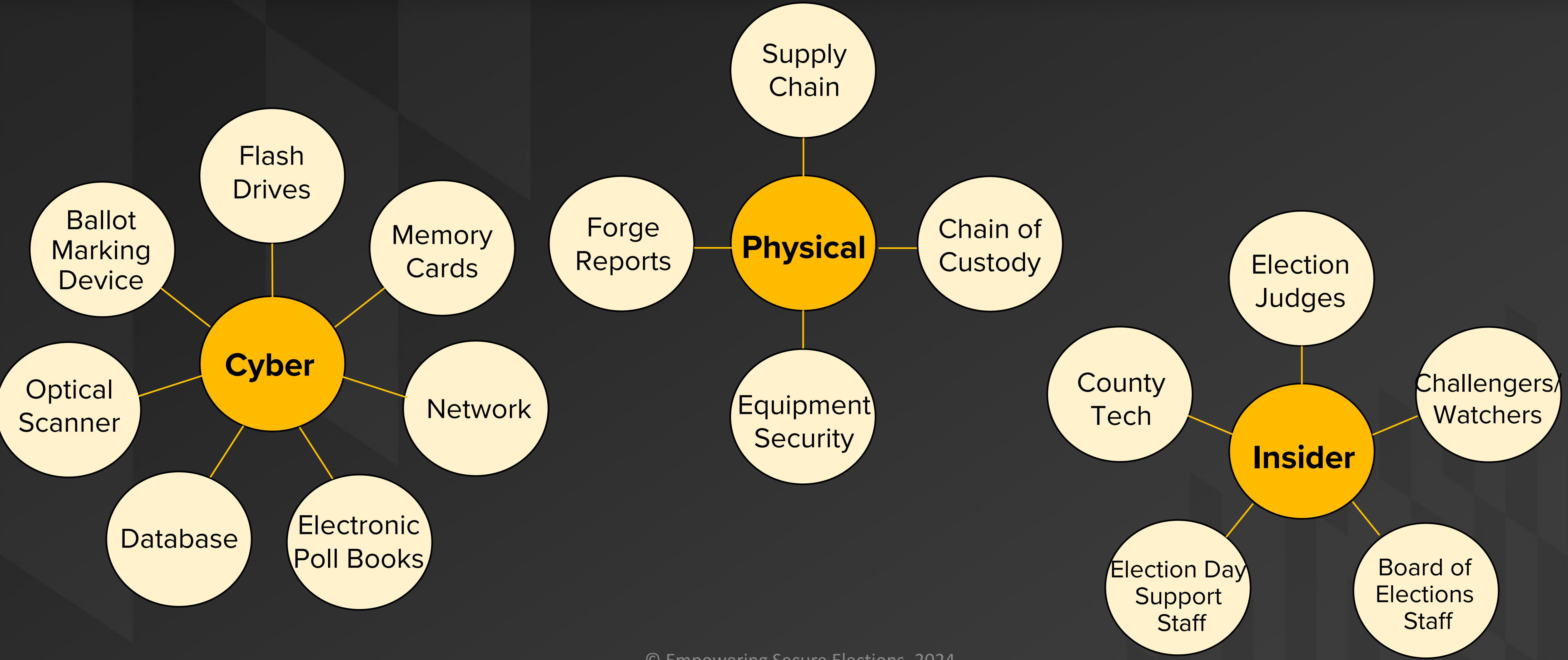
Goal - *A scenario analysis to categorize threat scenarios as cyber, physical, or insider with an adversarial or insider source.*

Approach – Analyze updated threat tree to identify source and timing of threats to enable the generation of informative threat scenarios.

1. Annotate each threat source as being a cyber, physical or insider threat
2. Annotate each threat with temporal information based on Voluntary Voting System (VVS) / NIST IR 8310 phase guidelines
3. Develop/adopt tooling to generate threat scenarios from an attack tree

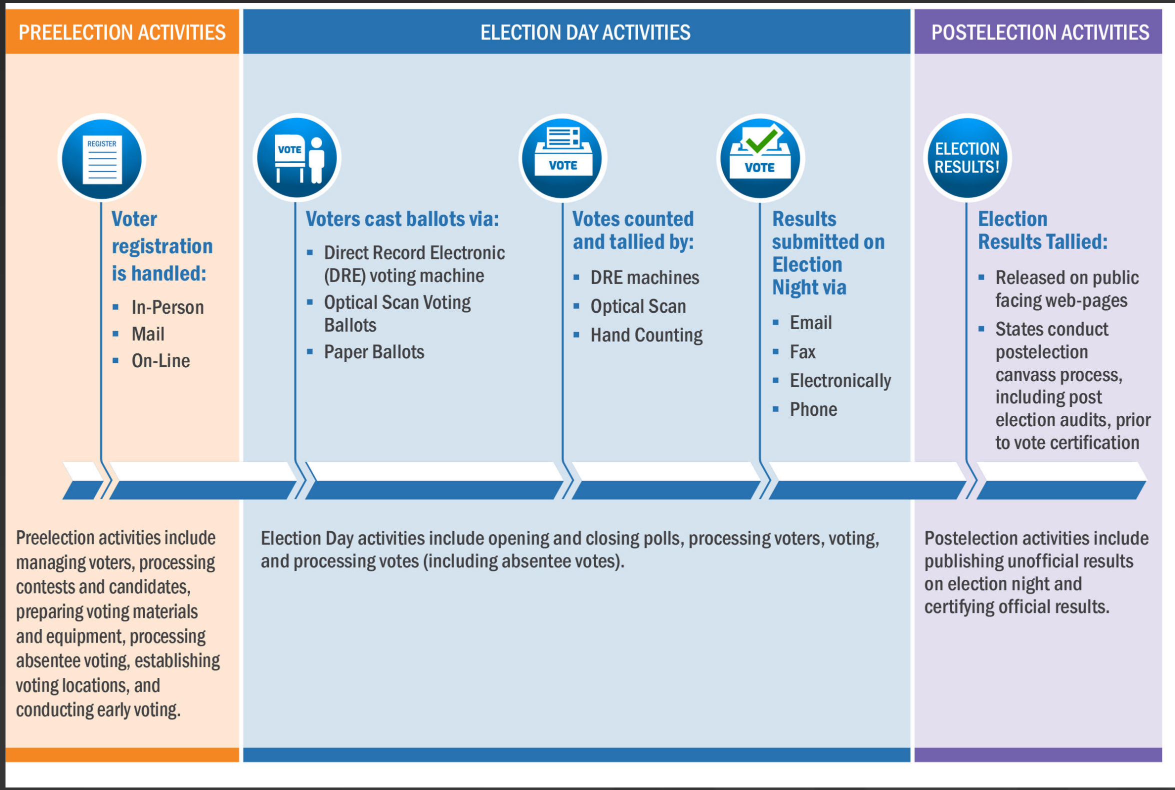
Status – Complete / Ongoing

Sources of Threat



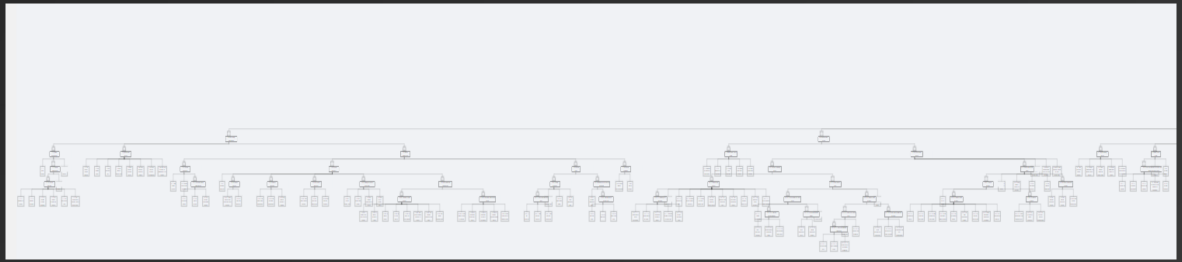
Timing of Threats

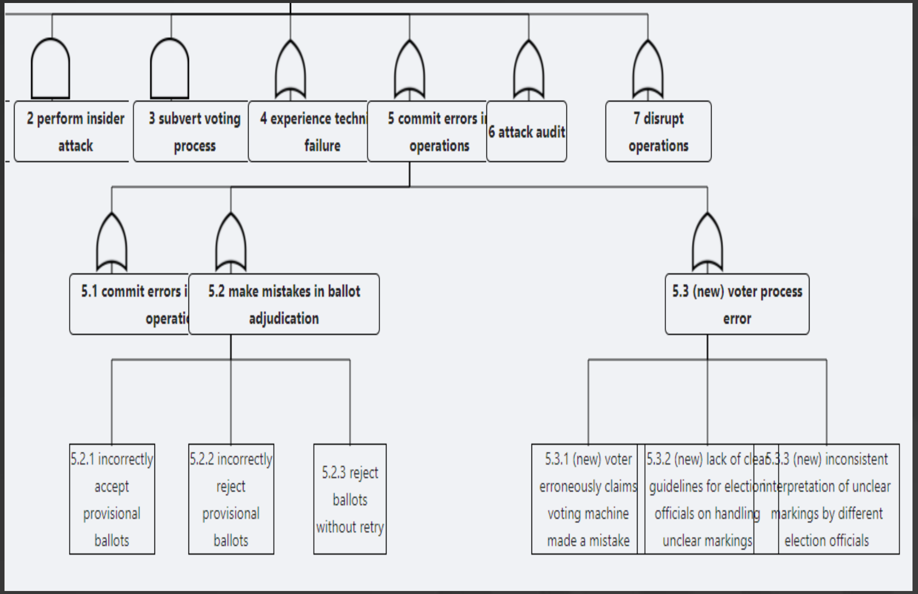
- Volunteer Voting System Guidelines (2015) and NIST IR 8310 (2021)
  - Phase 1 – Election Preparation
  - Phase 2 – Election Day Activities
  - Phase 3 – Postelection Activities
- To be used for later risk assessment of threat scenarios and mitigation development



Threat Scenarios from Threat Trees

- Threat scenarios are ”activations” of terminal nodes to cause a parent threat to occur
- Socio-technical, critical infrastructure threat trees too complex and needs tooling
  - Threat scenario generation
  - Relative likelihood occurrence calculation
  - General usability & dissemination





Threat Scenarios from Threat Trees Tooling

EMPOWERING SECURE ELECTIONS

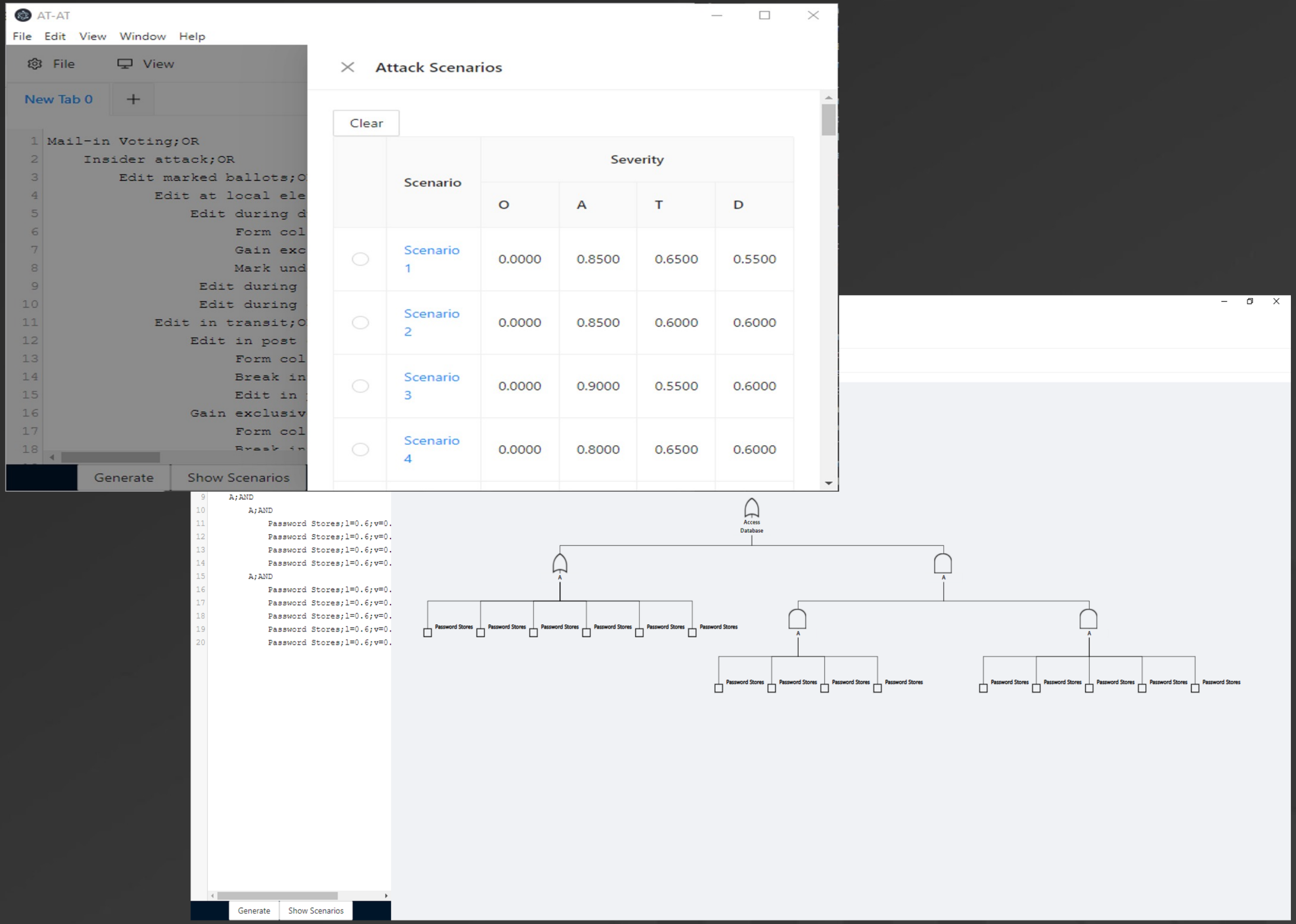
- Find COTS tool
  - EMFTA
  - OpenFTA
  - ALD Fault Tree Analyzer
- Build a tool
- Find a tool to modify
  - Open-source tool to customize for specific needs

*table

	Name	Description	Probability
Event crash	crash	The computer crashes	1.4000210000000003E-4
Gate OR			
Event Interrupt	Interrupt	Unhandled interrupt	4.0E-5
Event Broken	Broken	Device is broken	1.0E-4
Event software	software	Software error	2.0999999999999998E-9
Gate AND			
Event DBZ	DBZ	Divide By Zero	7.0E-5
Event Recovery	Recovery	Missing Recovery	3.0E-5

Threat Scenarios from Threat Trees Tooling

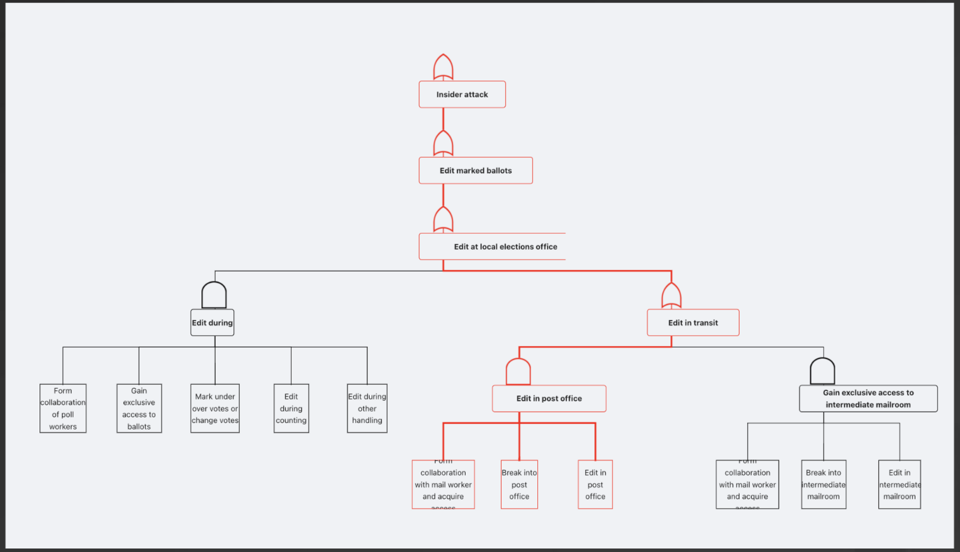
- AT-AT (Attack Tree Analysis Tool) OSS
  - Intuitive tree formatting
  - Some metrics calculations
  - Partial threat scenario analysis/generation
- Internally validated it’s correctness and fit for purpose



Threat Scenarios from Threat Trees Tooling Improvements

EMPOWERING SECURE ELECTIONS

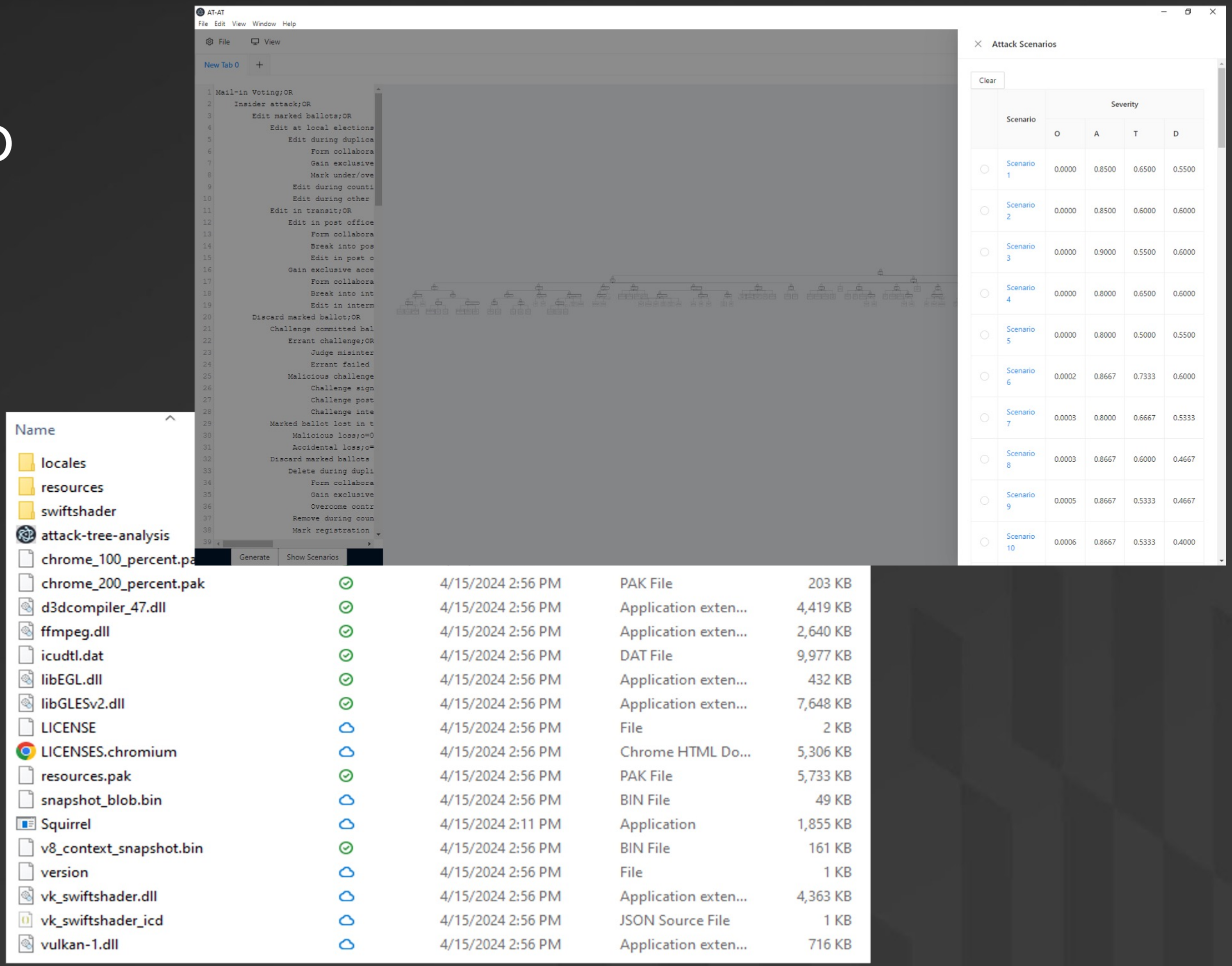
- Standalone, React JavaScript application available as beta tool from GitHub
- Changed the metrics being measured to reflect ESE's metrics: Attack Cost, Technical Difficulty, Discovery Difficulty, and Relative Occurrence
- Improved readability and presentation
- Instant scenario analysis
- Highlighting of specific scenarios



	Scenario	Severity			
		O	A	T	D
○	Scenario 1	0.0000	N/A	N/A	N/A
○	Scenario 2	0.0003	N/A	N/A	N/A
◉	Scenario 3	0.0002	N/A	N/A	N/A

Threat Scenarios from Threat Trees Tooling Ongoing Development

- Incorporating notion of timing into threat scenarios
- Highlighting of specific scenarios
- Exporting tree as a graphic
- Showing only the subtree associated with a scenario
- General UI improvements
- Dissemination as online application



Outcome 3 – Risk Assessment

Goal - A risk assessment of threat scenarios on the updated attack tree that considers insider / adversarial attack costs and technical difficulties as well as information assurance assessments of the difficulties to discover an attack.

Approach – Apply a utility assessment to each threat for scenario risk assessment

1. Using a Delphi approach to assign technical difficulty, discovery difficulty and attack cost to each threat
2. Generate all threat scenarios, with assigned utility assessment, to quantitatively calculate relative likelihood risk of threat scenarios

Status – Ongoing

Strength or Likelihood of Threat

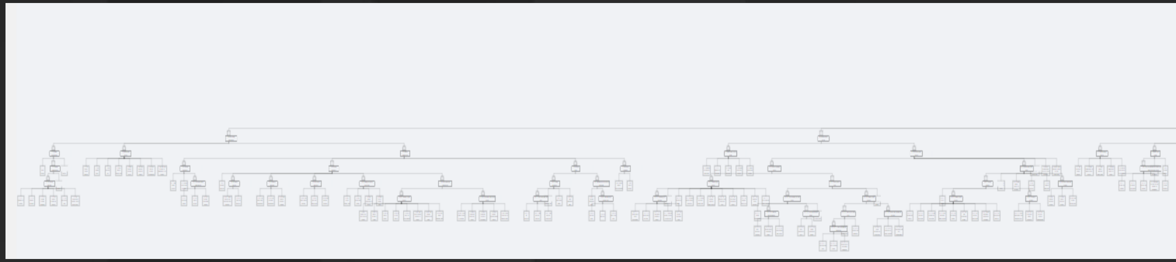
EMPOWERING SECURE ELECTIONS

- 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)

	Scenario	Severity			
		O	A	T	D
○	Scenario 1	0.0000	N/A	N/A	N/A
○	Scenario 2	0.0003	N/A	N/A	N/A
◉	Scenario 3	0.0002	N/A	N/A	N/A

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

Threat Scenarios from Threat Trees



	Scenario	Severity			
		O	A	T	D
○	Scenario 1	0.0000	N/A	N/A	N/A
○	Scenario 2	0.0003	N/A	N/A	N/A
◉	Scenario 3	0.0002	N/A	N/A	N/A

- Assess the existing mitigation analysis techniques that are specific to actions of adversaries and trusted insiders
- Develop an approach for risk modeling and mitigation analysis for socio-technical systems
- Identify attack scenarios to model threats across temporal phases and examine how risks may evolve
- Calculate relative likelihood risk of threat scenarios to socio-technical critical infrastructure equipment across temporal phases
- Develop policy implications and model the ability of mitigations to impact the relative likelihood of risks and threat scenarios

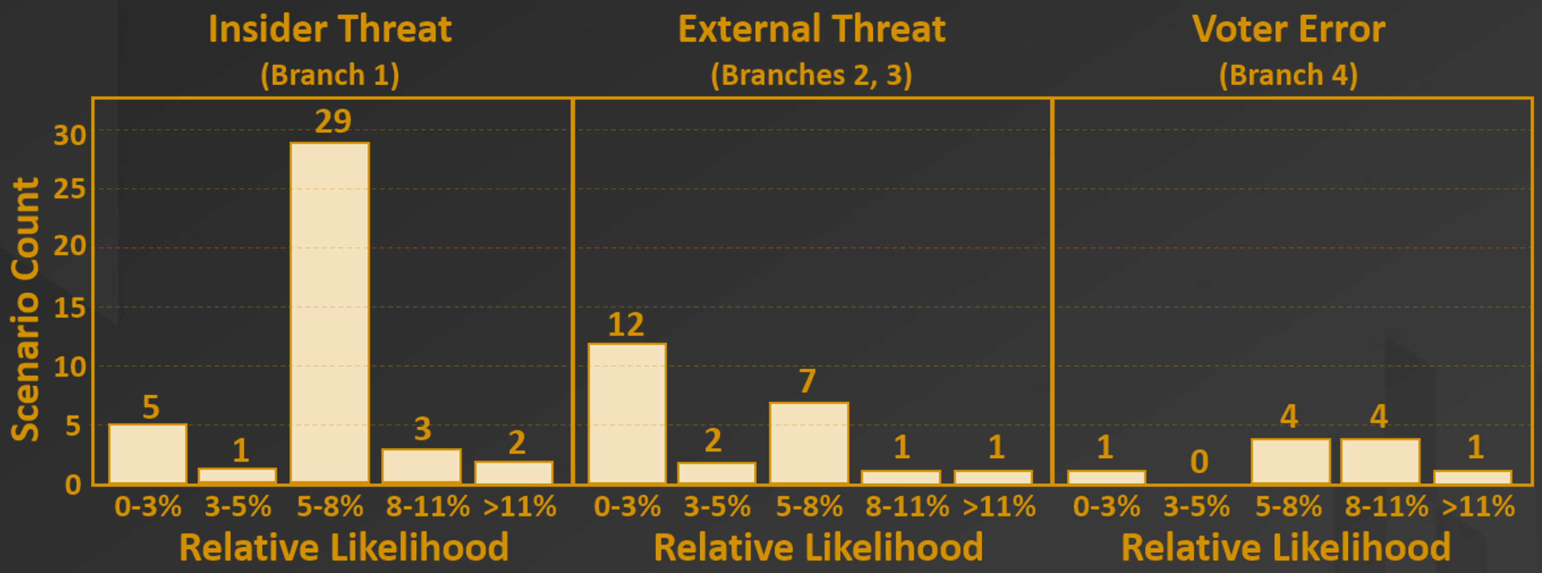
Threats of Most Concern - Ongoing

EMPOWERING SECURE ELECTIONS

Scenario	Threat		Relative Likelihood	Branch
S_7	X_9	Errant failed signature	0.12	Insider
S_{12}	X_{14}	Accidental loss	0.10	Insider
S_{23}	X_{28}	Fail to stuff envelope	0.11	Insider
S_{32}	**X_{36}**	**Lost in destination mailroom**	**0.13**	**Insider**
S_{47}	X_{53}	Malicious “messenger ballots”	0.10	External
S_{58}	**X_{61}**	**Debate and vote parties**	**0.12**	**External**
S_{64}	**X_{65}**	**Failure to sign correctly**	**0.13**	**Voter Error**
S_{66}	X_{67}	Failure to bundle correctly	0.11	Voter Error

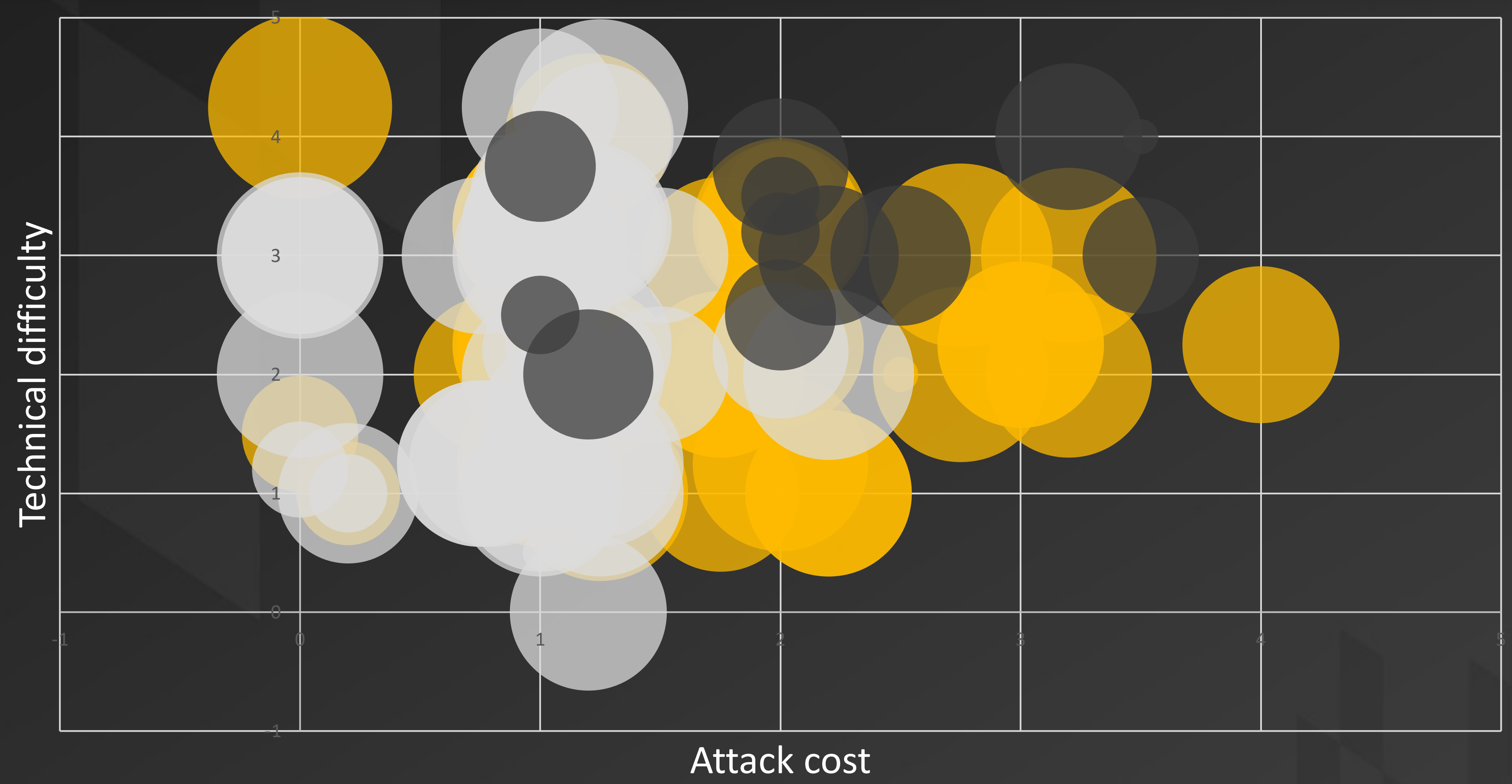
Scenario Likelihood - Ongoing

- Insider: Majority of scenarios
- External: Very low relative likelihood



Threat Impact - Ongoing

EMPOWERING SECURE ELECTIONS



- Considering attack cost, technical difficulty, discovering difficulty
- Yellow = insider threats, white = external threats, black = voter error threats

Moving Forward

Model the relative risks of adversaries and trusted insiders exploiting threat scenarios in developed attack trees, using critical infrastructure precinct count optical scanner (PCOS), in-person voting machines as a case study.

Next 6 months effort (items 3–4)

Outcomes	*Year 1*	*Year 2*	*Year 3*
1. A comprehensive, updated attack tree and mitigation analysis for critical infrastructure equipment and processes	√		
2. A scenario analysis to categorize threat scenarios as cyber, physical, or insider with an adversarial or insider source	√		
3. A risk assessment of threat scenarios on the updated attack tree that considers insider / adversarial attack costs and technical difficulties as well as information assurance assessments of the difficulties to discover an attack	√	√	
4. The identification of risks of most concern within the process across temporal phases		√	
5. An impact analysis of suggested policy implications and security mitigations (e.g., adversarial implications, human behavior interdictions) and their ability to reduce cyber, physical, and insider risks			√
6. The dissemination of the threat and mitigation analyses results		√	√
7. An assessment of the systematic threat and mitigation analysis approach's utility for use in national critical infrastructure socio-technical systems and processes, and recommendations for the adoption of the approach at the national level		√	√

Synergistic Work

EMPOWERING SECURE ELECTIONS

- Partnered with Maryland Boards of Elections to develop poll worker training specific to the cyber, physical, and insider threats to specific voting processes [Scala et al., 2020]
- Previously analyzed the mail-voting process to develop a threat tree and threat scenarios [Scala et al., 2022]
- Investigating how election misinformation spreads and its impact on voter confidence [Riley et al.,2023]
- Understanding the impact of poll workers' *cyber hygiene* on election security [Kassel et al., 2024]
- Analyzing Ballot Marking Devices (BMD) to develop threat trees and threat scenarios [tbd, 2024]
- Partnering with Maryland Boards of Elections to survey Maryland voters' perception and confidence of the voting process [Merivaki et al., 2024]

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
- Poll workers are highly seasonal, trusted insiders to a national critical infrastructure process that may inadvertently introduce risks
- Understanding threats enables for effective poll worker training, protective mitigation strategies, and policy development

Our Papers

EMPOWERING SECURE ELECTIONS

- A. Kassel, I. Bloomquist, N. M. Scala, and J. Dehlinger. “Analysis of Poll Worker Security Behaviors to Secure U.S. Elections”. Presented at *American Society for Engineering Management 2023 International Annual Conference and 44th Annual Meeting*, October 2023.
- N. M. Scala, J. Dehlinger, and L. Black. “Preparing Poll Workers to Secure U.S. Elections”. Presented at *American Society for Engineering Management 2023 International Annual Conference and 44th Annual Meeting*, October 2023.
- J. Riley, V. Gregorio, N. M. Scala, and J. Dehlinger. “Voting Perceptions and Impact of Misinformation”. Presented at *NATO Operations Research and Analysis Conference*, October 2023.
- V. Gregorio, J. Dehlinger, and N. M. Scala. “Protecting Maryland’s Mail Voting Processes through Poll Worker Training”. In *Baltimore Business Review*, January 2024.
- A. Kassel, I. Bloomquist, N. M. Scala, and J. Dehlinger. “Understanding the Impact of Poll Worker Cybersecurity Behaviors on U.S. Election Integrity”. In *Proceedings of the Institute of Industrial and Systems Engineers (IISE) Annual Conference and Expo 2024*, May 2024.
- H. Nguyen, N. M. Scala, and J. Dehlinger. “Analysis of Security Behaviors of Supply Chain Professionals”. In *Proceedings of the Institute of Industrial and Systems Engineers (IISE) Annual Conference and Expo 2024*, May 2024.

Questions?

EMPOWERING SECURE ELECTIONS

Dr. Natalie M. Scala

Email: nscala@towson.edu

Web: www.drnataliescala.com

Dr. Josh Dehlinger

Email: jdehlinger@towson.edu