CIRI Annual Meeting
December 6-7, 2022
Keynote Speaker

Brian Gattoni
CTO, CISA
CELEBRATING PARTNERSHIP

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

&

CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
CISA 101

**Mission**
We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

**Vision**
A secure and resilient critical infrastructure for the American people.
Current Threat Landscape

STOP RANSOM WARE

APT Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

SHIELDS UP
Joint Cyber Defense Collaborative

KEY JCDC CAPABILITIES

✓ Comprehensive, whole-of-nation planning to address risk both during steady-state operations and during an incident.

✓ Common situational awareness and analysis to equip public and private partners to take risk-informed coordinated action.

✓ Integrated cyber defense capabilities to protect the nation’s critical infrastructure.

✓ Flexibility in planning and collaboration to meet the cyber defense needs of the public and private sectors.

✓ Institutionalized exercises and assessments to continuously measure the effectiveness of cyber defense planning and capabilities.

✓ Work closely with the Sector Risk Management Agencies (SRMAs) to bring their unique subject matter expertise to tailored plans to address sector risk.

PARTNER WITH US FOR A MORE SECURE FUTURE

Collaborate with the JCDC to:

- Identify unique public and private sector planning requirements and capabilities
- Implement effective mechanisms for coordination
- Establish a set of shared risk priorities to inform a joint planning agenda
- Develop coordinated cyber defense plans
- Support joint exercises and assessments to measure the effectiveness of cyber defense operations
Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices

A Notice by the Homeland Security Department on 06/01/2022

AGENCY:
Cybersecurity and Infrastructure Security Agency, DHS.

ACTION:
Announcement of public listening sessions.

SUMMARY:
The Cybersecurity and Infrastructure Security Agency will facilitate a series of public listening sessions to build on existing community-led work around Software Bill of Materials ("SBOM") to specific SBOM topics.

(2) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(ivii) participating in a vulnerability disclosure program that includes

A mandatory vulnerability disclosure program shall provide a mechanism for SBOM developers to report vulnerabilities to the SBOM developer and any affected users. The vulnerability disclosure program shall include a process for handling and responding to reported vulnerabilities, including identifying and prioritizing vulnerabilities, reporting vulnerabilities to SBOM developers, and coordinating with affected users. The vulnerability disclosure program shall also include a process for ensuring that the SBOM developers are aware of the vulnerabilities and are taking appropriate action to address them. The vulnerability disclosure program shall be made available to SBOM developers and affected users through a publicly accessible website.

This notice is intended to provide guidance on best practices for developing and using SBOMs. The guidance shall include criteria that can be used to evaluate SBOMs, including the ability of SBOMs to identify software vulnerabilities and the ability of SBOMs to reduce the risk of cybersecurity incidents.

The guidance shall include criteria that can be used to evaluate SBOMs, including the ability of SBOMs to identify software vulnerabilities and the ability of SBOMs to reduce the risk of cybersecurity incidents.
Risk and Resilience

- **Connections** by technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity),
- **Distribution** methods that allow the movement of goods, people, and utilities inside and outside the United States (e.g., electricity distribution or cargo transportation),
- **Management** processes that ensure our national security and public health and safety (e.g., management of hazardous material or national emergencies), and
- **Supplies** of materials, goods and services that secure our economy (e.g., clean water, housing, and research and development).
Importance of R&D relationships
CISA is here to help
For more information:

www.cisa.gov
First some stats...

57

...the total number of projects executed (including those underway)
More stats...

22

...the total number of unique partners – academic + private sector
...the total number of “product” outputs
• Data sets, models, prototypes, software
More stats...

55

...the total number of academic papers & publications
More stats...

13/25/70

...the total number of unique MSIs/MSI faculty/MSI students supported

- 12 Summer Research Teams
- 5 Scientific Leadership Awards
More stats...

> 100

...the total number of students directly engaged
Our main challenges

- Identify key research needed for infrastructure resilience
- Execute impactful research possible at scale of CoE
- Make results useable --- **distill complexity** so that user can benefit w/o expert training
“We’re surrounded. That simplifies our problem...”
- Col. Chesty Puller, USMC
(Battle of Chosin Reservoir)
CIRI has

Developed understanding of resiliency lifecycle

Applied each phase to efforts in

- Research
- Tech transition
- Education and Workforce Development
CIRI has

Developed a solid understanding of

- scope
- interconnectedness
- interdependence

of critical infrastructure
- physical, cyber, and human/social
Examples

• Resilience Governance for Infrastructure Dependencies and Interdependencies; Flynn, NEU

• Identifying and Reducing Barriers to Infrastructure Insurance; Kunreuther, Wharton School, UPenn

• Regulatory Options for Managing Systemic Risks; Slayton, Cornell

• Scenario-based Flood Risk Mapping; Freitag, UW

• Community Resilience and Disaster Costs; McConkey, UIUC
CIRI has

Developed a solid understanding of the mission, strategic objectives, processes and culture of DHS

 Appropriately mapped our research portfolio and technology development roadmap to DHS mission
Examples

- Protecting the Nation’s 911 System from Cyber Attacks (UIUC, Karthik Consulting)
  - Researched requirements for PSAP cybersecurity
  - Developed & published NIST CSF-based PSAP Profile
  - Integrated Profile into Cyber Secure Dashboard
- NG911 Interoperability Testing (UIUC, TAMU)
  - Researched requirements for end-to-end testing of NG911 systems and components
  - Published recommendations for national interoperability testing framework
- Characterizing End-to-End Risks to 5G (GaTech)
  - Researched the end-to-end risks of 5G telecommunications infrastructure
  - How attacks on 5G can impact dependent infrastructure (i.e., connected autonomous vehicles)
  - Developed quantitative risk metrics
More Examples

- Safety & Security of Remote Bridge Operations (ABS Consulting)
  - Researched the cybersecurity risks to remote bridges
  - Developed & delivered Google Earth-based taxonomy of nations bridges
  - Developed & published NIST CSF-based Remote Bridges Profile
- Empirical Security Analysis of Wireless Emergency Alert System (Colorado Boulder)
  - Researched specific risk of spoofed message broadcast
  - Identified and tested mitigations to eliminate the risk
- EMP Risk Assessment & Mitigation (Synclesis, UIUC)
  - Researched EMP risk to 5G cell tower
  - Identifying mitigations to reduce risk
CIRI has

Demonstrated capability to successfully organize, scope, and manage multi-disciplinary, multi-institutional projects
Examples

• Toward Community Resilience through Comprehensive Risk Assessment, USC, UIUC
• Hybrid Quantum-Classical Reinforcement Learning in Controlled Quantum Networks, UTenn, Ucalgary
• Leveraging AI for Disaster Response, USC, UIUC
• Interoperability Testing Program, Texas A&M, U. Washington, UIUC
• Multi-Layer Cyber-Physical Supply Chain Risk Analysis, NYU, U. Michigan
• Research and Deliverables on Utilizing an Academic Hub and Spoke Model for Education, UIUC, Purdue, U. Tulsa, Auburn Univ.
• Quantifying Interdependence of the Logical-Physical Internet Topologies, UIUC, UC San Diego
• Measuring Business and Economic Resilience in Disasters-Business Resilience Calculator, USC, Ohio State
• Cybersecurity Assurance for Critical Infrastructure, UCLA, Carleton Univ.
• Review and Assessment of the Usage of Computational Methods for Humanitarian Assistance and Disaster, UIUC, USC, Harvard
CIRI has brought cutting edge technologies to critical infrastructure resilience:

- Software engineering
- Economics
- Quantum information
- Electromagnetics
- Data analytics, AI, ML/DL
- Operations analysis
CIRI has

Demonstrated capability to transition research outputs to the field/market
# Sample Tech Transition Efforts

<table>
<thead>
<tr>
<th>Project/Product</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRISM (Cyber Risk Scoring &amp; Mitigation)</td>
<td>Licensed to commercial company</td>
</tr>
<tr>
<td>Cyber Secure Dashboard</td>
<td>Pilot tests underway with PSAPs</td>
</tr>
<tr>
<td>Business Resilience Calculator</td>
<td>Completed RTI engagement</td>
</tr>
<tr>
<td></td>
<td>Provisional Patent application filed</td>
</tr>
<tr>
<td></td>
<td>Discussions with potential licensees underway</td>
</tr>
<tr>
<td>Port Disruptions Tool</td>
<td>Provisional Patent application filed</td>
</tr>
<tr>
<td></td>
<td>NSF iCORPs completed</td>
</tr>
<tr>
<td></td>
<td>RTI engagement completed</td>
</tr>
<tr>
<td></td>
<td>HSSS engagement completed</td>
</tr>
<tr>
<td></td>
<td>Discussions with potential licensees underway</td>
</tr>
</tbody>
</table>
CIRI has

Led significant efforts to enhance education and workforce development for the Homeland Enterprise
Examples

• Federal Law Enforcement Training Center (FLETC)
  • Researched requirements
  • Delivered recommendations for next-generation law enforcement education and training infrastructure
• Cybersecurity and Infrastructure Security Agency (CISA)
  • Completed research and developed requirements for a nationwide cybersecurity education and training network
  • Completed research and developed scalable cybersecurity curricula
    • 17 courses (credit-bearing and non-credit professional development)
    • 136 discreet training modules (“stackable”, for repurposing)
    • Cybersecurity fundamentals through advanced topics (ICS cybersecurity)
We’re looking forward to showing you examples of current accomplishments over the course of the next two days
Networking break

15-minutes
Annual Meeting: Assessment and Measurement of Port Disruptions

Gabriel A. Weaver, Lavanya Marla
University of Illinois Urbana-Champaign
The Problem

Our nation’s economy and national security are highly dependent upon the Maritime Transportation System (MTS).

- **Nationally**: The MTS accounted for more than $4.6 trillion of economic activity (1/4 of US GDP in 2014, 2019).
- **Globally**: The MTS accounts for more than 80% of global merchandise trade in volume and 67% of its value.

To handle ever-increasing shipping volumes maritime ports have become highly automated
- Heavily reliant on information and communications technology
- “Between 2022 and 2027, the global smart ports market is projected to increase from $1.9 billion to $5.7 billion. Throughout this process the sector will need to attend to the associated threats to security in the use of IT.” [UNCTAD 2022]

Maritime ports are at risk of disruption from cyber attacks and natural disasters
- Superstorm Sandy
- NotPetya, etc.

**How to enhance the security and resilience of maritime ports?**

**Our Contribution**: The CIRI Port Disruptions Tool (PDT) enables data-informed decision making regarding risk mitigation and management. Agile and resilient logistics.
What Will Success Look Like?

Via the Port Disruptions Tool (PDT), customers will:

- Employ data-driven analyses to manage emerging risks and their relevance/impact within their specific operational contexts.
- Use those analyses to more efficiently plan and prioritize risk mitigation activities.
- Continually estimate seasonal, economic impacts of disruptions within the MTS.
- Proactively identify bottlenecks and single points of failure from adopting new technologies to drive efficiencies.
- Easily share data and analyses with other stakeholders in the intermodal ecosystem to coordinate mitigation and response.

<table>
<thead>
<tr>
<th>Year</th>
<th>Date</th>
<th>Event/ Article Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>March</td>
<td>Suez Canal Obstruction</td>
</tr>
<tr>
<td></td>
<td>July</td>
<td>&quot;Supply-Chain Backlogs Turn Chicago into New Chokepoint&quot; [Wall Street Journal]</td>
</tr>
<tr>
<td></td>
<td>October</td>
<td>&quot;America's Jammed-Up Ports Need Help&quot; [Washington Post]</td>
</tr>
<tr>
<td>2022</td>
<td>July</td>
<td>&quot;Record container ship traffic jam as backlog continues to build&quot; [FreightWaves]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Russia strikes Ukraine's Black Sea port of Odesa hours after grain deals signed&quot; [NPR]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber attacks on the Port of Los Angeles have doubled since pandemic [BBC]</td>
</tr>
<tr>
<td></td>
<td>September</td>
<td>&quot;Freight train worker strike could cause massive supply chain crisis as well as halt commuter trains&quot; [CBS News]</td>
</tr>
<tr>
<td></td>
<td>December</td>
<td>&quot;Senate passes legislation to avert nationwide rail strike&quot; [Axios]</td>
</tr>
</tbody>
</table>
Benefits to Users

• Enhanced, data-driven risk management for owners and operators of ports and shipping companies.
• Ability to quantify the risks and benefits of integrating emerging technologies into their long-term strategic planning.
• Re-prioritize infrastructure assets *continually* due to an evolving natural and adversarial landscape.
• Ability to quantify the financial impact of historically-attested disruptions within the context of their shipping ports or region.
• More efficient responses to local and regional disruptions to commodity flows.
• Reduced losses from disruptions when they do occur.
Benefits to HSE

• National Economy:
  • More efficient, more resilient maritime-dependent supply chains
  • Reduced economic losses from disruptions at maritime ports

• US Coast Guard
  • Assess a broader range of types of disruptions across the maritime stakeholder ecosystem, including cyber.
  • Prioritize potential targets relative to evolving threat intelligence that may exploit dependencies vital to critical functions.
  • Reduce the time spent by Port Security Analysts to model risk.
  • Data-driven approach to injects for Area Maritime Security Exercises, in particular the cybersecurity committee.

• National Defense and Security
  • More efficient, more resilient strategic maritime ports.
  • Integration of real-time data sources within the PDT can provide more timely, more accurate data to planners to better estimate evolving DoD capacity needs.
  • Improved readiness of strategic maritime ports to support force projection missions.
Technology Transition Accomplishments

- Fall 2020: Army Cyber Institute (ACI) Jack Voltaic v 3.0 Exercise Ports Table Exercise Coordinator and Fort to Port Analyses Report
- Summer 2021: National NSF I-Corps Summer Cohort Participant at NERIN (100 interviews). Invited panelist on DHS CoE Workshop on Suez Canal Incident.
- Winter 2021/22: RTI International Technology Screening
- Summer 2022: Homeland Security Startup Studio (HSSS) Cohort Participant and formation of Koru Ports
- Fall 2022: Invited Speaker to NDTA Fall Meeting’s Transportation Academy
- Winter 2022/23: Participant in British Telecom (BT) Regional Security Summit. UIUC Office of Technology Management (OTM) to resubmit Patent Application
Activities Remaining

• Continue to engage with customers and potential licensing partners to develop opportunities for CRADAs and funded pilots.
  • Improve usability via PDT Model Builder (Deliverable 1.1)
  • Address requirement gaps opportunistically with customer engagement to access data and work toward funded pilot (Deliverable 1.2)
• Entity formation to maintain and license PDT IP.
Annual Review: Multi-Layer Cyber-Physical Supply Chain Risk Analysis for Improving the Resilience of IoT-Enabled Critical Infrastructures

Junaid Farooq
University of Michigan
Dearborn, MI

Dec. 06, 2022
Arlington, VA
The Problem

- IoT / ICT systems comprise of an interconnection of multiple hardware and software components.
- Multiple entry points for vendor involvement in system safety and reliability.

- DHS Component: CISA NRMC
- Challenge Area: ICT Supply Chain Risk Management (SCRM)
The Problem

Challenge:
- Supply chain risk is non-linear
- Overall risk from the supply chain is convoluted
- Difficult to identify vendors that are most critical

Our Approach:
- Analyze systemic risk as opposed to vendor risk
- Consider a composition of the component network and supplier network
- Decision support for vendor selection, onboarding, and upgradation
What Will Success Look Like?

**IoT Supply Chain Risk Analysis & Mitigation** (iSCRAM) software tool can:

- Ingest a schematic of components, system interconnects, and vendors
- Assess vendors based on cybersecurity standards
- Provide a holistic understanding of system risk from the supply chain

Integrated Risk Assessment

Identify critical vendors and components

Risk Optimized Vendor Selection
What Will Success Look Like?

• Easy to use software tool that can be used by end users to make supply chain risk assessments

• Beta testing and commercial launch of the tool

• Metrics for Success:
  • Number of use cases / application scenarios
  • Testing and validation on actual customer data
  • Number of initial adopters
Benefits

- Analyze Systemic Risk Posture
  - Compute Systemic Risk Score and Rank Vendors / Components

- Prioritize Security Resources
  - Recommendations for Improvement of Vendor Risk

- Enhanced Visibility of Supply Chain Risk
  - Identify Vulnerabilities and track down risk sources
Benefits

Potential End-Users:

• **Mass Transit:** Ensuring that organizations such as MTA are aware of the risk by using equipment from third party vendors

• **Automotive Sector:** Understanding the risk in autonomous vehicles from supply chain actors

• **Cyber Insurance:** Decide insurance premiums and scrutinize vendors based on cyber risk of the supply chain

Source: Adapted from the paper J. Goikoetxea, “Shift2Rail CONNECTA: The Next Generation of the Train Control and Monitoring System”, in Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Figure: Components and vendors involved in a rail car of the mass transit system.

Supply chain of new Denver regional commuter rail

Source: Adapted from the paper J. Goikoetxea, “Shift2Rail CONNECTA: The Next Generation of the Train Control and Monitoring System”, in Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Figure: Components and vendors involved in a rail car of the mass transit system.
Accomplishments (Technical)

- Development of iSCRAM Backend and Frontend software
- Web Deployment and Access Management
- Publication and Dissemination
  - 3 research articles and 1 book
- Hands–on tutorial at IEEE MILCOM 2022
Product

System Schematic

Ranking of Vendors

System Risk Ratings

Ranking of Components

Available: www.i-scram.com
Product

Main Dashboard

Risk Summary and Statistics

* Proprietary Copyright Software

Available: www.i-scram.com

Risk-Centric Vendor Selection

Vendor Selection
Accomplishments (Commercial)

• Approx. 20 end-user interviews, 3 NDA signed

• Selected for DHS sponsored commercialization assessment through RTI Innovation Advisors

• Awarded MTRAC Advanced Transportation grant at University of Michigan funded by Michigan Economic Development Corporation

• Contacts Initiated with BlockHarbor Cybersecurity, Lear Corp., and Resilience Insurance
Activities Remaining

• Beta Testing Partnership
  • NDAs have been signed
  • Testing and validation

• Licensing / Incorporation

• Sustainability: SBIR / STTR / Venture Capital
Thank You!

Contact: mjfarooq@umich.edu

Follow Us: www.i-scram.com
LUNCH BREAK
We will resume at 1:00 pm
Annual Review:

*Enhancing Water Distribution Networks Resilience with Scalable AI-based Planning*

Bistra Dilkina
University of Southern California
The Problem

• In US, average age of a current water pipelines is **45 years old**; 
  **C- on Infrastructure Report Card** from the American Society of Civil Engineers

• **143 million Americans** live in areas vulnerable to earthquakes
  • Earthquakes disrupt critical infrastructures, and specifically water infrastructure.
  • Water Service Disruption compromises public access to water and reduces effectiveness of disaster response (fire departments, hospitals, disaster recovery centers)

• **Critical water customers**
  • hospitals, fire/police stations, emergency evacuation centers, power, sanitation, etc need resilient water supply to provide life-saving services during and post disasters.

• Relevant DHS Components: FEMA, USCG among others

• Proposed solution: data-driven AI-based decision support for water infrastructure mitigation planning to inform strategic infrastructure network fortification before the disaster strikes

M 7.8 earthquake on San Andreas Fault, CA could cause **$24 billion in business interruption losses due to water supply interruption alone** (>13% of the total estimated costs)
What Will Success Look Like?

• Develop decision-support tool to strategically target infrastructure upgrades in water distribution networks
  • enable for the first time capability to (automatically) generate optimized service-zone-scale master plans for disaster-resilience mitigation planning
  • to meet the resiliency requirements of the local communities
  • data-driven and cost-effective by design

• Modular, usable, robust software tool

• Transition of our approach/tool to be incorporated with existing data platforms and planning workflows used by a spectrum of end-users
Benefits to end-users

• Los Angeles Department of Water and Power
  473 square miles, over 4 million residents, 733,900 active service connections
  • 23% of 2,742 critical customers at earthquake risk
  • 34% of 267,084 total pipes at earthquake risk
  • Pilot program using hand calculations – slow

• Provide owners and operators of water infrastructure with data-driven hazard assessment and cost-effective planning tool
  • **Hazard assessment**: in addition to pipes, which critical customers are at risk?
  • **Automated planning**: coordinated upgrades across the network wrt joint needs and costs
  • **Faster speed** at developing mitigation plans
  • Ability to plan on a **larger scale** (thousands of pipes, 10s of sq miles)
  • More **cost-effective** plans by using algorithms to search for optimal upgrades
  • Agility to **re-calculate, re-optimize, what-if analysis**

Action 61: Advance seismic safety, prioritizing the most vulnerable buildings, infrastructure, and systems

“Expand Seismic Resilient Pipe Network
The City will expand development of the seismic resilient pipe network. ... Resilient pipeline planning, design, and construction requires the development of new informational tools and mapping of geohazards ....”
Benefits to DHS

• Enhances the ability of local and state decision makers across the nation to perform mitigation planning
  • Enhances resilience by minimizing likely disaster disruptions
• Ways to show cost-effectiveness of planning – FEMA grant applications
• Help Disaster Response
  • Services critical to disaster response (hospitals, evacuation centers, fire/police departments) less likely to be compromised by water disruption
• Public Health and Damages
  • minimizes risks to public health and property damage (fire, water) through increased availability of water during earthquakes
Accomplishments

- **Flexible tool to aid in resiliency planning**
  - Highly parametrized: definition of hazards, costs, resilience needs

- **Map risk exposure**: hazard, infrastructure and customers

- **Master Plan**
  - Identify set of pipes that minimize costs to meet all resilience requirements
  - Showed NP-hard, developed **Mathematical Model**
  - **6%-23% more cost effective than baseline approach**
  - Scales to 1-3 service zones at a time

- **Sequential Planning** subject to yearly budget
  - Year by year pipes to be replaced that maximize resilience benefits as early as possible
  - **Dynamic Programming approach (optimal)**
  - Cost benefit analysis with various replacement budgets (miles/year) to quantify opportunity cost

- **Stakeholder engagement and requirement elicitation**
  - Los Angeles DWP, Seattle Public Utilities, East Bay Municipal Utility District (EBMUD)
  - Metropolitan Water District of Southern California, FEMA IX
  - C A Davis Engineering, Kubota Membrane USA

- **RTI Screening assessment completed**
Activities Remaining

- **Package** into a standalone tool with robust error checking, compatibility and documentation – improve usability
- **Pilot in-house training** and usage at LADWP with 5-10 engineers on site
- Address **requirements gaps** and design based on pilot feedback
- Continue to **engage with customers** and potential partners
- Explore pathways forward (funding, piloting, IP)
Technology Transition Project: Cyber Secure Dashboard

Glen Salo
Heartland Science and Technology Group
The Problem

• The prevailing cyber risk management processes (in government and the private sector) are inconsistent, opaque, and insufficient

• The prevailing practices...
  • Impede our progress towards enhancing the security and resilience of our critical infrastructure
  • Lead to continued year-over-year financial losses
  • Are inadequate to address national security threats by nation-state actors

Federal Bureau of Investigation Internet Crime Report 2021
The Solution

• Technology solutions are necessary but insufficient
• Increased emphasis on people and process is required
• **Solution**: A standards-based assessment, monitoring, management, and reporting tool
• **DHS Components**: CISA, TSA, USCG
What Will Success Look Like?

- Owners and operators of critical infrastructure will adopt and conform to national cybersecurity standards, processes, and best practices
  - DHS (CISA) Cyber Security Performance Goals, NIST CSF, the DoD CMMC, ...
- Standardized assessment methodologies will measure conformance
  - NIST SP 800-171A, NIST SP 800-53A, NIST 162 Handbook, etc.
What Will Success Look Like (cont’d)?

- Conformance will be measured for individual organization and entire supply chains
- Continuous improvement will be facilitated, monitored, reported
Benefits (to the user)

• Eases, accelerates, **lowers cost** of conformance to national standards
• **Operationalizes** standardized cyber management processes/practices
• **Harmonizes** internal and external (out-sourced) cybersecurity activities
• **Continuous visibility** of progress toward target posture
• Eases internal/external **stakeholder reporting**
• Supports individual organization and extended **supply chains**
Benefits (to homeland security enterprise)

• Facilitates **broad-scale adoption** of national standards & best practices

• Provides **common metrics/criteria** for assessing & reporting progress

• Provides a **common language/lexicon** for all stakeholders

• Facilitates **sound governance** and **policy** implementation

• Facilitates “ripple effect” as standards are enhanced/updated

• **Enhances the security and resilience** of our critical infrastructure
Accomplishments

• Software developed, tested, and available as a **SaaS offering**
  • Learn-by-doing, policies, standards-based assessment, monitoring
  • Plan of Action & Milestones (cybersecurity task management/harmonization)
  • Provides a pathway for continuous improvement and progress reporting

• Six cybersecurity standards
  • NIST CSF, MP, RBO, PSAP, CMMC, 171

• Four standards-based assessment methodologies
  • 171A, 53/53A, 162 Handbook

• Supply chain status aggregation/visibility
Activities Remaining

• Integrate with Cyber Talent Bridge
  • NIST NICE-based workforce management
  • Alignment of knowledge/skills to cybersecurity task assignment
  • Identify & mitigate skills and/or training gaps

• Integrate DHS CISA CPG

• Integrate Trustmark framework (federated ICAM)
  • Emergency response, law enforcement, other sensitive communities

• Deploy with government approved containers

• Integrate education and training
Annual Review: CyberTalent Bridge

Anderson Wiese

2wav
The Problem

What capabilities do I need?

Cynthia Jefferson
Incoming CISO
SME Manufacturing

Who in my talent pool has these capabilities?

What missing skills do I need to develop or recruit?
What will success look like?

Cybersecurity teams use CTB with CSD to manage compliance and workforce development.

CyberTalent Passports share skills-based capability statements.

- **JOB POSITIONS**
  - Information System Architect | A |
  - February 2021-present
  - Mega Internet Company

- **CERTIFICATIONS**
  - Certified Information Systems Security Professional (CISSP) | A |
  - January 2020

- **WORK RULES**
- **COMPETENCIES**
- **COURSES**
- **EXPERIENCES**
- **RECOMMENDATIONS**
Benefits

Tasking
Requirements to recommendations

Workforce
Assessment, development, recruiting

Sharable Passports
Encourage cooperation and integration

Frameworks
Connect cybersecurity frameworks
Accomplishments

CyberTalent Bridge works!

CTB is the first workforce tool engineered from the ground up in terms of the NICE Framework.

Bridges between isolated frameworks.

Realizes portable, sharable CyberTalent Passports

Evaluates talent capability by inference and confidence.
Activities Remaining

Commercial release integrated with Cyber Secure Dashboard.

CyberTalent Passport public release.

Optimize for scale.

Enhancements for potential industry partners:
Training agencies, community colleges, universities
Recruiters
Insurers
Annual Review: NG9-1-1
Interoperability Testing Program - Projects 2A & 2B

Walt Magnusen, Ph.D.
Texas A&M University
Internet2 Technology Evaluation Center
The Problem

• Statement of the problem:
  • The United States has identified the 911 system as critical infrastructure. While a $15 billion national transition to NG 911 is occurring we currently have no way of ensuring interoperability of sub-systems.
  • DHS CISA has the lead responsibility in interoperability for critical infrastructure. They are working with the US DoT NG-911 office, the FCCs Public Safety Bureau, the National Emergency Number Association (NENA) and others.

• How are you approaching it, and what makes your approach unique?
  • We have created a Stakeholders group that will provide guidance on the Governance of, Technology used and Financial model of a DHS NG-911 Interoperability Certification process. The stakeholders group includes DHS, DoT, FCC, NIST, State Agencies, Industry Associations and Academia. It also includes international participation.
What Will Success Look Like?

• Success will include;
  • A conformance testing system that is in the public domain encouraging more testing facilities,
  • At least one test facility that operates under a sustainable model,
  • All jurisdictions procuring NG-911 components requiring DHS Certification,
  • Overwhelming acceptance by all stakeholders,
  • An ecosystem that is standards conformant and interoperable
Benefits

• How will success benefit the Homeland Security Enterprise?
  • The initial promises of NG-911 included;
    • Additional capabilities for emergency callers (video, text, additional data)
    • Lower costs through additional competition, the use of off the shelf hardware and the acceptance of standards
    • Higher reliability thru call redirecting, diverse routing and network-to-network interconnection.
  • None of these promises can be realized unless the underlying NG-911 subsystems are interoperable.
Accomplishments

• Phase 2a
  • Document 10 call scenarios for end-to-end testing (7 of 10 complete).
  • Install and document first complete ESInet with required NGCS functional elements.
  • Test call conformance through ESInet working with Verizon for call ingress.

• Phase 2b
  • Establish stakeholders group membership and structure and schedule first full member face-to-face meeting.
  • Initiate contract with consultant for ISO 17025 conformance.
Activities Remaining

• Phase 2a
  • Complete second i3 ESInet and PSAP for end-to-end testing.

• Phase 2b
  • Hold stakeholders face-to-face meeting (2 March)
  • Produce outreach video
  • Complete and document ISO 17025 Certification for TAMU ITEC
  • Validate end-to-end testing model
  • Document operational cost model
Annual Review: EMP Risk Assessment and Mitigation Prioritization

Jose Schutt-Aine, Glen Salo, Daniel Shaw, Aosheng Rong, Victoria Shao
University of Illinois, Synclesis, Inc.
5G Infrastructure Resilience

• Electromagnetic Pulse (EMP) attacks have the potential to disrupt and damage electronics throughout our nation’s critical infrastructure, posing a serious risk to that infrastructure. Assessing the risk of such events is extremely challenging due to the complexity of our systems.

• This project addressed the threat of EMP to our nation’s critical infrastructure, which includes our nation’s power grid and mobile communication systems.
Our Approach

• Use uncertainty and randomness as a means of tackling and overcoming complexity for the purpose of mitigation.

• This approach differs fundamentally from traditional methods that cannot account for the multi-scale material and geometry complexity and the variabilities and uncertainties inherently present in the EMP problem due to the computational complexities.

• Our goals included both developing this capability and using it to assess EMP effects on the electronics in a 5G communications tower.
Objectives

- Ability to quickly assess and predict impact of an EMP attack on 5G infrastructure
- Ability to help preemptively mitigate effects of such attacks via Characterization, Validation, Simulation & Mitigation

Benefits & Potential Impact

- Critical to CISA
- Accurate risk assessment of EMP attack
- Help increase resilience to EMP attack
- Facilitate mitigation measures
5G Infrastructure
Hybrid Cable & Surge Protection Devices

The internal structure of a hybrid cable
Hybrid Cable

• Since fiber-optic cable uses light, not electricity, to propagate signals, it does not carry power to remote radios. A power cable must be added to provide the power to these devices: ➔ hybrid cable contains both types in a single sheath.
EMP Waveform

- **Initial Focus on E1 Pulse:**
  - \( V = E_0 k (e^{-at} - e^{-bt}) \), where
  - \( E_0 = 50kV \),
  - \( k = 1.3 \),
  - \( a = 4e7 \), and
  - \( b = 6e8 \)

E1-EMP: 50kV/m - 400MHz
E2-EMP: 0.1kV/m - 100kHz-1MHz
E3-EMP: 10V/m - < 1Hz
Cellular Tower EMP Model Flow

EMP Source (EMP E1 Pulse) → FFT (convert Pulse to frequency domain) → Electromagnetic Solver (SENTRi/HFSS) → Surface Fields on Cable → Compute Cable Coupling Model → LIM to produce final waveform

Cable runs from just below top of tower down to outside of the base station.
Accomplishments

• Extraction of Hybrid cable parameters as a function of frequency (code)
• Transient simulation of hybrid cable (code)
• Implement TVS device into simulator
• Implement MOV device into simulator
• Preliminary stochastic analysis of system
Transient Voltage Suppressors (TVS)
## Modeling MOVs

### Nonlinear Resistors

The circuit diagram shows two nonlinear resistors, labeled A0 and A1, each with their own characteristics.

### Table A0

<table>
<thead>
<tr>
<th>I(kA)</th>
<th>V(pu)</th>
<th>V(kV)</th>
<th>Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>1.40</td>
<td>217.0</td>
<td>21.7 kohms</td>
</tr>
<tr>
<td>0.1</td>
<td>1.54</td>
<td>238.7</td>
<td>2.38 kohms</td>
</tr>
<tr>
<td>1</td>
<td>1.68</td>
<td>260.4</td>
<td>134 ohms</td>
</tr>
<tr>
<td>2</td>
<td>1.74</td>
<td>269.7</td>
<td>69.75 ohms</td>
</tr>
<tr>
<td>4</td>
<td>1.80</td>
<td>279.0</td>
<td>47.01 ohms</td>
</tr>
<tr>
<td>6</td>
<td>1.82</td>
<td>282.1</td>
<td>36.23 ohms</td>
</tr>
<tr>
<td>8</td>
<td>1.87</td>
<td>289.9</td>
<td>29.45 ohms</td>
</tr>
<tr>
<td>10</td>
<td>1.90</td>
<td>294.5</td>
<td>24.91 ohms</td>
</tr>
<tr>
<td>12</td>
<td>1.93</td>
<td>299.1</td>
<td>21.78 ohms</td>
</tr>
<tr>
<td>14</td>
<td>1.97</td>
<td>305.3</td>
<td>19.37 ohms</td>
</tr>
<tr>
<td>16</td>
<td>2.00</td>
<td>310.0</td>
<td>17.65 ohms</td>
</tr>
<tr>
<td>18</td>
<td>2.05</td>
<td>317.7</td>
<td>16 ohms</td>
</tr>
<tr>
<td>20</td>
<td>2.10</td>
<td>325.5</td>
<td></td>
</tr>
</tbody>
</table>

### Table A1

<table>
<thead>
<tr>
<th>I(kA)</th>
<th>V(pu)</th>
<th>V(kV)</th>
<th>Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>1.23</td>
<td>190.5</td>
<td>1.9 kohms</td>
</tr>
<tr>
<td>1</td>
<td>1.36</td>
<td>210.80</td>
<td>210 ohms</td>
</tr>
<tr>
<td>2</td>
<td>1.43</td>
<td>221.65</td>
<td>110.8 ohms</td>
</tr>
<tr>
<td>4</td>
<td>1.48</td>
<td>229.40</td>
<td>57.35 ohms</td>
</tr>
<tr>
<td>6</td>
<td>1.50</td>
<td>232.50</td>
<td>38.75 ohms</td>
</tr>
<tr>
<td>8</td>
<td>1.53</td>
<td>237.15</td>
<td>29.64 ohms</td>
</tr>
<tr>
<td>10</td>
<td>1.55</td>
<td>240.25</td>
<td>24.025 ohms</td>
</tr>
<tr>
<td>12</td>
<td>1.56</td>
<td>241.85</td>
<td>20.1 ohms</td>
</tr>
<tr>
<td>14</td>
<td>1.58</td>
<td>244.95</td>
<td>17.49 ohms</td>
</tr>
<tr>
<td>16</td>
<td>1.59</td>
<td>246.45</td>
<td>15.4 ohms</td>
</tr>
<tr>
<td>18</td>
<td>1.60</td>
<td>248.00</td>
<td>13.777 ohms</td>
</tr>
<tr>
<td>20</td>
<td>1.61</td>
<td>249.55</td>
<td>12.47 ohms</td>
</tr>
</tbody>
</table>

The parameters for the nonlinear resistors are:

- \( L_0 = 0.00029 \, mH \)
- \( C = 6.9E-5 \, \mu F \)
- \( L_1 = 0.02175 \, mH \)

The circuit includes a transformer labeled \( R_1 \) with several ohm values, indicating the variability in impedance.
LIM Simulator

The LIM platform is optimal for accurate simulation of signals in hybrid cable.

Features
- Rapid transient analysis
- Transistor-level simulations
- Frequency-dependent components
- Fast transmission-line analysis
- Large netlists
- Time step control
- Tunable accuracy and speed
- Chip, package or board

Applications
- Power Delivery Networks
- IR Drop Analysis
- Analog/Mixed Signal Simulation
- Macromodel Analysis
- IC Verification
- High-Speed Link Design
LIM Results

Hybrid Cable – No Suppression

Hybrid Cable – With Suppression
High-Speed Link Simulation
Initial Stochastic Results

• Varied Incident Angle of EMP
  • \( \Theta \) and \( \phi \)

• Evaluated at stochastic collocation points on sparse grid
  • Final Metric: Signal Eye Width

• Adjusted shielding level
  • 5dB, 10db and 20dB

• Created interpolant function from results and generated probability distribution function

\[ \Theta_{\text{pol}} \]

\[ \phi_{\text{pol}} \]
Activities Remaining

• Validation & model enhancement of hybrid cable, arresters
• Behavioral modeling of PCB
• Refine EM coupling solution for surface currents
• Mitigation study via stochastic analysis ➔ LIM Enhancement
Hybrid Cable Model Validation

• Measure Cable S Parameters (VNA)
• Optimize with field solver
• Assess frequency dependence
• Perform iteration
PCB Modeling

- Identify points of entry (e.g. PDN)
- Reduce complexity via behavioral modeling
- Macromodels via MOR
- IBIS model implementation
- X parameters
Accurate Computation of the Surface Currents on Hybrid Cable over Lossy Ground Illuminated by EMP Waves

• Motivation
  • Hybrid cables with lean to an 5G RF tower is a multi-scale geometry. Finite element approximation of multi-scale geometries are prone to ill-conditioning over EMP frequency spectra range. Numerical experiments show that US Government code SENTRi and ANSYS’ HFSS break down at EMP frequencies.

• Proposal and Implementation
  • We are developing a customized code that utilizes the mixed potential integral equation together with graph-based loop-tree decomposition technique, for the accurate computation of the external currents on the shielding conductor of the hybrid cables under EMP excitation at the whole EMP spectra range.
  • Lossy ground effects will be included.
Summary

- Proof of concept established
- Electromagnetic extraction and circuit simulation are key components
- FEM field solver
- LIM simulation engine
- Validation & refining of model will provide robust tool for mitigation
Annual Review:
Protecting the nation’s 911 system from cyber threats - Present and Future

Karthik Balasubramanian
Karthik Consulting, LLC
The Problem

• The US 911 system (Public Safety Answering Point (PSAP)) is an essential part of the critical infrastructure of the United States, that spans several National Critical Functions, and needs to be protected from cyber-attacks.

• CISA Emergency Communications Division (ECD) and the Emergency Public Safety Sector and more specifically PSAPs across the nation are intended to be the primary beneficiaries of this project

• Propose criteria for categorizing and developing a curated “PSAP Profile”, using the NIST SP 800-53A controls and Cyber Security Framework (CSF) to measure and track the cybersecurity posture of PSAPs.

• Conduct consultative PSAP profile based “pilot” assessments of PSAPs
What Will Success Look Like?

• Following the CSF, conduct research and publish a curated list of tailored NIST SP 800-53A controls for measuring and monitoring the security posture and cybersecurity maturity of PSAPs

• Implement the PSAP Profile in the Cybersecure Dashboard (CSD) tool

• Conduct PSAP Profile based “pilot” assessments

• Understand the unique requirements of PSAPs migrating to NG911 and update the PSAP Profile, as necessary
Benefits

• As the PSAP threat landscape rapidly changes so does the urgency to secure and improve this critical infrastructure. This project addresses the Goals and Objectives identified in the CISA Strategic Intent document (published in August 2019) by proposing to enhance the current and ongoing security and resilience of the PSAP ecosystem.

• Create a more secure nation-wide PSAP system through the PSAP Profile and mapped cybersecurity controls.

• The 6000+ PSAPs and the 1000+ federal/DoD PSAPs can benefit from the PSAP Profile to help understand and track their cybersecurity posture and risks.
Accomplishments

• Phase 1 research of PSAPs completed and final report published
• PSAP Profile published and approved by CIRI/CISA/DHS S&T
• PSAP profile implemented in the Cybersecure Dashboard tool
• PSAP Profile based “Pilot” assessments completed
• Phase 2, further research to understand the unique requirements of PSAPs migrating to NG911 completed
Activities Remaining

• Analyze the results from the Phase 2 research of PSAPs migrating to NG911
• Update the PSAP Profile, as needed, to support NG911 type PSAPs
• Publish the final report
• Publish the updated PSAP Profile curated list of NIST SP800-53A controls
Networking break

15-minutes
Annual Review: Cybersecurity Education & Workforce Development

Casey W. O’Brien, UIUC
December 6, 2022
A Two-Phase Project

- **Phase 1**: Developing a National Needs Analysis and Strategy: 2020-2021
- **Phase 2**: Curriculum Development: 2021-2022
PHASE 1
Hub & Spoke Project

- “Research and Deliverables on Utilizing an Academic Hub and Spoke Model to Create a National Network of Cybersecurity Institutes”
- 3 partners, plus a network of 2/4-year schools (Hubs and Spokes)
- Emphasis on underserved populations
- IR and ICS security-related education and training
Hub & Spoke Project Deliverables

- Auburn: Incident Response Curriculum Guidance Document
- Purdue: Industrial Control Systems Curriculum Guidance Document
- Tulsa: Spoke School Guidance Document
Principal Findings from Phase 1

- Demographic imbalances in access to cybersecurity education and training
- Failure of existing education and training to provide employers clear competency outcome information
- Weakness in education and training for “post-boom” cybersecurity capacity
Recommendations for a Phase 2

- Curriculum development that provides multiple pathways
- Practical learning experiences with demonstrated, employer-recognizable performance outcomes (e.g., context mapped to a work role’s tasks)
- Flexible, modular architecture for incremental accredited learning progression (e.g., training > college/degree)
PHASE 2
Curriculum Development Project

- “Development of a Robust, Nationally Accessible Cybersecurity Risk Management Curriculum for Technical and Managerial Cybersecurity Professionals”
- 5 partners
- Hybrid curriculum model
Curriculum Development Project: Learning Principles & Processes

- **Dialogical**: Learners respond to content inputs (lecture videos, readings, links) via discussions and select response surveys
- **Collaborative**: Projects and labs involve peer review
- **Knowledge co-constructed by learners**: Learners research topics, make posts, and comment on each others’ posts
- **Advanced Learning Analytics**: Embedded formative assessments, mastery learning
Applying a Signature Orientation

Cyber
(technical)

Social
(human)

Cyber-social
Delivering a Stackable Program Architecture

- **Curriculum**
  - (Pre-Req, Foundational, Technical, Managerial)
  - Assembling courses into programs with varying durations and foci

- **Courses**
  - The equivalent of 3-4 credit hours each

- **Topics**
  - Can be stand-alone training modules

- **Core Concepts**
  - Aligned with NICE, performance outcomes, workplace roles & tasks

Flexibility to serve diverse populations and needs
Providing Alternatives Pathways

Pre-Requisite Curriculum
(divided into courses, 3-4 credit hours each)

Foundational Curriculum
(divided into courses, 3-4 credit hours each)

Technical Curriculum
(divided into courses, 3-4 credit hours each)

Managerial Curriculum
(divided into courses, 3-4 credit hours each)
Hybrid Curriculum

Pre-Req Curriculum
(divided into courses, 3-4 credit hours each)

Course 1: Foundations in Computing

Course 2: Foundations in Information Technology

The Pre-Requisite Curriculum is comprised of these 2 courses
The Foundational Curriculum is comprised of these 3 courses:

- **Course 1**: Foundations in Secure Networking for Cyber-Social Systems
- **Course 2**: Foundations in Secure Administration of Cyber-Social Systems
- **Course 3**: Foundational Technical and Organizational Concepts and Practices in Cybersecurity
Hybrid Curriculum

Technical Curriculum
(divided into courses, 3-4 credit hours each)

Course 1: Critical Infrastructure Security
Course 2: Incident Response Management
Course 3: Cyber Fundamentals

Course 4: Technical Processes for Software Security Engineering

Course 5: Applied Cryptography
Course 6: Cyber Incident Management
Course 7: Reverse Engineering
Course 8: Ethical Hacking
Course 9: Secure Software Construction

The Technical Curriculum is comprised of these 9 courses
Hybrid Curriculum

Managerial Curriculum
(divided into courses, 3-4 credit hours each)

Course 1: Cyber Ethics
Course 2: Cybersecurity for Educational Leaders

Wilkes University

Course 3: Management Processes for Software Security Engineering

The Managerial Curriculum is comprised of these 3 courses
Curriculum Development Project Deliverables

- Author Guide, Framework Mappings (NICE), Curriculum Development Lifecycle Recommendations
- 17 courses (136 training modules), with...
  - curriculum resources: Video lectures, hands-on activities, assessments, etc.
- Flexibly designed for both in-person and online delivery
Recommendations for a Phase 3

- Implementation, pilot & dissemination of Phase 2 courses/content
- Curriculum sharing architecture & platform for delivery and dissemination of the course materials via a common infrastructure, **CyberEd Bridge**
- Chunking of course content into training module (136)
What’s Next?
Grow the CIRI National Network

- Support both the management and running of the national Hub & Spoke network, as well as the curation and delivery of the curricula developed
Implement Partner Education & Training Program

- Executive Summary:
  - Creating cutting-edge education, training delivery systems, and content that results in a diverse pool of talent with skills needed to protect organizations and improve national security
Problem Statement:

- Organizations struggle to find, develop, and retain desperately needed talent (e.g., Cybersecurity)
- Aging workforce of highly-skilled and experienced workers
- Attracting new and more diverse talent pools
- Closing gaps in workers' skills and credentials
Implement Partner Education & Training Program

- **Problem Statement (con’t):**
  - Investing in talent that can keep pace with the latest industry advances
  - Implementing workforce training models that effectively develop and "up-skill"
Implements Partner Education & Training Program

- **Problem Statement (con’t):**
  - Current commercial training/offerings:
    - Focus on tip of the spear/specialists, in short supply
    - Don’t leverage Learning Science or evidence-based practices
    - One-size does not fit all
Implement Partner Education & Training Program

- Includes an interconnected set of solutions to meet employment needs:
  - *What are the populations being served?*
  - *What are these interconnected set of solutions?*
  - *What differentiates our solution from others in the marketplace?*
Implement Partner Education & Training Program

- **Populations Served:**
  - IT workers looking to transition into in-demand and hard to fill work roles (e.g., Cybersecurity) - 7 million IT workers in U.S.
  - Industrial Control Systems asset owners and operators
  - 911 call center operators
Implement Partner Education & Training Program

- **Additional Learner Populations:**
  - Career changers
  - Chief Human Information Capital Officers (CHICOs), HR
  - Underrepresented populations
  - Degree/certificate-seeking students
Implement Partner Education & Training Program

- **Employer Partners:**
  - Federal, State, Local, Tribal and Territorial government entities
  - K-12 and higher education
  - Regional technology councils
  - Professional & technology services
  - Non-profit organizations
Implement Partner Education & Training Program

- **Differentiators:** Cyber-Social:
  - Captures the relationship between computers (or computerized machinery) and their users
  - Technical + Human (Social) + Organizational
Implement Partner Education & Training Program

- **Differentiators:** Mastery-Focused:
  - *Mastery* of core concepts vs. *coverage* of 1,000s of concepts
  - Not trying to boil the ocean
Implement Partner Education & Training Program

- **Differentiators**: Blending Learning Science with Technological Advancements:
  - **Dialogical**: Learners respond to content inputs (lecture videos, readings, links) via discussions and select response surveys
Differentiators: Blending Learning Science with Technological Advancements:

- Collaborative: Projects and labs involve peer review
Implement Partner Education & Training Program

- **Differentiators**: Blending Learning Science with Technological Advancements:
  - Knowledge co-constructed by learners: Everyone researches topics and contributes content
Implement Partner Education & Training Program

- **Differentiators:** Advanced Learning Analytics:
  - Continuous assessment
  - Peer, machine, and instructor feedback
  - Formative assessments (for learning, not just of learning)
  - Incremental progress visualization - think “learning fitness tracker”
Implement Partner Education & Training Program

- **Differentiators:** Advanced Learning Analytics
Implement Partner Education & Training Program

- **Differentiators:**

  Standards-Aligned Concept Mapping
Implement Partner Education & Training Program

- **Differentiators:**
  - Course Content
  - Mapped to In-Demand Work
  - Role Tasks
Differentiators: Assessment-Driven:

- Course Readiness Assessments
- In-course diagnostic assessments
- Personalizes the learning path

<table>
<thead>
<tr>
<th>Foundational Tasks</th>
<th>Composite score</th>
<th>Comparative score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify ownership of gateway devices (16.77)</td>
<td>83.8</td>
<td>Average</td>
</tr>
<tr>
<td>Identify recon that is within project scope (15.63)</td>
<td>46.8</td>
<td>Low</td>
</tr>
<tr>
<td>Search online sources for useful information about a target (15.45)</td>
<td>53.5</td>
<td>Average</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Differentiating Tasks (with weights)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze data found on compromised machines to enable exploitation deeper into the network (24.02)</td>
<td>36.0</td>
<td>Average</td>
</tr>
<tr>
<td>Identify major assets subject to attacks (23.67)</td>
<td>87.2</td>
<td>High</td>
</tr>
<tr>
<td>Identify targets for potential exploitation (23.67)</td>
<td>56.0</td>
<td>High</td>
</tr>
<tr>
<td>Analyze data found on compromised machines for strategic value as seen by a worst case attacker (23.60)</td>
<td>26.2</td>
<td>Low</td>
</tr>
</tbody>
</table>

Overall Score

My Score | 54.9 | Average |
Implement Partner Education & Training Program

- **Differentiators: Performance-Based:**
  - Cloud-based lab platform
  - Real systems, tools
  - LTI, SSO
  - 24 x 7 support
Implement Partner Education & Training Program

- **Courses:**
  - Credit and non-credit offerings
  - Fully online, in-person, hybrid
Implement Partner Education & Training Program

- **Courses (con’t):**
  - *Foundations in Cybersecurity*: 1-2 hours
  - *NIST Cybersecurity Framework (CSF)*: 1-2 hours
  - *Cyber Secure Dashboard*: 1-2 hours
Implement Partner Education & Training Program

- **Specialized Certificates:**
  - Campus Graduate CERT in Cybersecurity
  - ITI small “c” certificate(s)
  - Multi-disciplinary: Gies, ECE, Education, iSchool
Contact Information

Casey W. O’Brien
Assistant Director, Cyber Defense Education and Training
Information Trust Institute
University of Illinois Urbana-Champaign
cwobrien@illinois.edu
+1-443-610-7775

M. Scott Sotebeer, PhD
Endicott Consulting
The Problem

• Increasing reliance and overdependence on government-supplied GPS Positioning, Navigation, and Timing (PNT) signals. 5g is the multiplier.

• Unintended vulnerabilities and “blind spots” in critical infrastructure- from commerce to transportation, the power grid, and communications.

• CISA seeks to understand and evaluate from industry, current 5g timing requirements, alternative backup sources, and issues of government supplied backup sources.

• Approach: critical team/critical knowledge.
  • Only works with carrier technology leadership; industry PNT/Timing experts; academia (unbiased/unfiltered analysis); DHS CISA/S&T partner.
What Will Success Look Like?

• A comprehensive, technical analysis of 5g timing requirements from one or more of the major carriers: T-Mobile, Verizon, AT&T.

• Identification of alternative backup timing requirements/sources.

• A comprehensive analysis of any issues/vulnerabilities with proposed government alternate timing sources: physical/technical environment, social implications, legal implications and framework, and economic requirements and implications.

• Industry and expert supported go/no-go decision framework for lab evaluation and testing of government supplied alternative timing sources.
Benefits

• Technical insight and knowledge – 5g carrier timing and backup requirements.
  • New tools for risk and vulnerability analysis – Critical Infrastructure.
  • Evaluation of carrier backup and government solution.
  • If compatible/desirable, more robust back timing alternatives shared between government and industry—accelerated redundancy and resiliency.

• Comprehensive analysis of current state of alternative timing sources: LEO, eLoran, Networks/fiber, Signals of Opportunity, etc.

• Demonstration framework for lab evaluation of government backup timing sources.
Accomplishments

Organized advisory of essential industry PNT/Timing technical and thought leaders including:

- Resilient Navigation & Timing Foundation
- Institute of Navigation: Precise Time and Time Interval Systems and Applications
- Microchip Technology
- University of Washington Computer Sciences/STEM (lab eval)
- Senior Director of Product Security, Cybersecurity Trust and Protection (CTP), T-Mobile
- President, Technology, T-Mobile
Activities Remaining

This is an 18-month project. We are focusing on critical milestones and key decision points.

**First 120 days**

- Convene working group.
- Create topical knowledge library.
- Create technical approach and analysis framework.
- Begin initial inquiry and learning process with carrier.
- Evaluate inputs and process for carrier engagement on technical timing and backup requirements.
Annual Review: BACKUP NETWORK TIMING FOR MISSION CRITICAL P25 LMR NETWORKS

Walt Magnussen, Ph.D.
Texas A&M University
Internet2 Technology Evaluation Center
The Problem

• Statement of the problem:
  
  • Many critical infrastructure systems are heavily dependent upon the Global Positioning System (GPS) system established in the 1970s for navigation. NG-911 relies on it for location in call routing, public safety communications systems require it for timing of Land Mobile Radio (LMR) and Public Safety Broadband Networks and many applications embed GPS based location services in their user interface. This GPS systems have vulnerabilities that stem from jamming, spoofing, inability to see enough of the constellation to determine an accurate location and other issues. This project does a survey of potential alternatives that could be used to mitigate these vulnerabilities.
  
  • This project has impact upon all DHS components (FEMA, Coast Guard etc.), Department of Defense, Department of Transportation, FCC and others.

• How are you approaching it, and what makes your approach unique?
  
  • We have engaged a faculty member with extensive background in PNT (Dr. Radu Stoleru) and we are leveraging the industry support that we have established over the years.
What Will Success Look Like?

• Success would be a comprehensive review of all of PNT requirements and a report documentation of the potential alternatives for Positioning, Navigation and Timing (PNT) solutions.

• A successful project would also include a recommendation for a PNT testbed that included at least two or three of the leading technologies. This recommendation would include a testbed design and projected pricing of both the testbed as well as a nation-wide implementation of recommended technologies.
Benefits

• How will success benefit the Homeland Security Enterprise?
• The results of this project should lead to recommendations that could help United States leadership make informed decisions on future investments in PNT augmentation and enhancement.
Accomplishments

• Project strategy meetings
• Determination of makeup of stakeholders group.
Activities Remaining

• Document network requirements for PNT data acquisition and distribution.
• Information gathering, data analysis and documentation of PNT alternatives.
• Provide a technology comparison matrix for the solutions researched.
• Provide recommendations for a potential Phase II testbed that would establish a PNT Testbed.
Virtualized ICS Testbed for Research, Training, and Education

CIRI Annual Meeting
December 2022
The Problem

- Industrial control systems use specialized hardware/software
- ICS workforce desperately needs **hands-on** cyber-security training
- **On-site** training does not scale
- **Cloud-based** training is not currently feasible
  - Clouds uniformize operating systems and architectures
Proposed Approach

• Make ICS testbeds work in the cloud
Key Technical Challenges

• Programs compiled for specialized processing chips don’t run natively
• Virtual machines need
  • To be embedded in virtual time
  • To be temporally correlated (so that all VMs advance in virtual time at the same rate)
Approaches

• Use instruction level emulation (e.g. QMU)
  • Working now with programmable logic controller (PLC)
• Leverage previous results to have software see ‘virtual clock’ rather than wall-clock
• Coordinate VM executions in time
Deliverables

• Prototype of working system, on models with 10 or more devices
• Performance studies of working system to identify bottlenecks and next steps
• Modules for security lab course that use prototype

Status

• Launch early 2023
• Two years duration
• Senior staff: Nicol, Levchenko, Luellen
• Half-time programmer
• Three graduate assistants
New Project: Promoting the Resilience of Communities and Critical Infrastructure Facing Wildfires

Presenter: Randall Sandone, University of Illinois Urbana-Champaign
PI: Paolo Gardoni, University of Illinois Urbana-Champaign
The Problem
Wildfires are a growing concern with significant annual losses

• Recent wildfires in California have become one of the deadliest and most destructive ones on record (killed 88 people, burned 14,000 residences and 530 commercial buildings, with over $12 billion insured losses)

• Wildfires can be caused by and interact with infrastructure like electric power
  – Transmission lines traversing heavily forested areas may trigger wildfires
  – Power outage or preventive shutoff can significantly affect communities and businesses (liability issues)

• Changes in the frequency and severity of wildfires and in exposure conditions contribute to the growing trend of annual losses
  – Climate change tend to favor extreme droughts, leading to longer fire seasons
  – Developments at the wildland-urban interface increase values at risk
Wildfires present a front-like geometry propagating toward unburned vegetation

- The local propagation speed, called the rate of spread (ROS), depends on topography, environmental, and fuel conditions
  - Elevation, slope, and orientation of terrain
  - Wind speed and direction
  - Vegetation properties

- Wildfire can also propagate with firebrand advections
  - Lofted embers can potentially initiate spot fires far ahead of the fire front
  - It is one of the most dangerous spreading mechanisms for wildland/urban interface

- The direction and speed of propagation depend on multiple physical processes

- The challenge is to capture these physical processes at a manageable computational cost
  - Complex physics coupled with uncertainty renders fully physics-driven models computationally intractable
  - Empirical models are too simple to yield accurate results
Regions outside of the footprint of a wildfire can also experience loss of service from critical infrastructure

- Damage to infrastructure due to wildfires can affect the overall functionality of critical infrastructure
- Other infrastructure supported by damaged infrastructure (like the water network supported by the power network) can experience disruptions due to infrastructure interdependencies
- Differently from other hazards, infrastructure like power networks can be both damaged by wildfires as well as the source of wildfires
- This project will develop models to predict
  - wildfire propagation, and
  - damage to critical infrastructure
- The project will also develop a meaningful visualization of wildfire propagation and damage
What Will Success Look Like?

For **future** wildfires, we will be able to
- predict the propagation pattern and impact areas for given conditions, like vegetation, terrain, and weather
- find the probability that a wildfire can reach specific targets

The formulation will also allow us to update predictions based on the effects of climate change

For **ongoing** wildfires, we will be able to
- provide real-time or faster predictions as a wildfire propagates
- update predictions in (near) real-time using the latest data on vegetation, weather, and fire propagation

The real-time updating will allow us to tailor the generic model to a specific region and time
What Will Success Look Like?

• For critical infrastructure, we will predict the damage to individual components and the effects on the infrastructure functionality.

• The model and visualization will be demonstrated by prediction in hindcast the Camp Fire in Butte County, California.
Benefits

• The developed models and visualization will be a milestone toward the identification of solutions and help prioritize mitigation strategies for reducing risks and promoting the resilience of communities and infrastructure
  – For future wildfires, the developed models will help achieve the desired infrastructure resilience by simulating the effects of mitigation plans to reduce wildfire losses
  – For ongoing wildfires, the real-time predictions of wildfire behavior and infrastructure damage will help optimize the management of human and economic resources

• Future work could extend these efforts to define a national wildfire risk index representing the long-term risk of communities to wildfires, and creating web-based maps for risk communication and decision making
Past Work

The project will build on our past work on wildfire propagation and the modeling of critical infrastructure

• We have already formulated a preliminary system of differential equations to model fire front dynamics and its stochastic variations
  – The equations capture the effects of weather conditions, topography, and vegetation properties

• Also, we have been developing a numerical method to solve such stochastic differential equations and update the solution based on observed data

• We also have experience with the modeling of damage and functionality of critical infrastructure subject to other natural hazards like earthquake, wind, and hurricane
Planned Activities

1. Formulate the equations for wildfire propagation
   - Balance the account of physics, required data, and computational time

2. Develop a computationally tractable approach to solve the equations
   - Necessary for real-time predictions and updating

3. Model damage to critical infrastructure

4. Test the developed models using past wildfire events
Networking break

15-minutes
ON THE HORIZON