Athens Journal of Sciences 2026, 13: 1-13
https://doi.org/10.30958/ajs.X-Y-Z

Community Engagement in Cybersecurity, Pervasive Computing and Democratic Use of CYb

By Michael M. Losavio, Avni Istrefi± & Shaban Bajrami•*

Community engagement practices can support effective cybersecurity and promote public safety and security. The foundations of Democratic Cybersecurity promote effective competent and safe use of computing systems across society and to all of its people. A failure to introduce general competencies with fundamental security principles of cyber systems increases the risk of damage to their effectiveness and potential injuries that may result from cyber system breach. We consider the means to mitigate these risks, and examine models for such action, in the contexts of the United States and the Republic of Kosovo and detail successful frameworks for implementation by all communities.

Keywords: *community, engagement, democracy, cybersecurity*

Introduction

Research Question: Can community engagement and the involvement of citizens in cyber security practices strengthen democratic cybersecurity in a world of growing threats and pervasive computing?

Integration of workforce education, criminal justice, and computer engineering applications can effectively establish better cybersecurity as a community-driven effort. Interrogating current programs and practices permits an identification of successful and replicable frameworks and propose innovative pathways for future development with a public cyber safety focus. Key initiatives include pioneering collaborations with a variety of groups to enhance cybersecurity education and training pipelines. It is vital to emphasize the role of workforce development in preparing skilled professionals, criminal justice frameworks of public integrity and safety, and engineering perspectives in designing resilient systems and practical solutions. These collaborations begin by outlining strategies for implementation, evaluation frameworks, and the potential for future programs, aiming to inspire interdisciplinary approaches and actionable solutions for strengthening national cyber defense and resilience.

*Associate Professor, University of Louisville, USA.
±Head, External and International Relations Division, Kosovo Academy of Public Safety, Ministry of Internal Affairs, Republic of Kosovo.
•Head, Curricula and Testing Division, Kosovo Academy of Public Safety, Ministry of Internal Affairs, Republic of Kosovo.

Literature Review

Buckland et al. (2015) analyzed the special challenges of trans-border cybersecurity and the democratic governance concerns in addressing this:

> Cyber security encompasses borderless challenges, while responses remain overwhelmingly national in scope and even these are insufficient. There are enormous gaps in both our understanding of the issue, as well as in the technical and governance capabilities required to confront it. Furthermore, democratic governance concerns – particularly regarding control, oversight and transparency – have been almost entirely absent from the debate. These concerns are exacerbated by the enormous role played by private actors (both alone and in cooperation with governments) in online security of all types. Given the pace at which states and private companies are reinforcing online security and preparing for cyber war, addressing democratic governance concerns has never been more pressing (Buckland et al. 2015, p. 7).

Ismail et al. (2024) surveyed cybersecurity activities in education and curriculum design, noting the challenge in workforce development for cybersecurity; they found a variety of challenges for educational institutions when designing effective cybersecurity activities and curriculum. Earlier estimates found as many as 1.8 million vacancies in cybersecurity-related positions in the United States along (Alhamdani 2019, Morgan 2015). They focused their surveys on needs within pre-university and university training, including training for teachers in those domains; this ranged from high-level technical skills to cybersecurity awareness and education campaigns. The latter includes the "Stop.Think.Connect" training where "This online awareness and education campaign emphasizes that cybersecurity is a shared responsibility for all who benefit from cyberspace. It encourages everyone to take a moment to stop and think about the potential threats in cyberspace."

Such expansive initiatives are supported by the National Initiative for Cybersecurity Education supporting education and training across all levels (Crabb et al. 2024). This mirrors similar initiatives such as that of the UK, "National Planning Policy Framework (2011)[1]. The "UK Cyber Security Strategy Protecting and promoting the UK in a digital world,"[2] emphasized the importance of this, directing that the UK "…conduct research on how to improve educational involvement with cyber security significantly at all levels – including higher education and postgraduate level." But this also includes a focus on prevention and public awareness, including "Look at the best ways to improve cyber security education at all levels so that people are better equipped to use cyberspace safely." In this the UK government partnered with private technology companies such as Microsoft and Symantec and major commercial operations such as HSBC ad Paypal.

Kerrick et al. (2024), Losavio (2025), Losavio et al. (2022) have argued for the need of a new way of approaching cybersecurity and cybersecurity skills through a

[1]Department for Communities and Local Government. *Draft National Planning Policy Framework: Consultation*. July 2011. GOV.UK.
[2]Department for Communities and Local Government. Draft National Planning Policy Framework: Consultation. July 2011. GOV.UK.

"democratic" model that directly engages people engaged with such systems. They note the effectiveness of the Cybersecurity Academic Excellence certification program for promoting this:

> The United States needs a new paradigm in the development of cybersecurity knowledge and skills, one that democratizes them for all people. The Cybersecurity Academic Excellence (CAE) model is one effective foundation that can be expanded to accomplish this democratized effect for a distributed model of cybersecurity. Options for this expansion use cybersecurity teaching projects across multiple domains include workforce skills training. Those domains range from computer science, engineering, human development and learning, and law enforcement, integrating the fundamental computing skills curricula of both middle and high schools as well as postsecondary studies in non-computing areas, from psychology to the humanities. This integrated approach is the essence of democratic cybersecurity.

This has been implemented and tested at several levels and disciplines, including:

1) Health care professionals.
2) Military staff and families.
3) Law enforcement officers.

These reflect the need argued by Grzegorzewski et al. (2023) that in a world of ubiquitous connections cybersecurity, as everyone's responsibility, needs a whole-of-society approach in cybersecurity, as detailed in their "Civil Cyber Defense - A New Model for Cyber Civic Engagement."

Similarly, Powazek and Menna (2025) argue this is needed if cybersecurity is to be sufficiently effective, that a "co-responsibility model" for cybersecurity detailing responsibilities of communities and special actors.

There is broad sentiment that the means by which any community or any nation approaches cyber security must include all of the Community. In the United States there is grown support for expanding cyber security skills in more and more disciplines to more and more people. This ranges from law enforcement and health care professionals to teachers, students and their families.

Methodology & Prior Work

We must consider the needed elements for an outline of a program for a basic cybersecurity program of four to five courses to promote democratic cyber security that are achievable in a reasonable period of time. A practical cybersecurity program should provide basic computing, programming and cybersecurity skills needed for the modern workplace, as well as in the home. For criminal justice in particular, this

knowledge is essential for democratic cybersecurity for the United States and other countries, such as Kosovo[3].

The research methodology to be used begins with an examination of prior and current programs for distributed, democratic cyber security, identifying key elements of each and conception of future models for implementation and testing.

That examination indicates that a fundamental course program addresses that need can be designed and implemented. Should students wish to go further in these studies, these courses map to curriculum in computer science departments such as those in science, engineering and mathematics departments[4]. There are similar curricula in other parts of colleges such as the business school.

Those five fundamental three-hour courses are:

1. Cyber Fundamentals – This course covers core computing and cybersecurity terminology and concepts and discusses current challenges and threats faced by individuals, organizations, and nations using current topics, case studies, and hands-on labs.
2. Cyber Applications - This course covers core computing skills for the workplace, from standard work applications to basic scripting and programming.
3. Programming Languages - This course introduces programming logic and constructs in Python and basic command line scripting in Linux and Windows environments. Arithmetic operators, logical operators, functions, classes/objects and other elements are covered in Python with possible examination of C++ and R.
4. Cybersecurity Fundamentals - This course covers and expands on core cyber security terminology, concepts, and challenges through case studies and discussions. Application to government, commercial and consumer environments will be a focus with hands-on exercises in areas such as network/device security hygiene, search techniques, incident response, and risk assessment.
5. Digital Forensics and Crimes Involving Computing - This course teaches students how to prepare for incidents, how to respond to incidents and investigate them, and how to reliably collect digital data and evidence from various types of storage media and sources of volatile data.

University of Louisville Computer Science Students - One Effort at Implementation that Incorporates These Elements

Any such implementation requires evaluation and systematization and should include a culminating experience/community engagement component relating to computing skills and services relating to less technically advantaged populations, such as handicapped, refugees, juveniles, low-income or senior citizen communities. It must

[3]The University of Louisville has been very successful in securing grants for cybersecurity training for various cadres, from military to law enforcement. The Kosovo Academy for Public Safety has secured access to instructors for its police officers in these cybersecurity areas.

[4]https://catalog.louisville.edu/undergraduate/minors/computer-science-minor/.

review and evaluate the benefit to learners and the community of current *ad hoc* community engagement components in computer science and computer engineering departments and discuss ways to systematically continue and promote these components.

Under a program in the department of computer science and engineering of the Speed Engineering School of the University of Louisville, over the course of a Fall or Spring semester, students trained and mentored community residents in a variety of computing and cybersecurity skills. The learners included students at Simmons College, the senior citizens of the Portland Plaza HUD senior citizens facility in the Portland neighborhood and individuals, some elderly or with disabilities, of a New Directions Housing St. William's center, to access the Internet for communication, information, socialization and communication services.

Computer science students worked with community members on skills and practices for the effective and safe use of the Internet for a variety of services. It presented students with the human factor in computing and issues of how to overcome some of the limitations on the use of computing by segments of the population. The effective and safe use of search was a key skill, along with the effective and safe use of email in the increasingly treacherous online environment. Connection with family was especially important; internet telephony applications allowed the learners to communicate with family all across the country and world without extra fees, a particular burden for people on fixed incomes.

The students generally found the experience worthwhile; the work connected their advanced skills back to individuals who may be using the technology, particularly those with minimal skills with digital technology. Those skills ranged from safe operation of computing and internet systems to technical development to make systems operational for the learners, such as writing device drivers for systems and installation and implementation of new wireless networks.

The people trained were appreciative of the help, especially in areas they were unable to address due to their lack of knowledge or skill. This was a particular issue for elderly and handicapped individuals with no prior experience with these systems. A hallmark case was setting up teleconferencing software to let them connect with family members despite having poor transportation options. The benefits of teleconferencing included connecting with family members in the military who were stationed abroad, but even applied to family members located elsewhere in the state and country.

The program was operational for over fifteen years, with hundreds of students and community members benefiting from it. Once the course was moved online it became more difficult to operate and the community projects ended in 2024.

Kosovo Academy for Public Safety - Evaluating Transnational Applications of Community Engaged Cybersecurity in Kosovo

The Kosovo Academy for Public Safety (KAPS) began a project to develop cybersecurity training of law enforcement in 2019. This project aimed to develop a cybersecurity shield against IT threats to law enforcement and security of the nation of Kosovo, threats both internal and external. The primary challenge was lack of

knowledge and awareness of cybersecurity by its local law enforcement. That would be remediated by cybersecurity training at multiple levels. These skills would also serve to prepare law enforcement for investigation and prosecution of cybercrime perpetrators.

The objectives of this project as set out in the proposal were:

1. To develop a cyber security capacity for Kosovo law enforcement agencies, including police, customs, corrections, probation, police inspectorate, and emergency management.
2. To develop a cyber security certificate program for professionals working in the law enforcement and IT security fields to train them in protection and mitigation of cyber-security crimes.
3. To offer seminars and workshops to law enforcement to make them aware of the dangers of cybercrimes and provide them knowledge to protect themselves and their agencies.

KAPS asked for the assistance of University of Louisville faculty to visit the academy for two-week periods to develop these objectives through planning, implementation and evaluation. This visit was supported by the US Embassy and via the Fulbright Specialist program administered by World Learning, a State Department contractor. These two-week periods would be separated by 4 to 6 month implementation periods by Academy personnel. These implementation periods and new visits by the specialists would permit development and training of law enforcement on cybersecurity, evaluation of the training and expansion of train-the-trainer programming for new instructors and overview programming for new audiences in the Public Safety and security community.

1) Academy Working Group, Prior Work, Project Outcomes

The KAPS working group for the cybersecurity project consisted of:

Shaban Bajrami, Acting Director of Department for Training and Educational Support
Abaz Ahmeti, Head of Training Division
Sami Zeka, Director of Department of Information Technology
Avni Istrefi, Head of International and External Relations
Mirnje Mernica, interpreter for the group
Skender Agaj of External Relations and
Muhamed Gerxhaliu, an IT consultant and instructor at Rochester Institute of Technology/American University of Kosovo volunteering on the project and providing technical support and guidance on the project.

The working group was supported in its efforts by Kastriot Jashari, director of KAPS and Emin Uka, head of Quality Assurance/Accreditation for KAPS[5]. An

[5]KAPS is accredited by the International Association of Directors of Standards and Law Enforcement Training (IADLEST) of the United States of America, which is supported by the US Bureau of Justice

outline of the course modules, objectives and topics and bibliography was developed to guide curriculum development; it considered, *inter alia*, of lesson plans for legal and computer forensic modules, review of IT basics, information security and network security modules.

The Academy structured its curriculum development on contemporary adult learning principles and formats. These formats progressed from topics to learning objectives, directed content, and finally training techniques in order to engage all learners across multiple learning modalities. The course outlines required delineation of:

1. Lesson duration
2. Means of concretization/presentation
3. Lesson goal
4. Lesson objectives
5. Introduction to the lesson
6. Delineation of each lesson objective with bibliography
7. Exercises, particularly those requiring hands-on engagement of the learner
8. Culminating Project/Exam for Assessment of the learner
9. Lesson summary
10. Reference materials
11. Appendices

Prior work on cybersecurity training for local law enforcement in the United States was reviewed with the working group. Based on this, a needs assessment survey for Kosovo law enforcement was developed and will be distributed. A preliminary set of topics based on the US experience was settled upon and used to design course plans for each of those topics based on the adult learning models of the academy.

The preliminary topics for the courses/course outlines for the basic series were:

- IT fundamentals
- Information Security
- Network Security
- Computer Forensics
- Legal/Ethical issues

Draft course outlines and lesson plans for all five Basic topic areas were completed by the University of Louisville faculty and Muhamed Gerxhaliu, the instructor at Rochester Institute of Technology/American University of Kosovo. Mr. Gerxhaliu of RIT/AUK provided key support for the project, including development of course plans in IT Basics, information security and network security. Funding to hire instructors, possibly including Mr. Gerxhaliu and his fellow instructors at RIT, would assure continuity of teaching in these areas.

Assistance of the US Department of Justice (See https://www.iadlest.org/, accessed 18 December 2022).

Sami Zeka, the director of IT for KAPS, configured a 30 seat computer laboratory to serve as a teaching space for the law enforcement learners. Challenges may include access to the appropriate teaching and analysis software beyond open source materials.

An exemplar of the draft course for Computer Forensics/*Forenzika Kompjuterike* and an exemplar of the draft course for Legal Issues with Cyber Security/*Çështjet ligjore me siguri kibernetike* were completed for use and guidance.

The working group planned to continue with course development with cybersecurity, subject to resources. This included development of advanced courses in cybersecurity and digital forensics. Access to industry-standard training resources would be helpful, although not budgeted for at this time.

2) KAPS Orientation and Assessment

As part of an orientation program, University of Louisville faculty gave a series of presentations on the results of US efforts in this area of cybersecurity for local law enforcement. The project included a series of seated and online presentations on the prior work and outcomes for law enforcement cybersecurity training. These provided overviews of training, cybersecurity modules and materials by University of Louisville faculty.

Dr. Cheryl Purdy discussed teaching Computer Forensics and IT Basics. Dr. Purdy teaches at several colleges on issues and practices relating to computer and digital forensics. As a sworn deputy sheriff, she testifies on digital evidence in criminal prosecutions. Computer engineering professor Dr. Adrian Lauf presented on Information Security, Network Security and the construction of virtual cybersecurity laboratory environments using ProxMox on secure multi-processor cluster[6]. The head of the University's Office of Industry Research and Innovation, Dr. Adel Elmaghraby, presented on the development and implementation of a comprehensive cybersecurity discipline in the organization. Topics covered included collaboration with industry and the academy, from training to advanced research projects. Criminal Justice department chair Dr. Thomas Hughes discussed the creation and implementation of law enforcement training and academic teaching programs geared towards managing innovation and changing policing. This discussion included resources offered through the University's Southern Police Institute (https://louisville.edu/spi) and the Department of Criminal Justice (https://louisville.edu/justice).

Additional online presentations by University of Louisville personnel working in this space are being developed. Presenters may include Dr. Jeff Sun and Dr. Sharon Kerrick of the College of Education and principal investigators on two IT cybersecurity training initiatives, and Mr. Mike Bassi, director, and Dennis Hippert, deputy director, of the Southern Police Institute of the University of Louisville.

An overview of training for prosecutors on cybersecurity and work with law enforcement was also presented. This would aid in the coordination between police and prosecutors on cybercrime investigations. This may be particularly important under civil law regimes where that coordination is more extensive than under the Anglo-American model.

[6]See https://engineering.louisville.edu/faculty/adrian-p-lauf/.

3) KAPS Beta Test Cohort

At the end of the two-week project closing Beta presentations on cybersecurity were done for about 30 Kosovar students of the Kosovo Academy for Public Safety from criminal law and psychology classes. These learners ranged in police rank from lieutenant to patrol officer and were assigned to intelligence, analysis, patrol and investigation. The group included correctional officers and a customs/immigration officer. Their studies were advanced beyond primary officer training and directed towards degrees in the bachelor's program of the Academy.

The presentations were disrupted towards the end due to outbreaks of communal violence; about half the class were call back to duty to address this.

Almost uniformly they were deeply engaged in the sessions, including discussion on outreach to communities to improve cybersecurity. There was a special concern for the cyber-safety of the elderly and the safety and habits of juveniles in this area. The officers opined that this was training of value to them.

The consensus for these officers was that this training is needed by Kosovo law enforcement, and the citizens of their republic, with a special concern about juveniles and their actions online.

Discussion

The participating students and learners agreed that the training was beneficial to them and their communities. Even as presenting new technical skill areas outside of traditional law enforcement training, the learners found them valuable when mapped to contemporary conditions. Those conditions found in public security and community life of the hyperconnected world of ubiquitous and pervasive computing presented new areas of vulnerability for the peoples of the community.

The need for such security for computing is seen in the repeated, effective attacks on cyber resources in all domains. It is particularly critical with the expansion of cyber systems to all areas of society. A "democratic" cybersecurity regime addresses that pervasive risk.

College and Community

The need for pervasive cyber security for pervasive computing offers useful and important engagement in the community to devise and implement the needed skills. These skills range from the technical to the personal importance of individuals acting safely with computing. The collegiate student community cybersecurity trainings by computer science and engineering students were of benefit to both the students and the community members.

For the students it was an introduction, re-introduction and reminder of the human-centered elements in effective and secure computational systems that directly interface with members of the community. For the community members it offered access to computing technologies and the knowledge for safe, competent use to

which they had little or no prior exposure. This opened to them the connection to a wider world that enriched their lives, with knowledge of some of the dangers involved and the means to avoid those dangers.

Kosovo Academy for Public Safety

The Kosovo Academy for Public Safety (KAPS) began its project to develop cybersecurity training of law enforcement in 2019. Delayed by the COVID-19 pandemic, recruitment of expert support began in Fall, 2022. The supporting University of Louisville faculty visited for two weeks in November – December, 2022, in person and online, with the KAPS working group. That working group developed an outline of the curriculum; a set of course plans for IT fundamentals, Information Security, Network Security, Computer Forensics and Legal/Ethical issues, that served as the foundation for the project.

The progress on this project in a very short time was remarkable. The Kosovo working group accomplished far more in that short time than anticipated, creating a foundation to quickly implement training and assess the outcomes. The preliminary beta test of the course material with a heterogeneous group of law enforcement indicates that this is both needed and would be welcomed. These findings should be interested with caution as these learners are a self-selected group of law enforcement officers seeking to advance their education and training beyond that needed for their positions As such they may be especially predisposed towards new learning in advanced areas.

Nonetheless, in both the significant progress made by the staff and positive response from the learning group of law enforcement officers, this project demonstrates a great deal of potential to improve the current and future safety of the people of Kosovo.

Comparison of College/Community and KAPS

Although each project had distinct training groups and professions, with different target beneficiaries, they both shared common outcomes:

1) Both groups, college computer engineering students and state/local law enforcement personnel, found the training of value for themselves and their respective professions.
2) Both groups noted the needed benefits for the people of their communities.

    a. For the college students it related back to their ethical and social obligations for good and safe computing, including their awareness of the needed for systems to reflect the skill level of the target users.
    b. For the law enforcement officers it related to their general goal of protecting their civilian populations and then to specific problems they had seen during law enforcement protection and investigation actions, especially as to juveniles.

3) Both groups supported continuing such training and community engagement relating to computing for the benefit of their professions and their communities.
4) Completion rates were 100% for both groups, although for the learners this was due primarily due this participation of the students/learners being required; community participants also generally completed their sessions, motivated by the value of the new topic they were being taught.

Community engagement beyond classroom learning correlates with improved success rates in the cyber security cohorts. This may be due to overall special components of community engagement. It may also be due to the special value community-based learning offers in connecting learning to immediate, practical and tangible benefits for both the learners and the community benefited.

First, by making learning immediately relevant to agreed goals, particularly the protection and security of people, the students realize their success is more than academic exercises but work that directly impacts people. They become responsible for more than just their grade assessment but also for the safety and wellbeing of others.

Second, this demonstrates that the complexity of human-cyber interactions must be considered, not just the solution of a technical problem. Goal-oriented students want to succeed and meet the goal; showing that complexity lets them know all they must address to succeed with an effective cyber security situation.

Lastly, the messiness of many human situations, especially as to cyber security, has become a valuable teaching and learning tool for successful implementation of any effective computing system beyond academic exercises. It demonstrates the need for cyber security and any functional analysis to expand well beyond immediate technical issues to embrace those messy and complex conditions – technical and social- and address them before people, possibly many people, are hurt. The injuries from the disruption of the security of people's homes, health, finances and families can be immense where those lives are touched by cyber systems.

Conclusion

These models serve as templates of means to promote greater effective cybersecurity throughout society. They are hallmarks of "democratic cybersecurity" where the practices and skills needed for secure computing are distributed along all tiers of society. These foundational lessons in cybersecurity should be portable across all jurisdictions, particularly due to common engineering elements in operating systems and the Internet and common use elements and vulnerabilities across cyber systems.

There is a critical general distributed need for such cyber security skills in our diverse communities as all embrace pervasive computing. A cyber-attack against Kosovo's neighbor Albania by the Islamic Republic of Iran is a harbinger of dangers to come.

The college students' and Kosovo law enforcement's efforts in expanding cybersecurity through traditional public security helped their communities. They can guide others in the protection of people in our ubiquitous, pervasive computing world. And that protection is sorely needed.

Acknowledgments

This work was supported by the University of Louisville, US Fulbright Commission and World Learning.

References

Alhamdani WA (2019) Adopting the cybersecurity curriculum guidelines to develop a secondary and primary academic discipline in cybersecurity postsecondary education. *Journal of Cybersecurity Education, Research and Practice* 2019(1): 2.

Buckland B, Schreier F, Winkler T (2015) *Democratic Governance Challenges of Cyber Security*. DCAF HORIZON 2015 Working Paper. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

Crabb J, Hundhausen C, Gebremedhin A (2024) A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education,* volume 1, 241–247.

Grzegorzewski G, Smith M, Koven B (2023) Civil Cyber Defense – A New Model for Cyber Civic Engagement. *The Cyber Defense Review* 8(3): 51–66.

Ismail M, Thorakkattu Madathil N, Alalawi M, Alrabaee S, Al Bataineh M, Melhem S, et al. (2024) Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports* 16(Dec): 100501.

Kerrick SA, Sun JC, Elmaghraby A, Losavio MM (2024) CAE Models for the Expansion of Cybersecurity Knowledge in the U.S. *Technology Interface International Journal* 25(1): 34–39.

Losavio MM (2025) Security and Privacy in Ambient Intelligence, the Internet of Things and Pervasive Systems: Interrelationships for Systems of Public Safety. In *Future of Information and Communication Conference*, 678–687. Cham: Springer Nature Switzerland.

Losavio M, Sun JC, Kerrick S, Elmaghraby A, Purdy C, Johnson C (2022) Integrating democratic cybersecurity: Empowerment of traditional law enforcement and democratic public safety. In RP Griffin, U Tatar, B Yankson (eds.), *17th international yearbook on cyber warfare and security*. Academic Conferences International, Ltd.

Morgan S (2015) Cybersecurity job market to suffer severe workforce shortage. *CSO Online* 28.

Powazek S, Menna G (2025) *The Roadmap to Community Cyber Defense: A Path Forward from the Cyber Resilience Corps*. Available at: https://cltc.berkeley.edu/publication/roadmap-to-community-cybersecurity/.