Agenda:
10:00am: Welcome and State of the Institute Remarks
10:20am: ICDT + Industry
10:40am: OCRI Overview
11:00am: ICDT + Engineering
11:25am: Outreach & Events
11:40am: Curricular Programming
12:00pm: Lunch
12:40pm: Technical Pillars
   Cyber Range
   Mobility & Manufacturing
   Full Stack
   Human Dynamics & Misinformation
1:20pm: Summary & Closing
Institute for Cybersecurity and Digital Trust

Town Hall
Industry
Industry Engagement
Mark Bartman and Don Boian

Next Steps:
• Codify the Industry Advisory Board ASAP – Quarterly meetings
• Collaboration from Industry to address research topics, interest areas will change frequently
• Presentation/communication skills are critical – build during internships
• Develop a “Conference of Centers” or “Inter-center Council” where representatives from all the Centers/Institutes at Ohio State can share ideas, needs, efforts, and make sure there is no duplication of effort.
• Partner with FCOB to develop a training session for Board members to better understand cybersecurity and digital trust (Executive MBA type program)
Outreach
Outreach & Events
Julia Armstrong and Helen Patton

Session Goals

• Identify the community on and off campus interested in student and faculty engagement
• Map the current landscape
• Use the time to discuss strengths and opportunities; form next steps and FY22 objectives
What Is The Cybersecurity Canon?

A Curated Catalog of Security Books.

Hall of Fame winners are:

“must-read books for all cybersecurity practitioners—be they from industry, government or academia—where the content is timeless, genuinely represents an aspect of the community that is true and precise, reflects the highest quality and, if not read, will leave a hole in the cybersecurity professional's education that will make the practitioner incomplete.”
How Are Books Chosen?

Book Criteria:

- Crowdsourced Recommendations
- Books are Read and Reviewed. Reviewers Recommend:
  - Hall of Fame (HoF) Candidate
  - In the Canon, for Niche Audience
  - Do Not Read
- HoF Candidates are voted upon by Committee
  - Remains a candidate for 5 years
- HoF Winners are awarded each May

https://icdt.osu.edu/cybercanon
How Does This Relate to ICDT?

Benefits:

• Industry Exposure
• Partnership with Professional Organizations (ISSA, etc.)
• Access to authors for speaking opportunities
2020-2021 Winners

https://icdt.osu.edu/cybercanon
Outreach & Events

Discussion Summary

• Discussion around possible future events & opportunities.
  Common themes for longer term plans:
  • high school outreach (students)
  • teacher training & curriculum (middle/high school)
  • Ohio State strengths/research areas --> faculty entrepreneurship
  • Ohio State academic units: build relationships and explicit integrations
  • The importance of human dynamics as it crosscuts all levels, disciplines
Outreach & Events

Objectives for FY22

• Improve website, newsletter and other communications
  • Add content to reach more varied audiences and provide resources, connections
  • Include curricular programs, OCRI resources, K12 opportunities, job board, etc.

• Support formalizing an ICDT Industry Advisory Board
  • Workforce development: traditional and non-traditional students
  • Integrations with formal learning (capstones) and emerging research areas

• Support each technical pillar in broadening engagement in their areas (examples)

• Host a Town Hall in Spring 2022
Curricular Program
Ohio State's Curricular Program
Eylem Ekici

Session Goals

• Presentation of ongoing curricular initiatives
• Questions / Feedback / Suggestions
• New Program / Track Proposals
Ohio State's Curricular Program

Target Audience:

• Students with BS degrees
• Working Professionals

Different backgrounds, abilities, constraints

STACKABLE CREDENTIALS
Ohio State's Curricular Program

Certificates

• Topical concentration
• Completely online
• Caters to wide range of backgrounds

Professional MS Program

• Combines certificates
• Group work and project focus
## Cybersecurity Tracks

<table>
<thead>
<tr>
<th>Core Courses</th>
<th>Offense &amp; Defense (12)</th>
<th>Design &amp; Implementation (12)</th>
<th>Cyber Analytics (12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Cybersecurity (3)</td>
<td>Introduction to Cybersecurity (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Security (3)</td>
<td>Introduction to HW Security (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security (3)</td>
<td>Securing Autonomous Systems (3)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Offensive Security (3)</td>
<td>Offensive Computing (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Introduction to Cryptography (3)</td>
<td>Reverse Engineering and Malware Analysis (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Security (3)</td>
<td>Software Security (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reverse Engineering and Malware Analysis (3)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## MS

<table>
<thead>
<tr>
<th>Complete Two Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethics in the Information Age (3)</td>
</tr>
<tr>
<td>Independent Studies (Group Project) (3)</td>
</tr>
</tbody>
</table>
Ohio State's Curricular Program

Outcomes

• Two Proposed Tracks:
  - Cybersecurity Analytics
  - Management of Cybersecurity

• Proposals for improved education mechanisms:
  - Integrated cybersecurity education at the BS level
  - Adjustable levels of knowledge
  - ODEE helping points
Technical Sessions

- Cyber Range
- Mobility & Manufacturing
- Full Stack Security
- Human Dynamics
The Ohio Cyber Range (OCR) is a shared environment for supporting cybersecurity training and credential-building. Bekah Michael is the Executive Staff Director for the Ohio Cyber Range Institute.

### Session Goals

- Engage colleagues to use and create range materials
- Possibly facilitate proposal writing to NSF SatC EDU and/or the Department of Labor.
Cyber Range

• Ohio Cyber Range, 3 Laboratories (0-2-Hero, ThreatGen, ICS-ICS Cyber) by our Regional Programming Center, Smart Manufacturing & Mobility “Command Center”
• Mark Bartman described the history and role of the Ohio National Guard (& OC3).
• Bob Pardee offered to provide technical support and experience teaching on the range. His group drives ICS-ICS Cyber and an expansion with MITRE attack.
• Julia Armstrong reviewed OHI/O and the importance of the RPC/OCR opportunity.
• Anish Arora described his role as the CSE chair and the POWWOW project with interactions with the OCR. The ARUBA wireless access points are key.
• Hesham Elgamal described serving as the ECE chair and the co-founder of the ICDT institute and the key importance of integrating education, research, and outreach.
• David Sweasey described the interest of the College of Arts & Sciences.
Cyber Range

- Atal Bhargava and Matt Booth plan to keep testing ICS-ICS Cyber and ThreatGen.
- Cathy Xia described her past research (e.g., on password policies) and interest.
- Deborah Boyd and John Witcomb described OH-Tech and managing key resources.
- Irem Eryilmaz described her progress in designing and teaching OSU's Cybersecurity 101, which is open to graduate students. She is interested in games.
- John Hoag described the opportunity to work with the state of Virginia.
- John Wiseman described the Ohio Department of Education (ODE) funding committee and plans to expand and possibly supplement our ODHE funding.
- Qazi Maira U Din described is work with Qadeer Ahmed in smart mobility.
- Tu Feng described her work on Thingworx to help OCR manufacturing and mobility.
- Zhiqiang Lin (ZQ) reviewed his work on vulnerabilities and the cybersecurity club.
Cyber Range
Main objective(s) for FY22

- Ted Allen and Bob Pardee will lead some workshops on the OCR.
- The 3 laboratories will be tested, improved, and shared through the cyber range (0-2-Hero, ThreatGen Exercises, and ICS-ICS Cyber).
- At least 4 courses at OSU will regularly use some range materials in training (Ted Allen, Irem Eryilmaz, ...).
- 2 NSF Secure & Trustworthy Cyberspace EDU proposals (allen.515).
- Bob Pardee participates in the OCRI advisory meeting. Please email pardee.10@osu.edu with any suggestions or questions.
Mobility + Manufacturing
Qadeer Ahmed – MAE/ECE/CAR
Vimal Buck - Center for Design and Manufacturing Excellence (CDME)

Session Goals:
• Offer an overview of progress toward a cybersecurity testbed and gather perspectives on current projects happening at Ohio State and in industry within this space, specifically from faculty not aware or currently working with ICDT.
• Gaining feedback from industry representatives and other groups interested in this discipline as to their needs.
• An open discussion on areas ICDT should focus on regarding mobility and manufacturing for the next few years.
Qadeer and Vimal gave an overview on the OCIMM project and the goal of establishing a campus-wide cybersecurity test bed and eventually connecting it to the OCRI.

Vimal presented on the progress to date of deploying the CDME\ISE testbed and gave a broad overview of research areas in manufacturing:
- potential for theft\access to technical information
- potential for alteration of technical data and processes
- potential for supply chain disruptions or denial of process control.

Qadeer presented on the progress to date of deploying the testbed at CAR and gave specific research areas being researched at CAR:
- Perception based attacks for connected and autonomous vehicles.
- Position, Navigation and Timing security in automated vehicles
- Possibilities of remote navigation and its associated challenges.

Kristie Pfosi, Director of Cybersecurity from Aptiv presented on the overview of current state of the industry in automotive cybersecurity and on the challenges facing Aptiv, a tier one automotive supplier.

Professor Tawfiq Musah presented on his research on challenges of physical layer cybersecurity (chip to chip links) in the mobility and manufacturing space.
Open discussion ensued:

- Working on similar problems that manufacturing and mobility industry are dealing with.
- Strong need to have skilled practitioners
- Introduce cybersecurity at early stages and in all stages of development.
- Industry largely uses OEM/manufacturing tools and tries to keep some of the protocols and communications secret to enable cybersecurity. (Supply chain issues)

Goals:
- Continue building out the testbed in 2022.
- Collaborate with additional faculty in pursuing adjacent areas (e.g. high speed communication links, automotive and manufacturing data communication protocols).
- Find areas for increasing human interaction with respect to trusting increasingly automated manufacturing and automotive systems.
- Collaborate with identifying areas of interest to industry that align with curriculum development in cybersecurity.
Full Stack
Full Stack
Zhiqiang (ZQ) Lin (CSE) and Waleed Khalil (ECE)

Session Goals:
• Hearing the needs from the faculty members
• Defining the metrics for the success of ICDT
• Identifying strategic areas of focus for ICDT
Why ICDT

• ICDT provides a platform, and allows affiliated faculty members to have convergent (interdisciplinary) research

• ICDT provides opportunities for center-scale collaborative proposals
  • NSF’s Engineering Research Centers (ERC)
  • DOD (DARPA, MURI, Air Force, Army, Navy, NSA)
  • DHS, DOE, DOT, NIST

Incentivize Faculty Members

• Buying out teaching time (Hesham)
• Providing seed funds (Waleed)
• Lowering the indirect cost rate for industry grant (Xinmiao)
• Cluster hiring (Hesham)
• Negotiating with OAA for the Support (Anish)
• Providing professional grant writing support (Mark)
Success Metrics:

- JobsOhio
- Return on investment (ROI)
- External Metrics such as practical impact
- Short/long term metrics
- ROI quantification as key to long term success
Strategic Areas

Existing Strengths

• Supply Chain Security
  Air Force COE for Analog and Mixed Signal Domain Security
  OSD’s Microelectronics & Security Education (MEST) Center
• AI/ML
  The AI Institute
• Systems (HPC center)
• Networking (NextG, WiFi, Bluetooth)
• Software (Language security, software hardening)
• Mobility (CyberCAR)
  Center for Automotive Research (CAR)
• Manufacturing
  Center for Design and Manufacturing Excellence (CDME)
• Sensing (The IoT Testbed)
  NSF Advanced Cyberinfrastructure POWWOW

New Emerging Areas

• Healthcare
• Ubiquitous Computing
• (Post)-Quantum Computing
• Defense Logistics AME
• Root of Security in DoD FETT
• Full Stack Bug Bounty Programs
Main Objectives for FY22

• Fostering more collaborations among faculty members
• Engaging more with Funding Agencies, and Industry Partners
• Engaging with OSU PIs and leadership to define and agree on short/long term investments, incentives and success metrics

Action Plans

• Creating working groups
  • Defining the research thrusts
  • Planning for proposals
  • Metrics, investment and incentive strategies
• Holding workshops
  • Brainstorming
  • Knowing the strengths of each other
• Inviting PM/PD for virtual/campus visit
• Planning an NSF IUCRC-like center
Human Dynamics
Human Dynamics and Misinformation
Duane Wegener (Psychology)

Session Goals:
• Identify common interests that link human dynamics to technology development/use/impact
• Assess potential participation by current institute affiliates
• Identify gaps in expertise and potential types of contributors to engage throughout OSU
Human Dynamics and Misinformation

Major Common Interests: Meaning of "trustworthy information"

- Algorithms in AI or ML aimed at efficiency or maximizing attention
- Information theory defining bits of information without context
  - Ignores quality of information, perhaps undermining trustworthiness
- Indicators of trustworthiness using natural language
- Trust of sources of information; Use of existing beliefs to screen information
  - Many social/behavioral factors – social engineering/human factors
- Different meaning of "trust" across levels of analysis
Human Dynamics and Misinformation

Other Key Points:

• Need to reach out (across ASC – from math to philosophy, linguistics, cognitive psychology, communications, political science, and more)
  
• Assembled group was missing types of expertise that have been previously funded in these areas

• The educational/curricular roles remain in flux (important to address; can differentiate our efforts; but constraints exist)

• Human dynamics in Cybersecurity are much broader than misinformation or "untrustworthy" information – many connections and opportunities to leverage for funding
Human Dynamics and Misinformation

Outcomes:

- Identified strong interest and synergy surrounding trustworthiness of information (consistent with major theme of the institute)
- Identified some expertise missing from the current group
- Identified some potential funding programs to pursue
Human Dynamics and Misinformation

FY22 Objectives:

• Identify and communicate directly with researchers working on related problems across the university [partners in that effort?]

• Create working group(s) surrounding trustworthiness of information
  • Possible workshop of talks that span full range of levels of analysis to broaden interest on campus and connect potential collaborators

• Form groups to pursue funding that integrates technical and human facets
  • Having 2-3 groups funded to pursue these questions would help establish this aspect of the institute
Wrap Up

- Summary
- Final Comments & Next Steps
For more information contact:

Institute for Cybersecurity and Digital Trust
icdt@osu.edu
icdt.osu.edu
Ohio Cyber Range Institute  
Current State  
June 2021
OCRI Vision and Mission

Improve Cybersecurity for the Citizens of Ohio

Sponsored by the Ohio Department of Higher Education, the Ohio Adjutant General's Department office of the Ohio National Guard, and headquartered at the University of Cincinnati, the Ohio Cyber Range Institute will support collaborative cybersecurity programs across Ohio. The goal of the OCRI is to advance an integrated approach to cybersecurity education, workforce, and economic development in cyber-related fields throughout the state.
OCRI and OCR

The Ohio Cyber Range Institute (OCRI) is more than just the Ohio Cyber Range (OCR). The OCRI hosts and manages the OCR. The OCRI includes the curriculum development, research, workforce development, and industry connections that don’t utilize the OCR.

Examples include

- Ohio Cybersecurity Curriculum library
- cybersecurity awareness workshops
- K-12 unplugged activities
- cybersecurity research
- student portfolio
Impact Report
1/2018-5/27/2021

43 Counties Impacted*

Programming

- Higher Ed Classes: 375
- K-12 Classes: 138
- Cyber Exercises: 35
- Camps & Seminars: 30

8517 Cyber Citizen Users

185 Instructors

*K-12 & Higher Ed courses tracked at institution county.
OCRI Ecosystem

11/2019 – 5/2021

13 OCRI-RPCs

Still Accepting Applications
## Accepted Proposals

<table>
<thead>
<tr>
<th>Title</th>
<th>PI/Co-PI</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT LEGO-Style Security Labs</td>
<td>Saeed Al-Haj – Ohio Northern University</td>
</tr>
<tr>
<td>Capture of the Flag Challenge Module</td>
<td>Harleigh Hodge – Ashtabula County Technical and Career Campus</td>
</tr>
<tr>
<td></td>
<td>Co-PI: Kenneth Atchinson – Baldwin Wallace University</td>
</tr>
<tr>
<td>Introduction to Digital Forensics</td>
<td>Bilge Karabacak – Franklin University</td>
</tr>
<tr>
<td></td>
<td>Co-PI: Mark D. Riley – Hocking College</td>
</tr>
<tr>
<td>Router Configuration, Access, and Security</td>
<td>Dr. M. Ajmal Khan – Ohio Northern University</td>
</tr>
<tr>
<td>Communicating about data breach incidents: A training program focused on business, ethics and privacy laws</td>
<td>Phoebe Tsai – Cedarville University</td>
</tr>
<tr>
<td></td>
<td>Co-PI: James D. Robinson – University of Dayton</td>
</tr>
<tr>
<td>K-12 Modules and Bootcamps</td>
<td>Todd Mitchell</td>
</tr>
</tbody>
</table>
Regional Programming Centers

- Lorain County Community College
  - Conversion of CBE courses, expansion of mentorship programs, developing partnerships with additional 2- and 4-year institutions
- University of Dayton
  - Creation of Cybermindfulness PSAs, Range Cyber Portfolio development, configuration of Dayton Regional Cyber Range
- Ohio University
  - “Freshmen Kits” – exercises in software and hardware with evaluation, working to connect to local K12 partners on Cyber awareness & exercises within a publicly available workshop
- The Ohio State University
  - Ethical hacking tutorial on sandbox, working through the Ohio Cybersecurity Initiative for Mobility and Manufacturing (OCIMM), partnering with Texas A&M utilizing robots from AIMS lab
- University of Akron
  - Integrating Cybersecurity into other programs/departments at UA, partnering with Baldwin Wallace and Boy Scouts, Northern Ohio InfraGard Cyber Camp
- University of Cincinnati
  - Continuing to run bootcamps, competitions, and engaging CHEST, CAE-CD, CCSP
Regional Programming Centers

- Cedarville University
  - Engaging Lakota HS and support from students, developing curriculum/modules for the Ohio Cyber Range
- CinDay Cyber at SOCHE
  - Held job fair where 36 companies engaged with students, engaging Girl Scouts, focused on helping those underrepresented in Cybersecurity
- PAST Foundation
  - Developing a digital lab on-site to physically house an access point to the Ohio Cyber Range, planning to run a middle school Cyber program, connecting to schools, community members and industry experts
- Owens Community College
  - Newly designated
- Rio Grande Community College
  - Newly designated, begun outreach to local nonprofits, planning to deliver workshops in local area
- Eastern Gateway Community College
  - Newly designated
- Stark State College
  - Newly designated
Welcome to the first Ohio Cyber Range Institute (OCRI) Newsletter.

Ensuring that our ability to leverage the internet for commerce, communication, and staying connected with friends and family requires that cyberspace remain secure. As we have learned over the past eight months, the digital backbone to Ohio's economy has never been more important as many of us have had to rely on working and communicating remotely in order to stay safe and connected. As we overcome the pandemic, unlocking the potential of Ohio's citizens to work and stay connected in virtual space will not recede. In fact, being able to manage cyberspace is and will increasingly become a skill-set that will position people for great paying jobs and careers, both in technical areas and across all business activities.

The state of Ohio is advancing a new model to enhance the cybersecurity of its citizens, the state, and the nation and create new pathways to the 21st-century workforce. Leveraging the research and educational power of its university and college system in partnership with five state agencies, the state of Ohio created the Ohio Cyber Range Institute, hosted at the University of Cincinnati, to galvanize the integration of cybersecurity efforts across education, workforce, and economic development.

Subscribe to the OCRI Quarterly Newsletter: https://www.ohiocyberrangeinstitute.org/
Links & Resources

• Newsletter: [https://www.ohiocyberrangeinstitute.org/](https://www.ohiocyberrangeinstitute.org/)
• RPCs: [https://www.ohiocyberrangeinstitute.org/rpc](https://www.ohiocyberrangeinstitute.org/rpc)
• Events: [https://www.ohiocyberrangeinstitute.org/programs-events](https://www.ohiocyberrangeinstitute.org/programs-events)
• OCRI Program Coordinator: Adam Sedlacko [sedlacam@ucmail.uc.edu](mailto:sedlacam@ucmail.uc.edu)