# Integrating Democratic Cybersecurity: Empowerment of Traditional Law Enforcement and Democratic Public Safety

**Michael Losavio, Jeffrey C. Sun, Sharon Kerrick, Adel Elmaghraby, Cheryl Purdy and Clay Johnson**
**University of Louisville, Louisville, Kentucky, USA**
Michael.Losavio@louisville.edu
Jeffrey.Sun@louisville.edu
Sharon.Kerrick@louisville.edu
Adel@louisville.edu
Cheryl.Purdy@louisville.edu
Clay.Johnson@louisville.edu

**Abstract**: The expansion of pervasive and ubiquitous computing, especially with the advancement of the Internet of Things and the Smart City concept, extend the novel means of criminality and its investigation. We argue that current forms of investigation and discovery are not sufficient to limit injuries onto persons and communities. Nonetheless, cybersecurity approaches within criminal justice, criminology, and workforce development – together – offer models that significantly benefit efforts to address public cybersecurity harms, yet they have been largely overlooked. This paper draws on an interdisciplinary lens to address cybersecurity, including criminal justice and workforce development integration and employing empowerment theory. Applying empowerment theory, this presentation demonstrates the effects from integrating cybersecurity and forensic practices into traditional law enforcement. The effects are positive as public safety will be needed to provide public safety and security in our hybrid technical world. Thus, this paper illustrates how we must, in essence, "democratize" cybersecurity through its distributed availability. We present means to achieve this and results from efforts to promote this integration through several coordinated, yet differently targeted programs at one research university.

**Keywords**: democratic, distributed, cybersecurity, law enforcement, public safety

## 1. Introduction

The expansion of pervasive and ubiquitous computing, especially with the advancement of the Internet of Things and the Smart City concept, extend the novel means of criminality and its investigation (Chow, Losavio, Joshua, and Koltay 2018). Indeed, higher education has tackled the privacy, breach, and harms associated with data analytics and cyber for many years (Sun 2014), but its solutions are relegated to a specialized group so operations continue in spite of the high degrees of harm and continuous threats. We argue that current forms of cyber investigation and discovery are not sufficient to limit injuries onto persons and communities.

Traditional public safety relies on distributed efforts of citizens, police, courts, and corrections. By contrast, cybersecurity efforts have tended towards limited points of security via IT technical systems and guardians. Our societal solutions focus on narrow expertise and limited actors. In many nation-states cyber crisis employs a public-private partnership to address attacks, but often one entity takes the lead. For instance, Czech and Estonian responses centers around a "network administrative organization" approach where an outside entity manages the network activities with enforcement power (Boeke 2018). Denmark operates off a "lead-agency" model, and Netherlands established a "participant-governed network" to better link the private organizations with the government agencies (Boeke 2018).

This paper applies empowerment theory. While the term empowerment is somewhat of a hackneyed saying and captures many constructs, some of which are not empirically sound, here, the concept of empowerment theory is more than simply encouraging and motivating others (Wilkinson, 1998). Broadly speaking, empowerment theory connects processes and structures that individuals and groups employ to reach common goals (Perkins & Zimmerman, 1995). It is conceptualized as a process and outcome theory; macro and micro theory (with consideration of the meso range); and organizational, intrapersonal, and individual levels (Amor, Xanthopoulou, Calvo, & Vázquez, 2021; Perkins & Zimmerman, 1995). For purposes of this article, we adopt Leong, et al.'s (2015) empowerment theory. It is an applied crisis response version of that considers the structural, psychological, and resource empowerment settings. This model connects relationships between empowerment settings, in which structural and psychological empowerment are connected with the attainment of shared identification of the activity or outcome, structural and resource empowerment are connected with the attainment of collective

participation, and resource and psychological empowerment are connected with the attainment of collaborative control toward the outcome. Given its nesting in information and communication technology (ICT) and application in a crisis management setting, its use as the type of empowerment theory for cybersecurity seems appropriate.

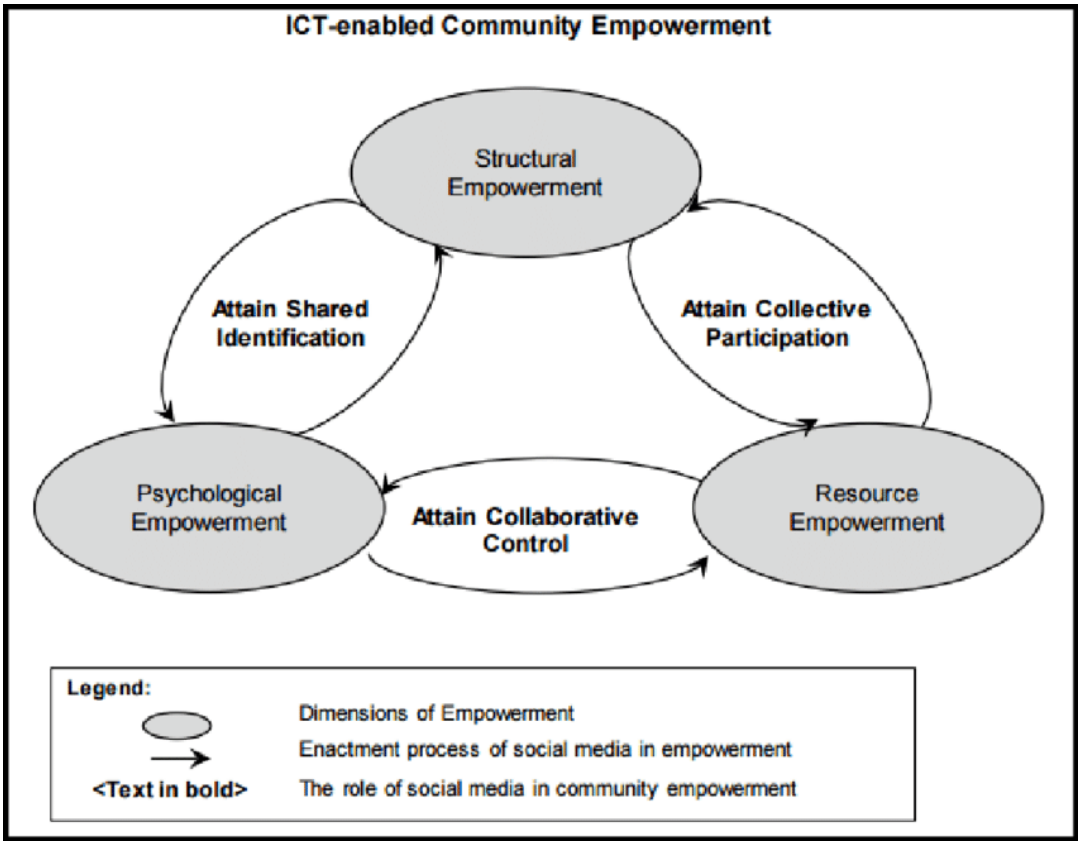


**Figure 1**: Leong, et al.'s (2015) information and communication technology enabled empowerment theory

Drawing on empowerment theory, the authors demonstrate, through multiple-related cyber training programs, that the rapidly shifting information technology environment make it is necessary to expand public and citizen engagement in cybersecurity. This approach is to, in effect, take principles of democratic knowledge and governance and extend them into the realm of security for cyber-resources by empowering people around us. The goal is empower through structural, psychological, and resource empowerment settings to build a workforce in cyber but drawing not simply on development of cyber experts in computer science, engineering, or information technology. Instead, we develop a generalized and wide scope of cyber workforce akin to "leadership" allowing many to enter this space, not selected few who reside in a tech-tower. Stated another way, this approach demonstrates how we must empower small organizations, from small businesses to non-governmental organizations (NGOs) to local law enforcement agencies to educational institutions, as well as the citizens themselves, to engage in cybersecurity.

This application of the empowerment theory presents solutions to the principles in criminology for effectively reducing crime, such as the Routine Activity Theory and the Opportunity Theory. Routine Activity Theory and the Opportunity Theory opine that crimes occur during vulnerable stages through opportunity seeking behaviors of criminals. Through empowerment theory, we envision opportunity reductions and closures in cyber gaps. Accordingly, these implementations to close these gaps and design empower-thriving settings (among structural, psychological, and resource empowerment settings) cyber breaches will be reduced. That is, a distributed cyber workforce development at the micro-level, which may be expanded across domains of multiple professions, much like leadership training and development, will protect people by reducing the numberof vulnerable targets subject to attack. At the same time, by expanding available "guardians" as to reduce and deter thoseintending to participate in wrongdoing, we will have enhanced our cyber public safety.

It is essential for cyber-safety to anticipate future risks and vulnerabilities to systems. To do so, it is important to ask whether there are constantly changing issues as to greater vulnerabilities or greater disruptions, and whether there can be effective technical protections. For physical capabilities, our policymakers, organizational leaders, and educational institutions have a sense of how to avoid many risks and protect people from vulnerabilities at concerts, sporting events, community gatherings, and festivals. The challenge is associated with cyber attacks when they involve computers, networks, and the cloud, but they also involve cell phones, watches, cars, televisions, and even refrigerators. Although this paper addresses a regional effort, this concern of cyber breaches is, on the broader note, to be considered as a national/international issue threatening all of us and nearly all things. Accordingly, we are charged (and could be empowered) to look at potential solution sets and ask whether various activities or interventions are scalable by size of nations and whether they are portable to varied nations (or even areas/regions).

Globalization has led to integration across many dimensions. It will be important that as many as possible can be protected, even as the ubiquity of computing will grow with the Internet of Things, the Smart City, Big Data, and universal and pervasive computing generally, as seen in Figure 2.


**Figure 2**: The Integrated Domains of Public Safety, Cybersecurity and Digital Forensics

Under the democratic accountability implicit in Western constitutions, law enforcement and public safety are vital to the liberties and protections of citizens. Together, they may assure better community protection and engagement under the rule of law. Standing alone, however, neither is sufficient. One example of a close engagement between law enforcement and the people is community policing as an approach. Community policing involves assigning officers to certain areas so they become familiar with the local citizens in their assigned area. If applied to cyber security, we must consider several questions including:

1. What is a community for cyber security?
2. How do we embrace and empower communities to understand and observe the community norms or notice outlying coded behaviors?
3. What alternatives might we have to cyber community policing?

Several scholars suggest that we resort to the provisions under the U.S. Constitution to issue letters of marque and reprisal against malicious entities for counter-cyberattacks (Ayers, 2021). However, the question then becomes: would that really work, or would it just open up the Pandora's cyber-box of furies to haunt us? Thus, we posit that an integrated system, which is based on community empowerment of public safety, is needed for cybersecurity.

## 2. Case Study-Ransomware and a Distributed Model Protection

Cybercrime and extortion are moving down to the consumer level, hitting small businesses as well as large enterprises. Styled "Ransomware," this attack consists of malware, like a computer virus, that has been downloaded to your system and encrypts all of your files, then shows a ransom note stating that you will get the decryption key if you pay the amount demanded. If the attacker demands bitcoin or similar digital tokens, it is difficult, if not impossible, to trace. If you do not pay the "ransom", at best you may lose use of those files; at worst, critical, confidential documents will be posted on the Internet. Major businesses have been hit, and many have

paid millions to avoid critical service disruptions, ranging from energy infrastructure (e.g., fuel pipelines) to medical systems (e.g., hospitals).

Cybercrime is a serious risk for small businesses, organizations, and families, coming from an explosion in ransomware attacks tied to its profitability. For example, Forbes Magazine (Shankar 2021) noted that ransomware operators are targeting law firms, which are usually small businesses that are data and information intensive. The confidentiality of information that law firms possess is vital, and there is a professional obligation subject to sanctions for its violation. The motivation is, as always, money, whether it be directly or indirectly. Consider the value of confidential data from corporate entities, it is ideal for investing ahead of public announcements about data breaches such as sensitive information like individual tax returns or breaches making them perfect for identity theft fraud. Forbes cited the American Bar Association's *TechReport 2020: Cybersecurity*, which noted significant problems with cybersecurity across law firms and the accompanying potential ethical risks for lawyers (Loughane 2020). The risks of losing client data to the opposing party or a third party wishing to disseminate the information beyond litigants present real threats in terms of financial, psychological, and possibly physical means (as the disclosures often evoke long-term physical reactions).

The Cybersecurity & Infrastructure Security Agency ("CISA") of the U.S. Department of Homeland Security, in an effort to help guide those without their own IT security units, built online guidance and resources to help the distributed operations for our society (Cybersecurity and Infrastructure Security Agency 2020). The CISA Ransomware Guide, available for free download, provides a resource on the "best practices" to prevent attacks and a checklist to respond and recover, if and when, an attack occurs (Cybersecurity and Infrastructure Security Agency 2021). Because the pessimists in cybersecurity opine that it is not a matter of "if," but only "when," a cybersecurity breach will happen, response and recovery planning is essential.

The CISA Ransomware Guide opens with a review of the best practices for the prevention of a cyber attack, beginning with the preservation of protected off-line backups through regular maintenance for vulnerabilities. It covers the benefits and limitations of standard cybersecurity systems and notices the particular role played by the human condition in the success of employee-targeted phishing attacks. The self-help tools offered by CISA then provide a checklist to review your preparation for threat/risk prevention discussions with third parties that may have access to target systems.

This guide still requires due diligence on the part of the citizen-user. This due diligence can range from preparatorytalks with IT specialists about future emergencies to consultation with professional liability insurers on both the coverage they offer and the support they can provide in the event of an attack. And, yet again, the training of employees and users on the proper practices for cyber-safety and security is essential. The technical is simply not enough, and by reinforcing this across an enterprise, security is enhanced, hopefully enough to prevent compromise.

## 3. Distributed Cybersecurity, Local Law Enforcement, and Democratization of Cybersecurity

The democratization of technology and the democratization of knowledge are sometimes used to address the process by which both become more available to more and more people in society. This ranges from the open-source movement, open-source meaning "software in which the source code is freely available for others to view, amend, or adapt" (Poynder 2001), to the ease of use of proprietary devices. It supports inclusion, opportunity, and accountability.

The University of Louisville has focused on issues relating to distributed democratization of cybersecurity, with analysis and position papers regarding the importance of cybersecurity as part of overall governance in a world of ubiquitous computing (Keeling, Shutt, Losavio 2011), (Elmaghraby, Losavio 2017), (Keeling, Losavio 2009) (Losavio, Elmaghraby 2021) (Chow, et al 2018).

These papers led to support from the National Security Agency of the U.S. Department of Defense in 2017 via their Cyber Workforce Development Program. This project was directed by Dr. Adel Elmaghraby, Director of Research and Innovation for the University of Louisville's Digital Transformation Center. The concepts behind this program are based on the changing context of cybersecurity criminal conduct in the world. It grew in

importance because of the ubiquity of computing in the modern world, so cyber attacks could arise from many sources, including nanny cams, emails, text messages, and social media applications.

A decade earlier, the historical context would indicate some, but not much, overlap between the domains of cybersecurity and digital forensics (i.e., the discipline of finding and examining electronic evidence). But such connections were not initially in the works or fully conceived by many of our counterparts. The lack of overlap is clearly changing, such that we must examine the relationships of cybersecurity and digital forensics within the overall structure of public safety, both now and in anticipation of future issues arising from the pervasiveness of computer systems, from the Internet of Things to the Smart City, as shown in Figure 2, above.

To address this cyber readiness, we test various systems relating to local inclination – local needs in defense, local needs in healthcare, local needs of educational institutions, and local needs law enforcement – as they relate to cybersecurity. We examine both the inclination and capability – of defense workers, healthcare workers, educators, and state and local law enforcement to address cybersecurity and cybercrime issues.

This examination of potential online cybersecurity training programs began with five modules for local law enforcement agencies; the program had 111 learners with a waiting list of approximately 100. At least 18 law enforcement occupations, ranging from detectives to criminal intelligence analysts, were present in this first cohort. Officers working in Crimes Against Children and Professional Standards units were in attendance at the first cohort, as were law enforcement personnel from 17 different states, ranging from Alabama to Wyoming. Members of the learning cohort had backgrounds from a surprising range of disciplines, including psychology, organizational management, counseling, criminal justice and public administration, as shown in Figure 3.

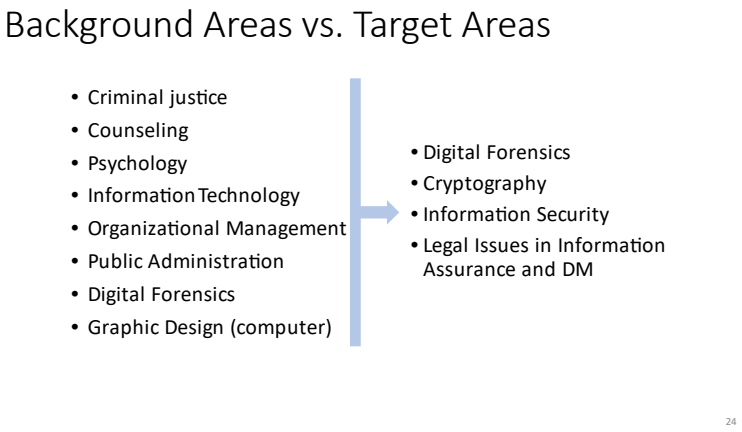


**Figure 3:** Learner Backgrounds

The five modules covering cybercrimes were law and practice, infrastructure technology, network security, information security, and a review of computer forensics.

None of the learners were compensated beyond the courses themselves and, to the best knowledge, worked on these courses in addition to their regular work requirements or academic obligations in other programs. Learners began to drop out of the courses, with several noting a conflict with work. In one instance, a homicide detective notified via email that he would be late getting her/his work completed due to a new homicide investigation, only to send another email the following week stating that s/he would have to drop the course entirely due to a *second* homicide investigation that had opened. This became an issue throughout the course, shown here in Table 1.

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 |

25

Expansion of Cyber Security Training into Other Domains

This cybersecurity training for state and local law enforcement was followed by a series of similar,broad-based cybersecurity trainings in other domains. Those projects are:

1. U.S. Department of Defense C4 Training Funding;
2. U.S. National Security Agency CAE Cybersecurity for Healthcare Industry; and
3. U.S. Department of Homeland Security Cybersecurity Training for Law Enforcement Funding.

### 3.1 U.S. Department of Defense C4 Training

The U.S. Department of Defense C4 project is a cybersecurity workforce development project via the State government of the Commonwealth of Kentucky. It is directed by Dr. Jeffrey C. Sun, professor of higher education and law and associate dean of the College of Education and Human Development for the University of Louisville. Under this 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 in Phase III to diversify Kentucky's defense sector, in alignment with the Economic Adjustment Assistance for State Governments Program. During the period of the grant, funding provides a start-up seed program for developing cyber talent. It is a three-phased operation beginning in October 2019 and ending in March 2022, followed by a transition from a grant-based project to an independent university program. The objectives of the project are to:

- Enable functions to shape, set and administer a world-class cybersecurity program for military-connected participants;
- Execute unique research-based cybersecurity educational pathways;
- Empower employment search success; and
- Grow, scale, and sustain program outcomes.

If these objectives are met, the result will be attainable increased cybersecurity opportunities for Kentucky generally, and for those wishing to work in these fields specifically. Beginning with gap analysis, this project will continue through training cyber experiences, including in the Cyber Range for practical problem-solving in cybersecurity, as detailed in Figure 4:

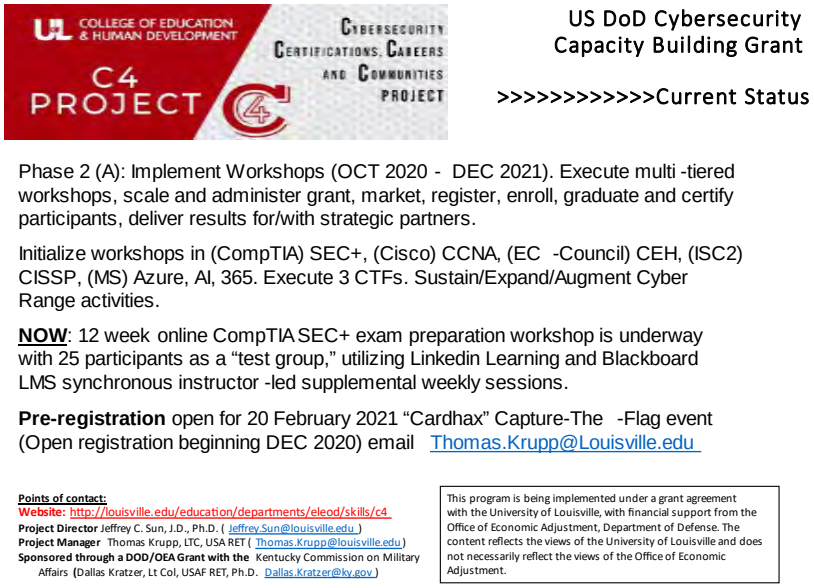


**Figure 4:** DOD C4 Project Overview

The multiple phases of this project begin with recruitment and extend through the initialization and implementation of workshops and standard credentials, particularly through CompTIA. Information is distributed detailing these objectives and points of contact on the project, as shown in Figure 5:

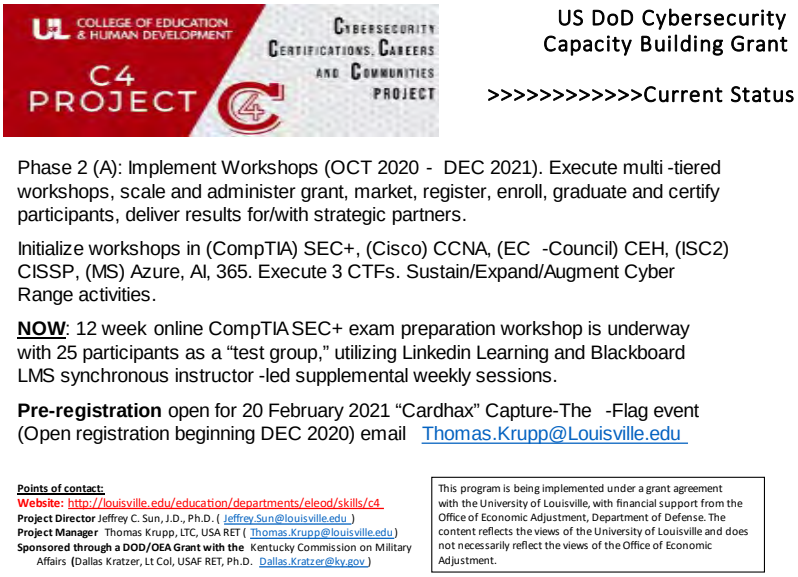


**Figure 5:** Workshops and Credentials

### 3.2 National Centers of Academic Excellence (NCAE) Cybersecurity in Healthcare

Concurrently, a project relating to cybersecurity for the *healthcare industry* was implemented under the direction of Dr. Sharon Kerrick, assistant Vice President for Digital Transformation. This project focused on cybersecurity skills within the healthcare industry, a primary target of cyberattacks via ransomware. For instance, in November 2020, the Vermont National Guard were mobilized to aid the University of Vermont Medical Center in recovering systems after a hacking incident (Scott, 2020). In another instance, a wrongful death action has been filed against a hospital for failing to protect against a ransomware attack[1] that led to the death of an infant (Collier 2021).

[1] The party alleged that the hospital failed to inform the mother of the attack prior to or when she arrived to deliver her baby, which resulted in diminished care and no tests being administered to see that the umbilical cord was wrapped around her baby's neck, resulting in severe brain damage and eventual death.

This project tests the use of online, mentored training in three levels of depth in the discipline: Explorer, Practitioner, and Professional. The Explorer module begins with IT basics and security principles through policy and legal /ethical foundations, and it begins to introduce issues relating to coding and artificial intelligence data mining. The Practitioner module dives deeper into information and network security, forensics, cryptography and cyber threat hunting, intermediate data mining, and legal/regulatory issues within the healthcare industry via HIPAA.

Lastly, the Professional module moves further into database security, cloud security, advanced data mining, and Deep Learning/AI, among other topics. These are followed by industry certifications that establish the skills of the learner for current and future employers. This is shown in Figure 6:

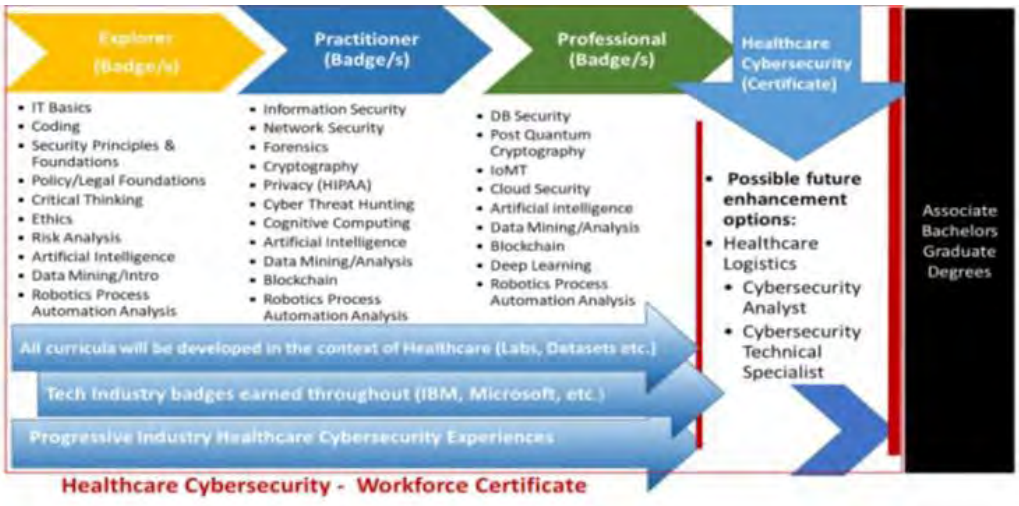


**Figure 6**: NCAE Cybersecurity in Healthcare Programmatic Areas

### 3.3 The U.S. Department of Homeland Security Law Enforcement Cybersecurity Project

The U.S. Department of Homeland Security 2022 Law Enforcement Project follows the earlier NCAE-funded effort in 2017. The 2022 Law Enforcement Project follows the same general topic structure with enhanced use of online learning systems.

A comprehensive analysis by the Police Executive Research Forum ("PERF") found local police agencies are still in the early stages of developing comprehensive strategies for responding to and preventing cybercrime. Additional work needs to be done to ensure that every police officer will know how to respond to a cybercrime call; detectives will understand the avenues that are available for investigating these crimes; and local, state, and federal authorities will have an effective system for sharing information, connecting cases committed by the same offenders, and coordinating investigations. It is critical for the police to have the skills to respond to and investigate cybercrime cases as effectively as they handle other types of cases. Communities will expect their local police to be familiar with cybercrime issues, cybercrime prevention, and investigation. Further, community education on cybersecurity was deemed vital. Police departments often offer education programs to teach people about common cyber-threats and the basics about how they can stay safe online.

Sociological, criminological, and criminal justice/law enforcement models support means of programmatic use of law enforcement for cybersecurity. In structuring public safety solutions to cybersecurity, especially those engaging law enforcement, the rules for our system of justice must be incorporated into the solution.

Supported first by the National Security Agency and then by the U.S. Department of Homeland Security's Science and Technology Directorate, the online training program should increase the pool of cybersecurity professionals in multiple domains by identifying, recruiting, and training practitioners and students in law enforcement and public safety disciplines, including police, probation and parole, military, and other public safety areas. The project does this through a multi-tiered training and education program to develop cybersecurity and forensic skills at the undergraduate and graduate levels. This will include, at a minimum:

- a set of fundamental courses on computer and network operations and security for those in need of basiccomputer and network operations and security skills; and

- a subsequent series of intensive online courses in advanced cybersecurity techniques and issues for thosewho have shown exceptional skills in operations and security.

These teaching programs were developed through collaboration by the Department of Criminal Justice; the Department of Educational Leadership, Evaluation and Organizational Development; the Department of Computer Information Systems of the Business College; and the Department of Computer Science and Engineering. We hope cybersecurity practices can be deployed in the community and used both to expand civil cybersecurity protection and to provide skills for the use of law enforcement deterrence and incapacitation of offenders.

This project integrates traditional public safety personnel into the cyber-safety regime. This integration will provide a broad distribution of cybersecurity skills, advice, and counsel across a community which may, in turn, serve to better harden citizen targets—whether that be the elderly, families, or small businesses—against attacks. These attacks may be directly against these victims. Or, they may seek to attack others, who may be more lucrative and vulnerable targets. In turn, these public safety professionals will have cybersecurity skills they can use once they leave public service life and move into other domains that need their skills for cybersecurity (perhaps, corporate consulting groups). Detailing their ability to cross into corporate and other settings, we outline the outcomes of these learners. By participating in the program, learners will:

1. Increase the pool of cybersecurity professionals in multiple domains by identifying, recruiting, and training practitioners and students in law enforcement and public safety disciplines;
2. Integrate criminal justice systems and practices into cybersecurity; and
3. Advise local law enforcement, which is at ground zero for cyber-criminality and its victims, on effective ways to respond, advise, and arrest attckers.

The training, which began in 2021, built on a needs assessment by Professor Jason Gainous that found, *inter alia*, that:

1. Most agencies both internally investigate cybercrime incidents and report instances of cybercrime to other reporting agencies;
2. Generally speaking, agencies are lacking in both general and specialized training as part of their basic training, or as part of in-service operation, and do not have dedicated cybersecurity and cybercrime units that have staff with a specialized focus; and
3. Agencies are short both on offering community training and on resources for community training.

The training cohorts began with a total number recruited of 174, but only 171 continued. Regarding the rank of those recruited, there is an almost even split for most common, with police detectives/investigators (n=34, 19.5%) just slightly outnumbering patrol officers/troopers (n=33, 18.9%). The two most common ranks were followed closely by police lieutenants (n=27, 15.5%). Police captains, sergeants, and non-sworn personnel were equally common (n=15, 8.6%) and were slightly more common than police chiefs/assistant chiefs (n=13, 7.4%). The least common among the ranks were majors (n=4, 2.3%), deputies (n=3, 1.7%), corporals (n=2, 1.1%), commanders (n=1, 0.6%), and sheriffs (n=1, 0.6%). Other titles/ranks registered included agents/special agents (n=4, 2.3%), instructors/directors (n=2, 1.1%), and miscellaneous military designations (n=2, 1.1%).

As to the states, cities, and departments participating, there are 32 states participating, including Washington D.C. (see full list below), and registration interest was received from officers in Nigeria and Beirut as well.

Across the United States, individuals from police departments, sheriff's offices, and other governmental departments have registered for the course using 117 unique addresses and just as many zip codes. This suggests that our course has permeated departments and has been spread among divisions within the same city and department. The U.S. states represented include Pennsylvania, Indiana, Massachusetts, Michigan, New York, Kentucky, Illinois, Tennessee, Florida, North Carolina, Arkansas, South Carolina, Vermont, Mississippi, Missouri, Ohio, Alabama, Washington,South Dakota, Connecticut, California, Georgia, Oregon, Virginia, North Dakota, Iowa, Kansas, Colorado, Nebraska, Minnesota, Arizona, and Washington D.C.

This data demonstrate both an existing need for the skills among local law enforcement and an interest in training to provide the skills across multiple dimensions. The variety of law enforcement departments in the multitude of states represented in the cohort to a broad geographic and the wide departmental interest in having the skills available demonstrate the significant need – perhaps in regional clusters through an empowered

approach. Horizontally, interest in cybersecurity skills and detectives/investigators and patrol officers. This interest extended into the domain of police lieutenants and sergeants, with interest also shown by law enforcement officers at the captaincy level as well as by non-sworn personnel. A surprising number of police chiefs and assistant chiefs were also represented in the training.

Vertically, there was learner interest from 107 departments (with a few providing several law enforcement officials from their departments) coming from in over 100 different cities across 33 states, from Alabama to Washington state. This supports the wide interest and the need for the services across law enforcement in the United States.

Training has come in the basic series of five courses that cover IT basics, legal issues, network security, information security, and computer forensics. Although all of the initial learners across the three cohorts are participating only for training, we will review the impact of continuing law enforcement education accreditation for the program. Kentucky Law Enforcement Council approved the basic training series or law enforcement continuing education, which will also be available to other departments around the United States under reciprocity agreements. For example, Kentucky accepts reciprocity from law enforcement training on a case-by-basis upon submission of the application for reciprocity credit and information regarding the applicant's work history. Project participants will be advised to contact the training officer for their department as to reciprocity application per state law. For example, Arkansas's Commission of Law Enforcement Standards and Training, Rule 132.0 0.17-001, 1008 Waiverfor Equivalent Training, provides "(4) The Commission is authorized to enter into standing reciprocity compacts or agreements with those states which by law regulate and supervise the quality of law enforcement training and which require a minimum number of hours of classroom training in the Basic or Recruit Course equivalent to standards established by the Commission" (Arkansas Commission on Law Enforcement Standards 2021). Another example is the Texas Commission on Law Enforcement, which accepts Out of State Service/Training Credit for Peace Officers (Texas Commission on Law Enforcement 2021). A list of training accreditation sites by state is available through Lenoir Community College, at https://www.lenoircc.edu/pdf/SA-BLET.pdf (Accessed 5 December 2021).

These results and the data they produce support the proposition that law enforcement cybersecurity training is desired by state and local law enforcement in the United States and has the potential of increasing distributed cybersecurity across the United States.

## 4. Conclusion

The wide participation in these projects across multiple dimensions—from law enforcement and public safety to healthcare to national defense—reflects an underlying sentiment for many to protect those in their communities from all threats, to the extent they can.

The diversity of skills, backgrounds, positions, and education in those participating in this new learning demonstrates a broad and deep interest in this new frontier. Further, the participants' commitment to take on additional workloads of cybersecurity education in addition to their full-time jobs demonstrates a commitment to mastering new knowledge to enhance their skills.

Such opportunities must expand to build an adequate cybersecurity regime to protect all of our fellow citizens. These training programs can advance formal credentialing through the development of a structured curriculum that is translatable to a broad array of education contexts, and it will build a distributed security regime to protect and empower more and more people in our United States.

## Acknowledgments

We wish to thank the U.S. National Security Agency, the U.S. Department of Defense, the Commonwealth of Kentucky, and the U.S. Department of Homeland Security for their support in making these pilot projects possible in pursuit of the cybersecurity of all Americans. This research was funded by a National Centers of Academic Excellence in Cybersecurity grant H98230-20-1-0347, which is part of the National Security Agency. Continued activities within the online law enforcement training program are conducted with DHS S&T under contract number 70RSAT20CB000021. In addition, we express our appreciation and impactful partnership with the U.S. Office of Economic Adjustment, Department of Defense (DOD) and the Kentucky Commission on Military Affairs

for the Cybersecurity, Certifications, Careers, and Communities (C4) project under the Federal Award Identifier Number HQ00052110003.

## References

Amor, A. M., Xanthopoulou, D., Calvo, N., & Vázquez, J. P. A. (2021). 'Structural empowerment, psychological empowerment, and work engagement: A cross-country study.' *European Management Journal*, 39(6), pp. 779-789.

Arkansas Commission of Law Enforcement Standards and Training. (2021) *Rule 132.0 0.17-001, 1008 Waiver for Equivalent Training* [Online]. Available at https://www.law.cornell.edu/regulations/arkaNCAEs/Ark-Admin-Rules-132-00-17, [Accessed 5 December 2021].

Ayres, T. (2021) "A Maritime Solution for Cyber Piracy", [online], Wall Street Journal, https://www.wsj.com/articles/a-maritime-solution-for-cyber-piracy-11620922458.

Boeke, S. (2018). 'National cyber crisis management: Different European approaches.' *Governance,* 31(3), 449-464.

Chow, K.P., Losavio, M., Joshua, J., and Koltay, A. (2018) "The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy and Security", *Security and Privacy*, 1(3).

Collier, K. (2021) *Baby died because ransomware attack on hospital, suit says* [Online]. Available at https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 [Accessed 28 November 2021].

Cybersecurity and Infrastructure Security Agency. (2020) *Ransomware Guide* [Online]. Available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf [Accessed 28 May 2021].

Cybersecurity and Infrastructure Security Agency. (2021) *Stop Ransomware* [Online]. Available at https://www.cisa.gov/ransomware [Accessed 11 Jan. 2022].

Elmaghraby, A.S. and Losavio, M.M. (2017) Smarter Cities Need Smarter Security**.** In T. Saadawi and J. Colwell, eds. *Cyber Infrastructure Protection, Vol III*. Carlisle, PA: US Army War College Press. pp 137-156.

Leong, C. M. L., Pan, S. L., Ractham, P., & Kaewkitipong, L. (2015). 'ICT-enabled community empowerment in crisis response: Social media in Thailand flooding 2011.' *Journal of the Association for Information Systems*, 16(3). https://doi.org/10.17705/1jais.00390

Losavio, M. and Elmaghraby, A. (2021) Artificial Intelligence, Smart Technologies and the Internet of Things:Caution with the Safety, Security and Privacy Eco-system. In Rocha, A. and Isaeva, E. (eds.) *Science and Global Challenges of the 21st Century - Science and Technology Perm Forum 2021*, 18-20 October 2021, Perm, Russia: Springer, Cham. pp 92-102. Available from https://link.springer.com/chapter/10.1007/978-3-030-89477-1_10#citeas .

Losavio, M.M., Keeling, D., and Elmaghraby, A. (2009) A Distributed Triage Model for Digital Forensic Services to State and Local Law Enforcement. In *2009 Institute of Electrical and Electronic Engineers (IEEE) Fourth International Workshop on Systematic Approaches to Digital Forensic Engineering,* 21 May 2009, Berkeley,CA: IEEE. pp 36-37. Available from https://ieeexplore.ieee.org/document/5341551.

Losavio, M.M., Shutt, J., Keeling, D. (2011) The Information Polity: Social and Legal Frameworks for Critical Cyber Infrastructure Protection**.** In: T. Saadawi and L. Jordan, eds. *Cyber Infrastructure Protection.* Carlisle, PA: US Army War College Press. pp 129-158.

Loughnane, J. (2020) *ABA Techreport 2020: Cybersecurity* [Online]. Available at https://www.lawtechnologytoday.org/2020/10/techreport-2020-cybersecurity/ [Accessed 11 Jan. 2022].

Paulson, S. L. (1988). An empowerment theory of legal norms. *Ratio Juris*, *1*(1), pp. 58-72. https://doi.org/10.1111/j.1467-9337.1988.tb00004.x

Perkins, D. D., & Zimmerman, M. A. (1995). Empowerment theory, research, and application. *American Journal of Community Psychology*, *23*(5), 569-579. https://doi.org/10.1007/BF02506982

Poynder, R. (2001) "The Open Source Movement: Does This Software Provide a Viable, User-Friendly Aleternative to Proprietary Solutions?", [online], Information Today, https://www.infotoday.com/it/oct01/poynder.htm.

Scott, P. (2020) *Vermont Army National Guard Cyber Response Team to Support UVM Health Network in Response to Ongoing Information Technology System Disruption* [Online]. Available at https://governor.vermont.gov/press-release/vermont-army-national-guard-cyber-response-team-support-uvm-health-network-response [Accessed: 11 Jan. 2022].

Shankar, AJ. (2021) *Ransomware Attackers Take Aim at Law Firms* [Online]. Available at https://www.forbes.com/sites/forbestechcouncil/2021/03/12/ransomware-attackers-take-aim-at-law-firms/?sh=795f79eba13e [Accessed 11 Jan. 2022].

Sun, J. C. (2014). Legal Issues Associated with Big Data in Higher Education: Ethical Considerations and Cautionary Tales. In: Lane J. E. (ed.), *Building a Smarter University: Big data, Innovation, and Ingenuity*. Albany: SUNY Press. Chapter 2.

Texas Commission on Law Enforcement. (2021) *Out of State Service/Training Credit or Peace Officers… Application* [Online]. Available at https://www.tcole.texas.gov/sites/default/files/FormsAppsPubs/Service%20and%20Training%20Credit_11.30. 2021.pdf [Accessed 5 December 2021].

Wilkinson, A. (1998), 'Empowerment: Theory and practice.' *Personnel Review*, 27(1), pp. 40-56. https://doi-org.echo.louisville.edu/10.1108/00483489810368549