



National Security Agency Centers of Academic Excellence

5 January 2022



Michael Losavio, Department of Criminal Justice and Mike Bassi, Southern Police Institute

Sharon Kerrick, Department of Educational Leadership, Evaluation and Organizational Development

Adel Elmaghraby, Winnea Professor of Computer Science and Engineering, and Adrian Lauf, Department of Computer Science and Engineering

Jeffrey C. Sun, Associate Dean, College of Education and Human Development

Im Ghiyoung and Andrew Wright, College of Business

Richard Maiti, Kentucky State University

University of Louisville
Kentucky State University

The Role of Centers of Academic Excellence in Democratizing Cyber Security

What the...???

For better or worse, we and our allies are democracies under the rule of law.

Those attacking are less and less so...

 Q. 1 – Does our status as democracies change how we respond to cyber threats?

• Q. 2 – If not, is our current response sufficient?

• Q. 3 -- If so, how do we respond to be sufficient?

Consider the threat space for computing in democratic societies

- Heterogenous
- Distributed
- Disparate Implementations
- How can we possibly address these vulnerabilities against vectors of attack?

Your challenge:

For the course of this talk, and after, consider if, and how, we can <u>possibly address these</u> vulnerabilities against vectors of attack.

• If we don't, it won't go well for us.

So...

- Traditional public safety relies on distributed efforts
 - Citizens- We The People
 - Police
 - Courts and Corrections
- But Cyber Security tends towards limited points of security via IT technical systems and guardians
- We must expand public and citizen engagement in cyber security

We must "Democratize" Cyber Security

- Empower small organizations, from small businesses to NGOs
- Empower local law enforcement to engage
- Empower the citizens themselves

• See, e.g., Routine Activity Theory: reduce available victims, deter offenders and expand suitable guardians for cyber public safety

Why?

- Well, back home...
- The Vermont National Guard was deployed to help a Vermont hospital recover from cyberattack.
 - Vermont Gov. Phil Scott <u>called members of the state's National Guard</u> to aid the University of Vermont Medical Center in recovering systems and data disrupted in a hacking incident the week of Oct. 25, 2020.
- Countless examples exist.
- It is getting worse...

• What does the future hold?

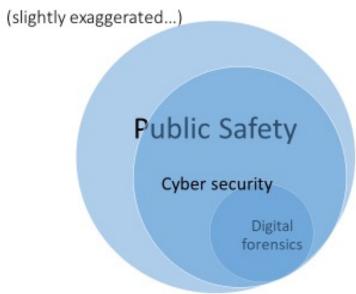
- Greater vulnerabilities?
- Greater disruption?
- Can there be effective technical protections?

• For this project:

- Is this scalable by size of nations?
- Is this portable to varied nations?
- How will we know if it is effective?

• For US?

And with tomorrow's IOT, Smart City, Ubiquitous networking, Big Data...



• The democratization of technology and the democratization of knowledge can address this as both become more available to more and more people in society.

• This ranges from the open source movement to ease of use of proprietary devices.

• It supports inclusion, opportunity and accountability.

• Law enforcement and public safety under the democratic accountability implicit in Western constitutions are vital to the liberties and protections of citizens

• Community policing is one example of a close engagement between law enforcement and the people they are to protect

• Together they may assure better community protection and engagement under the rule of law. Each alone is insufficient

- Cyber security is primarily about protecting people from malicious use of cyber technologies.
- It falls within the values of a democratic society and can benefit from the democratization ideal. It is time for the democratization of cyber security.
- A key component of that will be expanding cyber security engagement through the community.

- There are alternatives...
- Several suggest that we resort to the provisions under the Constitution (US) to issue letters of marque and reprisal to entities for cyber attacks., Thomas Ayres, "A Maritime Solution for Cyber Piracy," Wall Street Journal, 13 May 2021, https://www.wsj.com/articles/a-maritime-solution-for-cyber-piracy-11620922458
- Security engineering alone cannot assure cyber security, just as law enforcement cannot alone assure public safety. Engagement of the academy, state and local law enforcement, private security and regulatory agencies and communities themselves can better extend public safety in the cyber realm.
- This matches the need to design for the usability and psychology of the end users of ICT systems as primary considerations in the engineering for information security; this is just as public security requires "user" engagement if cyber safety is to improve in the face of growing threats.

• we must plan for what the future may hold...

And So Some Transformative Projects: Cyber Security Projects and Outreach

- National Security Agency Cyber Workforce Development Funding - 2017
- US Department of Defense C4 Training Funding
- NSA CAE Cyber Security for Healthcare Industry
- US Department of Homeland Security Cyber Security Training for Law Enforcement Funding

Dr. Sharon Kerrick NSA CAE Cyber Security Pilot for the Healthcare Industry – **PATHWAYS** to Credentials

Explorer Practitioner Professional Healthcare (Badge/s) (Badge/s) Cybersecurity (Badge/s) (Certificate) IT Basics Information Security DB Security Coding Network Security Post Quantum Security Principles & Forensics Cryptography Foundations Cryptography IoMT Possible future Policy/Legal Foundations Privacy (HIPAA) Cloud Security enhancement · Critical Thinking · Cyber Threat Hunting Artificial intelligence Associate options: Ethics · Cognitive Computing Data Mining/Analysis Bachelors Risk Analysis Artificial Intelligence Healthcare Blockchain Graduate Artificial Intelligence Data Mining/Analysis Logistics Deep Learning Degrees Data Mining/Intro Blockchain Robotics Process Cybersecurity Robotics Process Robotics Process Automation Analysis Analyst Automation Analysis Automation Analysis Cybersecurity All curricula will be developed in the context of Healthcare (Labs, Datasets etc.) Technical Specialist Tech Industry badges earned throughout (IBM, Microsoft, etc.) **Progressive Industry Healthcare Cybersecurity Experiences**

Healthcare Cybersecurity - Workforce Certificate



Cybersecurity
Certifications, Careers
and Communities
PROJECT

US DoD Cybersecurity Capacity Building Grant

Overview>>>>>>>>>

The Project: The Commonwealth of Kentucky requested a \$2 million grant to develop cybersecurity education programs and continue efforts in workforce development for transitioning service members, veterans and dependents. This grant is Phase III to diversify Kentucky's defense sector, in alignment with the Economic Adjustment Assistance for State Governments Program. During the period of grant, funding provides a start-up seed program for developing cyber talent.

Concept of Project Operation: A three-phased operation beginning in October 2019 through March 2022, followed by a transition from a grant-based project to an independent university program.

Lines of Effort:

- 1. Enabling functions to shape, set and administer
- 2. Execute unique research-based cybersecurity educational pathways
- 3. Empower employment search success
- 4. Grow, scale, sustain program outcomes

Key Tasks and Goals:

<u>Certification Workshops</u> Develop research-based multiple cybersecurity education-to-defense industry employment pathways that account for and capitalize on the military Family and the diverse Kentucky workforce

- -A Gap Analysis Report: On the DOD contractor labor needs for the region within the labor requirements for cybersecurity positions
- -A Diagnostic Tool: To assess participants' preparedness and interest for placement into the different tracks, administered to all incoming participants

<u>Cyber Experiences</u> Implement a cyber studies credentialing experiential curriculum that harnesses UofL's unique academic environment to deliver quality instruction that meets or exceeds the defense industry standard

- -A Cyber Range: A space for participants to test their cybersecurity and problem solving skills in a mock real world environment while gaining experience
- -Multiple CTF/Hack-a-thons: Opportunities for program participants to deepen and demonstrate their cybersecurity knowledge and skills

<u>Career Community</u> Champion an equitable cybersecurity community education ecosystem in Kentucky that is both sustainable and scalable

- -An Advisory Board: Of industry, academic and government experts to guide the project
- -An Ecosystem Report: On the sustainability and scalability of the program

Our Endstate:

A uniquely Kentuckian cybersecurity educational path:
With research-based, quantifiable positive outcomes in the areas of student success (retention and persistence), employment, and career advancement for alumni with an emphasis in the defense industry.

An improved perception of Kentucky: As a defense-industry (cyber) workforce educational leader.

An increased capacity to provide sustainable cybersecurity opportunities: To Kentuckians that allows for both governmental and private economic growth.



US DoD Cybersecurity Capacity Building Grant

>>>>>>>Current Status

Phase 2 (A): Implement Workshops (OCT 2020- DEC 2021). Execute multi-tiered workshops, scale and administer grant, market, register, enroll, graduate and certify participants, deliver results for/with strategic partners.

Initialize workshops in (CompTIA) SEC+, (Cisco) CCNA, (EC-Council) CEH, (ISC2) CISSP, (MS) Azure, AI, 365. Execute 3 CTFs. Sustain/Expand/Augment Cyber Range activities.

NOW: 12 week online CompTIA SEC+ exam preparation workshop is underway with 25 participants as a "test group," utilizing Linkedin Learning and Blackboard LMS synchronous instructor-led supplemental weekly sessions.

Pre-registration open for 20 February 2021 "Cardhax" Capture-The-Flag event (Open registration beginning DEC 2020) email Thomas.Krupp@Louisville.edu

Points of contact:

Website: http://louisville.edu/education/departments/eleod/skills/c4
Project Director Jeffrey C. Sun, J.D., Ph.D. (Jeffrey.Sun@louisville.edu)
Project Manager Thomas Krupp, LTC, USA RET (Thomas.Krupp@louisville.edu)
Sponsored through a DOD/OEA Grant with the Kentucky Commission on Military
Affairs (Dallas Kratzer@ky.gov)

This program is being implemented under a grant agreement with the University of Louisville, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the University of Louisville and does not necessarily reflect the views of the Office of Economic Adjustment.

2017 NSA Cyber Workforce Education

2020 DHS Cyber Security for Law Enforcement

Focus on State and Local Law Enforcement Cyber Education



Bringing Public Safety Personnel into Cybersecurity Careers

- Increase the pool of cyber security professionals in multiple domains
 - by identifying, recruiting and training practitioners and students in law enforcement and public safety disciplines
- Integrate criminal justice systems and practices into cyber security
- Local law enforcement is at ground zero for cyber criminality and its victims
 - Can respond
 - Can advise
 - Can arrest

Boot Camp: September 2017 until June 2018

Table 1 - Initial Data on Participation in Introductory Courses

Topic	Enrollment	Completion
Cyber Crimes: Law and Practice	111	completed
Infrastructure Technology	67	completed
Introduction To Network Security	59	completed
Introduction To Information Security	47	completed
Computer Forensics	32	completed

Core Element - Community Engagement by Law Enforcement in Cyber Security

Schools

• Small businesses & government agencies

Citizens

2021 DHS Needs Assessment

- Follow up on design
- Data collection in process

Closing thoughts

- So, can this work?
- If so, how do we make it work?
- This will need all of us!

- Thank you
- For comments of any type, please email michael.losavio@louisville.edu – just keep it clean!