2020

Cyber-Informed: Bridging Cybersecurity and Other Disciplines

Char Sample
Boise State University

Sin Ming Loo
Boise State University

Connie Justice
Indiana University at Purdue

Eleanor Taylor
Idaho National Laboratory

Clay Hampton
Indiana University at Purdue

Cyber-Informed: Bridging Cybersecurity and Other Disciplines

Char Sample[1,2], Sin Ming Loo[2,1], Connie Justice[3], Eleanor Taylor[1] and Clay Hampton[3']
[1] Idaho National Laboratory, Idaho Falls, USA
[2]Boise State University, Idaho, USA
[3]Indiana University at Purdue, Indianapolis, USA
Charmaine.Sample@inl.gov, Eleanor.Taylor@inl.gov
smloo@boisestate.edu
cjustice@iupui.edu, cthampton@iupui.edu
DOI: 10.34190/EWS.20.092

Abstract: A recent study by Cybersecurity Ventures (Morgan 2018), predicts that 3.5 million cybersecurity jobs around the world will be unfilled by 2021. In the United States, the demand for professionals with cybersecurity expertise is outpacing all other occupations (NIST 2018). These reports, along with many others, underpin the need for increasing workforce development initiatives founded in cybersecurity principles. The workforce shortage is across all cybersecurity domains, yet problems continue to persist, as the lines between combatants and non-combatants are blurred. Combating this persistent threat, which is a 24/7 operation, requires a more aggressive and inclusive approach. Higher education institutions are positioned to fully support cybersecurity workforce development; cybersecurity needs people with different perspectives, approaches, ways of thinking, and methods to solve current and emerging cyber challenges. This need is especially pressing when assessing the digital landscape — a tireless and ever-expanding connectivity supported by societal needs, and economic development yet compromised by the common criminal to nation-state sponsored felonious activity. Educators need to consider augmenting their approaches to educating students to include cybersecurity content. In this technology forward world, one that is expanding more rapidly than society and policy can react, increases the imperative for fundamental cyber defence skills. Accordingly, all students, no matter the major, should, minimally, understand the implications of good versus bad cyber hygiene. STEM graduates will require awareness of cyber issues that impact the security of programs, systems, codes or algorithms that they design. Operationally focused cyber-security graduates require a curriculum for careers dedicated to protecting and defending cyber systems in domain specific environments. In a world of Internet of Things (IoT), the ability for individual disciplines to understand the impact of cyber events in environments outside of traditional cybersecurity networks is critically important. This will provide the next generation defenders with domain specific cybersecurity knowledge that is applicable to specific operating environments.

Keywords: cybersecurity curriculum, workforce development, cybersecurity curriculum design, cybersecurity degrees

1. Introduction

The warnings for the cyber-workforce shortfall have been sounded for years, yet the gap continues to grow (ISC2 2019, NIST 2018) Cybersecurity Ventures (2019) recently predicting a 3.5 million worker shortfall. The growth of the Internet of Things (IoT) (Morgan 2018) promises to exacerbate this problem. In general, the future digital landscape promises increasingly more complex cyber-attacks from criminals to nation-state actors making basic cybersecurity hygiene the responsibility of all users not just the cybersecurity indoctrinated.

In addition to the cyber workforce development gap, a divide between technology savvy citizens and their counterparts is also noteworthy. This coincides with the introduction of technology courses in the public-school system (Blazer 2008), along with the popularity of newer technologies, the ubiquitous use of devices, and proliferation of social media and mobile apps. A recent Pew research survey (2018) found that more than nine-in-ten teenagers, 13 to 17, reported owing or having access to a smartphone and almost half reported being on-line on a near constant basis. Technology adoption rates have soared across the US (Ritchie & Roser 2019) and serve to illustrate the need for greater cyber awareness and proficiency (aka cyber hygiene). As more of the population becomes cyber-aware, cyber hygiene knowledge could potentially address the cybersecurity skills gap while introducing different disciplines to cybersecurity.

The past 10 years Internet enabled home electronics sales increased making possible the ability for many home users to become unwitting accomplices in cyberattacks. In 2017 there were approximately 8.4 billion connected internet of things (IoT) with well over 20 billion predicted in 2020 (Gartner 2017). IoT devices such as thermostats, smart TVs, and appliances, offer greater convenience by leveraging an Internet connection, but at the cost of granting access to uninvited guests. Most users remain unaware of basic security settings on their Wireless Access Point (WAP), or the firewall settings provided by their Internet Service Provider (ISP) and how to modify these settings. For example, the re-purposing of IoT devices into bots for botnets creates an

inadvertent increase in installation base and scale through IoT device default set-up increasing vulnerabilities, and opportunities for malicious attacks.

Widespread IoT deployment presently, and for the foreseeable future, supports the argument that cyber proficiency is as important as reading. In cybersecurity terms, our education system fails to keep up in the age of IoT. While adoption rates of apps and the latest incarnation of technology remains healthy, few have the deep understanding of how these products actually work, and the security ramifications of using these products in their native installed state (Lorenz 2020). Consider the outrage over Facebook's selling of personal data (Isaak & Hanna 2018), Amazon's application of AI/ML to use personal data to sell more products (Levy 2018), the Marai botnet attack using open ports and default passwords (Antonakakis 2017) and most recently the Zoom hacking (Lorenz 2020). These examples underscore the need for a curriculum of cybersecurity for non-professionals training.

The need to introduce cybersecurity into other disciplines is well documented (LeClair 2013; Henry 2017), the problem is in the details of "how" to do so. Efforts to integrate various disciplines and cybersecurity have had mixed results, suggesting that while the general idea has merit, the implementation may have faults. Boise State University (BSU) and Indiana University at Purdue (IUPUI) are two institutions in a growing number that have recognized the need for cybersecurity to extend beyond the traditional academic silo and make teachings available to wider audiences. What follows is a review of the experiences of two universities in extending cybersecurity beyond the traditional academic disciplines to develop a more interdisciplinary and inclusive approach which include, but are not limited to, computer science and engineering.

2. Background

Fundamentally, any digital system can be "hacked" by a persistent adversary and is often only bound by the imagination of the attacker and creativity of the defender (Carey and Jin 2019). As these events continue to gain complexity and sophistication, a cyber informed approach across several disciplines may increase both the skill and size of the future workforce. Much like the move to remote work resulted in many institutions adding Microsoft Office courses and certifications, the interdisciplinary nature of cyber security suggests a need to educate the masses in a similar fashion and approach, from introductory and basic usage through advanced and expert levels.

Introducing cybersecurity education into existing curriculum offers the opportunity to increase the number of cyber-aware workers in the workforce. In doing so, the workload decreases on cybersecurity professionals, and an additional potential outcome is attracting non-traditional majors to cybersecurity, especially as cybersecurity definitions continue evolving and expanding from STEM domains into other domains. Although challenges remain at universities for students, as course catalogues can be difficult to navigate, prerequisites can create barriers to entry, especially across colleges within the same system, and inabilities to identify or track extracurricular learning opportunities (Cybersecurity Curricula 2017).

The skills gap remains and there is currently no viable way to fill the demand without addressing future university curriculum and workforce development training processes. Meeting this challenge requires strategic education efforts to create a foundation for a broader talent pipeline in support of the needs facing industry, government and academia. The objective is not only to create awareness and interest in cybersecurity careers but also to develop and deliver cyber hygiene courses across universities and community colleges and increasing workforce development training while providing the community at large with tools and resources, to significantly increase education and training aligned with cyber objectives and career paths.

The current approaches to cybersecurity are not sustainable, scalable, or anticipatory (Borg 2018). The rapid adoption of digital technology, IoT, the promise of 5G, and integration into a vast and often unrecognized communications web will eclipse existing methods to identify and mitigate cyber risks. These factors drive the urgent need for expanding the cybersecurity talent pool, for addressing current needs, future innovations and protecting critical infrastructure.

Attaining digital safety in this increasingly connected world, requires problem solvers with different perspectives, approaches, ways of thinking, and methods (Nisbett 2010; LeClair 2013). The solution cannot be a purely computer-based curriculum approach. Historically, cybersecurity workforce preparation came from

computer science and information technology majors, yet many industry leaders (i.e. Cliff Stoll, Dan Geer and Radia Perlman), do not have degrees in Computer Science or Cybersecurity. In fact, a gap exists between materials covered and field requirements. Computer Science is algorithm focused and IT courses are designed to train students to run and/or manage IT systems. Cybersecurity requires broader knowledge on protecting information, technology, processes and people.

There are several cybersecurity professionals, without computer science and information technology degrees, that have found their way to the discipline through informal methods and have learned the required skills and received the formal certifications as they progressed in their careers (Tribe of Hackers1, Tribe of Hackers2). Cybersecurity is multidisciplinary and benefits from a workforce of various majors across a university campus, expanding cybersecurity into holism and creating proactive problem solvers. By pushing the boundaries of a traditional STEM-based approach, with the goal of leveraging the learning environment and endorsing critical thought across all disciplines, students can learn valuable insights from each other. Borg (2018, p.2) discussed the perspective issue providing evidence that an over reliance on STEM courses can be detrimental leaving students "less equipped to do cyber security well".

Creating this new course curricula requires a true mix of disciplines where cybersecurity concepts can be shaped and shared in environments beyond traditional computer networks, where other data, beyond cyber event data, shapes the narrative. In this environment, students will learn comprehensively about cybersecurity with an operational as well as an informational focus covering information assurance, security operations, forensics, and disaster recovery — while providing the foundational knowledge needed to become a cybersecurity leader. Preparing the next generation of cybersecurity professionals with the necessary skills, requires continual investment in all areas of cybersecurity research, education, training, communication and outreach. This effort complements the work being supported by other education institutions; thus, combining our forces to help meet the ever-increasing cybersecurity workforce needs.

Cybersecurity is more than a technology solution, the discipline reflects the interactions of humans, machines, and networks. Cyber-safety prevails when human factors and other disciplines are included in the solution. The lateral thinking needed for cybersecurity is similar to epidemiology, requiring many different areas of expertise to understand the agent, host and environment. Using this metaphor, (Zhang et al., 2014; Zhang et al. 2015), cybersecurity depends on herd immunity - the resistance to the spread of a contagious disease within a population that occurs if a sufficiently high percentage of people are immune to the disease, generally through vaccination, or in this case, education.

Much like the work performed at Cambridge University on inoculating people against fake news (Roozenbeck & Van der Linden 2019), cybersecurity relies on proper training to prevent security breaches. Education and training are proven methods that help inoculate populations from cyber threats delivered through innovative and inclusive, broad programs, two of which are outlined in this paper. At Boise State University, three identified levels reflect general delineations in cyber security including users, operators and full-time cyber security professionals. Another effort to address the diverse needs of the cybersecurity workforce from the Purdue School of Engineering and Technology at Indianapolis, IUPUI, offers courses, a certificate, minors, and concentrations within a degree program to tackle broader demands.

3. Cybersecurity Course Offerings

Education as commonly defined, is the pursuit of "knowledge, skills, beliefs, and habits." [1] Education is a life-long pursuit, and develops skills in critical and strategic thinking, problem solving, and research. Training is singularly focused on a single objective. Upon completion, a specific task or skill is mastered. The learner need not understand the theory behind the skill as long as the student demonstrates task mastery. Education can include training as reinforcement after studying the critical thinking and other components of life-long learning, but the main focus of education is to prepare the learner to adapt to the ever-changing cybersecurity landscape.

The higher educational system provides mechanisms for education and training. Community colleges (CC) or two-year colleges serve multiple purposes, preparing learners for entry into four-year colleges or universities while also offering applied or certificate-based programs that are more task based or skill specific.

Four-year colleges and universities responsibilities are to educate learners, offering bachelor, master and doctoral degrees in support of lifelong learning, research, and critical thinking. The primary goal of higher education is to create a well-rounded learner, proficient in the chosen major, adaptable to new technologies while avoiding the technology specific traps that can come at the expense of rapid technology changes and adoption. Learners who understand the underlying foundation and theory and can think abstractly, and in research terms, will be able to lead in future new solutions.

3.1 Boise State University (BSU)

Boise State offers several certificate programs along with the degree programs, attempting to address the diverse needs of the future cybersecurity workforce (Boise State Catalog, 2020). Boise State observes the needs of three student types in the cybersecurity education; users, operators and creators. These levels are presented in no particular importance and encompass necessary components for student preparation, production and fortification in cybersecurity and the IoT.

3.1.1 Level 1: Cybersecurity for All

A set of courses providing a cyber security knowledge for everyone. The objective is to raise the cybersecurity awareness across the campus. The Cybersecurity for All certification consists of four-courses offering awareness training covering cyber-physical systems (CPS), Internet of Things (IoT), home office security and incident response recovery. These four courses provide a basic understanding of cybersecurity hygiene that is necessary for any Internet user.

3.1.2 Level 2: Cyber Operations

The objective of this operationally focused certificate program is to prepare students by providing industry certification opportunities for those interested in cybersecurity as a career. Students are trained to think critically and develop strong problem-solving skills that can be applied to understand and solve data-driven cybersecurity problems. This certification requires the student to demonstrate proficiency in four courses that cover information assurance with critical thinking, cybersecurity foundations, cyber operations and cyber forensics with recovery. In addition to certification training, this course offering covers gaps not addressed in many industry certifications thereby developing students capable of solving new problems that appear in the cyber domain as well as being able to translate those skills into other domains. This certification consists of twelve credit hours and includes: information assurance, applied critical thinking, offensive security, defensive security, recovery and forensics while requiring one industry security certification. The program includes a multidisciplinary group exercise designed to apply the lessons learned in the courses to a real-world setting requiring both technical and interpersonal skills (McChrystal 2015, Lencioni 2002, Lencioni 2016).

3.1.3 Level 3: Cyber-Informed Engineering

A set of courses that provide cyber-informed engineering skill sets with the objective is to educate the future engineers and scientists to incorporate cybersecurity (as a requirement) into the design process for more resilient systems. In order to protect against cyber threats, the course developer(s) require awareness of the system being designed (software, hardware, firmware, control systems etc.) in addition to understanding different ways in which an adversary can compromise the system through denial, deception, disruption, destruction and deterrence. The courses teach countering compromise through robustness, resilience and other methods to design security controls into a system that meet performance criteria and enhance protection, hence the broad interdisciplinary knowledge requirement. This program was introduced in August 2018 with an introduction course in cybersecurity. Other cyber contents are incorporated into existing STEM courses.

3.2 Purdue School of Engineering and Technology Indiana University-Purdue University Indianapolis (IUPUI)

The Purdue School of Engineering and Technology, IUPUI, offers courses, a certificate, and minors, and concentrations within a degree program that attempt to address the diverse needs of the cybersecurity workforce (IUPUI Catalog 2020).

3.2.1 Level 1: Information Security Specialty

A minor that provides a cybersecurity background for everyone. The objective is to raise awareness of cybersecurity across different disciplines throughout campus. The minor consists of four courses that offer base knowledge in computer architecture and data communications. Additionally, the minor consists of a cybersecurity awareness foundational course that teaches the novice about threats and vulnerabilities on the Internet; how to protect home systems, small business systems, IoT devices, and what to do to recover from an

incident. The end user is the most vulnerable asset to the cybersecurity ecosystem and providing an education to all users, regardless of discipline, will help to protect our cyber domain. The courses are available to the entire campus community for educational purposes with aid in the overall education of the larger community.

3.2.2 Level 2:

The Information security concentration in Purdue School of Engineering and Technology, IUPUI, Computer Information Technology (CIT) program focuses on preparing students with a solid foundation in information assurance and network security. These students gain skills in practicing information assurance data management security by understanding networking and concepts on protecting systems connected to the internet. Below are a few courses available for the concentration:

- The Programming for NetSec class prepares students though "hands on" experience with scripting and programming within the network security realm. These skills are frequently used in future courses or professional career when task automation or script writing can be used to reduce repetitive tasks or job functions that exists as a part of their job duties.
- The Networking Operating System Administration course is designed to engage students to develop a deeper understanding of operating systems and how networked servers' function, as well as introducing the concepts of virtualized environments compared to minimal installs on physical hardware.
- The Advanced Network Security course introduces additional disciplines by analyzing the mentality of attackers and reviewing the Attacker Methodology/Cyber Kill Chain. These viewpoints provide keen insights as to why security is a crucial step in networked systems.
- Digital Forensics course demonstrates the needed skills for a digital forensics career and requisite proficiencies to present evidence that pass legal proceedings standards.
- The IT Risk Assessment course provides an overview of a typical IT risk assessment and audit while teaching students how to give recommendations and reports for IT systems designed to help ensure a safer and more secure environment.

3.2.3 Level 3:

IUPUI's new cybersecurity degree builds off the Information Security concentration and offers the students more involvement in the offensive and defensive aspects of cybersecurity, applying their knowledge to learn more in-depth attacking and defending skills and processes. The Offensive Cybersecurity course enables students to practice and demonstrate concepts in an actual, connected, systems environment. The coursework includes a competition with a complete report on findings including what additional measures might be implemented to help mitigate future incidents, exposures or vulnerabilities.

In addition to the aforementioned courses, development plans exist for a security architecture course with different areas of concentration, including: Industrial Controls Cybersecurity, Cybersecurity Risk Assessment, Defensive Security, and Digital Forensics. These areas of focus would enable a deeper concentration to obtain in-depth knowledge for each related career path, allowing students to tailor their interests to a specific job role or research area post-graduation.

Students must be able to integrate cybersecurity learning with other disciplines. Experimental integrated learning was implemented in two undergraduate STEM courses through cross-curricular instructional units. The courses, Big Data Analytics and IT Risk Assessment, have content connections and were taught in parallel. The goals of this approach were to investigate the effectiveness of cross-curricular integrated instructional units for courses that are content connected and study the effectiveness of these projects based on inquiry levels. These units were integrated to enhance students' capabilities in connecting and transferring knowledge from one setting to another, improve students' understanding of the subjects in the courses and interpreting the larger impacts of information technology. We hypothesize that the hands-on projects will enhance students' interdisciplinary problem-solving skills by connecting knowledge, as well as research experiences and capabilities.

4. Observations on course execution

Higher education has the "build-it they will come" mentality in some cases and in other cases a hyper-response to industry at the expense of vision. Although both problems are very different the end result is oftentimes the same, a failure to graduate intellectually adaptable students capable of solving current and future cybersecurity

problems. Students who have gone through a degree program have neither the thinking skills nor job skills. Student who complete training certifications have specific skills that do not always adapt to novel problems.

One way to solve this problem is collaboration between security industry practitioners and universities. The universities need to work with industry to develop the program and curriculum. Academia offers abstract concepts that encompasses larger problems while industry practitioners (the subject matter experts) provide knowledge of real-world instantiations of those larger concepts. An additional benefit in this approach is that often times industry experiences disruption through technology changes and novel attacks first, this approach allows for greater sharing.

Delivery modes need reviewed. Content consumption in society has changed, academia has not adjusted. The face-to-face delivery as the primary method of teaching should be re-evaluated. Pedagogy favours face-to-face interactions, but andragogy favours "hands-on" exercises. Undergraduate students are young adults and may benefit from the introduction of andragogy techniques mixed with traditional pedagogy. Asynchronous concepts taught online and reinforced with applied laboratory exercises might produce better outcomes. Short-term bootcamp style learning can act as larger integrated lab exercises.

CIT in the Purdue School of Engineering and Technology, IUPUI has a program that combines theory and practice. The Living Lab (LL) allows students to apply networking, cybersecurity, database, website and application development concepts and techniques learned from prior CIT courses to service, internal and/or external projects. The Living Lab emulates an industry IT department in which students work on one or more projects as part of an IT team spending 200 working hours per semester equalling internship credit. The Living Lab provides students an experiential and service IT learning environment. By presenting students with a real production IT environment, enabling the students upon graduation to contribute immediately and directly to their employment workplace. Students solve real world IT and cybersecurity problems with little or no supervision while meeting business standards of managing, documenting and reporting their work via weekly status reports.

LL Statistics showed that from 2008-2020, 569 projects launched, thus, allowing 518 students to gain valuable real-world operational experience. "Hands-on" experience was obtained in the LL that could not otherwise be obtained in business due to risk concerns. The LL provides an example of industry partnership and academia working together to provide reinforced learning of broad academic concepts through real life examples. The LL allows for operational environment immersion, along with cyber-physical security workshops and training in support of IoT security at water/wastewater treatment facilities, and traditional risk assessments

At Boise State University, the Cybersecurity for All, and Cyber Operations, programs will go live in August 2020. The Cyber Informed Engineering program courses have been offered twice in the last two years reaching approximately 65 students representing a wide range of students, motivations and skillsets. The courses have been well-received, and most students have performed well, remarking on an appreciation for the course content and career field opportunity diversity.

However, a recent exercise revealed problems reflecting a lack of self-regulation, constrained mindsets and limited interpersonal skills. A penetration testing hands-on activity, using an air-gapped learning network for practicing lessons in a heterogeneous network consisting of wired and wireless components. Activities include WiFi penetration, network scanning and password cracking. Students were to leave a mark on the Raspberry Pi by using the default userid and password then access to the shadow password file. Leaving this network running for days allowed students to apply classroom lessons learned. However, someone changed the default user password and root password of the Raspberry Pi keeping other students from finishing the exercise, thus providing the educators a learning opportunity. One problem observed was the lack of understanding operating systems such as Linux makes the coursework challenging. For this reason, foundational courses that can be viewed as "how to" classes deserve consideration for cyber initiatives; however, providing the right amount of challenge and support on relevant learning tasks requires further investigation.

Cybersecurity observations from CIT@IUPUI lead to significant program changes. The Information Security and the Network Security Certificate has been taught since 2004., Echoing Boise State, IUPUI also noticed that the students' lack of Linux experience was a detriment in the learning process, particularly in advanced cybersecurity courses such as Advanced Network Security, Digital Forensics, and Wireless Security. In response to this problem IUPUI added Linux modules to earlier 100 and 200 level networking and security courses. Additionally, a 300-

level scripting/programming course using Python and Linux was also added. In all network, security and programming courses instructors are encouraged to standardize on the Linux operating system.

Recognizing other disciplines are becoming increasingly interweaved within cybersecurity, was an additional observation illuminating the need for the CIT program to update our curriculum (Sample & Justice 2018). The CIT program is working with other disciplines on campus to create certificates that will include other aspects of cybersecurity such as law, psychology, sociology, data science, international studies and other areas of study (Sample & Justice 2018). Of particular note, the inclusion of data science may force a marriage of disciplines since the best insights result from subject informed queries.

5. Conclusions

By examining two institutions of higher learning commonalities, differences were also discovered. Both programs continue to evolve in offering interdisciplinary courses that can more effectively address threat analysis and IoT in various environments. Both programs have maintained traditional cybersecurity courses that can be found at most universities and both observed the need for fundamental skills. Both programs offer cybersecurity for non-majors, that teaches basic cyber hygiene and may offer an opening for non-traditional students to ultimately pursue cybersecurity while bringing fresh perspectives that Borg (2018) deems necessary. This outreach can bring a multidisciplinary approach to cybersecurity and open the aperture to a diverse pool of talent, creative problem solvers and critical thinkers that will be an essential part of the solution

Cyber threats will continue to grow in creativity and sophistication as will the demand for a skilled cyber informed workforce capable of protecting and preventing such attacks. Furthermore, the introduction of artificial intelligence promises to disrupt the workplace. Without changes to university curriculum there is no viable way to sustainably address the workforce needs of today or the future. Significant intervention is necessary to build future talent pipelines, expand current capacity and enhance workforce development efforts with skilled professionals who are highly adaptive and capable of solving a wide variety of problems.

References

Blazer, C. 2008. Literature Review: Educational Technology. Research Services, Miami-Dade County Public Schools.

Boise State University Catalog [Online]. Available: https://www.boisestate.edu/registrar-catalog/ [Accessed].

Boise State University Course Catalog [Online]. Available: https://majors.boisestate.edu [Accessed].

Borg, S. 2018. Seven Overlapping Theses On Cyber-Security Education [Online]. Available: https://www.cerias.purdue.edu/nace/papers/Borg.pdf [Accessed].

Brown D. 2019. Your smartphone is 7 times dirtier than your toilet. Here's how to clean it. [online] USA TODAY. Available at: https://www.usatoday.com/story/tech/2019/02/26/your-smartphone-screen-probably-disgusting-heres-how-clean/2950106002/

Carey, M.J. and Jin, J., 2019. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World. John Wiley & Sons.

Cary, M.J., and Jin, J., 2019. *Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity,* Wiley.

Corera, G., 2016. *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*, Pegasus Books.

Cybercrime Magazine. (2019). Cybersecurity Jobs Report 2018-2021. [online] Available at: https://cybersecurityventures.com/jobs/, Visited: March 9, 2020.

Henry, A.P., 2017. Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements (Vol. 4). ACCS Discussion paper Available at: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf

Indiana University – Purdue University Indiana (IUPUI) Available: https://et.iupui.edu/departments/cigt/programs/cit/undergrad/bscit/plan

Isaak, J. and Hanna, M.J., 2018. User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), pp.56-59.

Isc2.org. (2019). 2019 Cybersecurity Workforce Study. [online] Available at: https://www.isc2.org/Research/Workforce-Study

LeClair, J., et al. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, ACM.

Lencioni, P. (2002). The Five Dysfunctions of a Team: A Leadership Fable, Jossey-Bass.

Lencioni, P. (2016). The Ideal Team Player: How to Recognize and Cultivate the Three Essential Virtues, Jossey-Bass.

Lorenz, T., (2020).” ‘Zoombombing’: when video conferences go wrong”, *The New York Times.* [online] Available at: https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

McChrystal, S., Collins, T., Silverman, D., Fussell, C., (2015). Team of Teams: New Rules of Engagement for a Complex World, Portfolio.

McKinsey & Company. (2019). Growing Opportunities in the Internet of Things. [online] Available at: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things, Visited: March 9, 2020.

National Institute of Standards (2018). "New data show demand for cybersecurity professionals accelerating", Available at: https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating

Nisbett, R. 2004. *The Geography of Thought: How Asians and Westerners Think Differently and Why. Simon and Schuster*.

Roozenbeek, J. and Van Der Linden, S., 2019. The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, *22*(5), 570-580.

Sample, C. and Justice, C., 2018. Suggestions for Addressing the Changing Needs of the Cyber Security Workforce. [online] Available at: https://www.cerias.purdue.edu/nace/papers/Sample.pdf

Segal, A., 2015. The Hacked World Order: how nations fight, trade, maneuver, and manipulate in the digital age., New York Public Affairs.

Staff, W. (2018). How Amazon Rebuilt Itself Around Artificial Intelligence. [online] WIRED. Available at: https://www.wired.com/story/amazon-artificial-intelligence-flywheel/

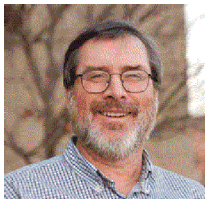
Trend Micro Report. (2019). Into the battlefield: A security guide to IoT botnets. Available at: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets

Zhang, C., Zhou, S. and Chain, B.M., 2015. Hybrid Epidemics—A Case Study on Computer Worm Conficker. *PloS one*, *10*(5).

Zhang, C., Zhou, S., Cox, I.J. and Chain, B.M., 2015. Optimizing Hybrid Spreading in Metapopulations. Scientific reports.

Dr. Char Sample is the Chief Cybersecurity Research Scientist for the Cybercore division at Idaho National Laboratory. Dr. Sample is a visiting academic at the University of Warwick, Coventry, UK and a guest lecturer at Bournemouth University, Rensselaer Polytechnic University and Royal Holloway University. Dr. Sample has over 20 years' experience in the information security industry. Dr. Sample's research focuses on deception, and the role of cultural values in cybersecurity events. More recently she has begun researching the relationship between human cognition and machines. Presently Dr. Sample is continuing research on modeling cyber behaviors by culture, other areas of research are data resilience, cyber-physical systems and industrial control systems.

Pardis Moslemzadeh Tehrani is a senior lecturer at the Faculty of Law, University of Malaya. Her research interests lie in the areas of cyberterrorism, cyberlaw, and international humanitarian law. Pardis's research has been widely published in peer-reviewed journals and she has presented papers at national and international level conferences. She is a member of the editorial review board in several journals. She is also an international scientific member of the Australian and New Zealand Society of International Law.



Richard L. Wilson teaches in the Philosophy and Computer and Information Sciences at Towson University in Towson, MD and is a Research Fellow in the Hoffberger Center for Professional Ethics at the University of Baltimore. Professor Wilson has taught a wide variety of Applied Ethics courses including Engineering Ethics, Computer Science Ethics, Medical Ethics, Environmental Ethics and Business Ethics, and has a wide variety of publications in all of these areas. Previous experience also includes being an Ethics for the Department of Justice for the United States Government

Author Biographies

Pascal Ahr is a Bachelor of Science and Masters student of Electrical and Computer Engineering in Embedded Systems at University of Kaiserslautern (TUK) Germany. He works as research assistant at the German Research Center for Artificial Intelligence (DFKI). His research focusses on the field of Hardware - Physical Layer Security (PhySec) and Physically Unclonable Functions (PUFs).

Khalil Akbariavaz is a phd student at the Faculty of Law, University of Malaya. Research interests include public international law, Human rights, International Humanitarian Law, Rights of civilians, Rights of Children and Women and Middle East Politics. Khalil has presented papers in national and international Conferences. He has translated and edited a number of articles and books from Arabic and English to Persian.

Francis Xavier Kofi Akotoye is a PhD student at the University of Pretoria, South Africa. He received his MEng in Computer Science and Technology from Hunan University, China in 2007. His research interest are in digital forensic, computer security and mobile computing.

Hisham Al-Assam is senior lecturer in Computer Science, the University of Buckingham. He teaches Introduction to Computer Systems, Web Applications Development and Information Security,Web Technologies and Applications, and Information Security in Communications Key research interest is machine learning in security and healthcare. Security applications include deep learning for biometric recognition, dynamic signatures, privacy-aware biometric template security, and multi-factor remote authentication.

Ossama Al-Maliki is a Ph.D. research student at the University of Buckingham. Research focuses on the EMV contactless card specifications and improving the security of the EMV payment protocol. His M.Sc. degree was

Michal Konopa, MSc. is professor assistant in the Institute of Applied Informatics of Faculty of Science at the University of South Bohemia in České Budějovice. received his MSc in Informatics (Charles University in Prague, 2010). His main research area is machine learning and its application to computer network security problems. Other professional interests are algorithms, programming, and SAT solving.

Arturs Lavrenovs is a security researcher at NATO CCD COE focusing on the web and network technologies while teaching security courses, performing applied and academical research, and contributing to cyber exercises. Arturs has taught web technology and IT security courses at the University of Latvia where currently he is a PhD candidate.

Rudi Le Roux is currently completing his Bachelor of Arts degree at Stellenbosch University whilst residing in Stellenbosch. Rudi has a passion for IT security and early intrusion detection. Rudi spends his free time honing his hacking skills and familiarizing himself with the Kali operating system.

Louise Leenen's specializations are Artificial Intelligence applications in Cyber Defence and mathematical modelling. Currently an Associate Professor at the University of the Western Cape in South Africa, she was Chair of the International Federation for Information Processing's Working Group 9.10 on ICT Uses in Peace and War from 2014-2019. Holds a PhD in Computer Science from the University of Wollongong in Australia.

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Professor (Cyber security) in the University of Jyväskylä. He has over 40 years' experience in C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Cyber Security MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has over 130 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.

Christoph Lipps is a researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence's (DFKI) Intelligent Networks research group. He graduated in Electrical and Computer Engineering from the University of Kaiserslautern, where he lectures. Research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs) and the identification and authentication of various entities, including biometric authentication of humans, participating in the communication and network environment.

Sin Ming Loo is a professor at Boise State University with interests in cyber-physical systems security. He is responsible for Hartman Systems Integration and Cyber Lab for Industrial Control Systems laboratories. He holds a joint appointment with Idaho National Lab. He is a member of IEEE/CS, ISSA, Tau Beta Pi, and amateur radio (KI4AKS).

Andre Lopes is a student studying computer science. He obtained his undergraduate degree at Monash South Africa and is currently studying for his master's degree at the university of Cape Town, South Africa.

Dr. Tim Lynar is a Lecturer at the University of New South Wales. Tim is an expert in machine learning and agent-based modelling. Previously, Tim worked at IBM research for 7 and a half years, in that time he worked on a variety of projects cultivating substantial industry experience with a focus on machine learning and an emerging focus on Cyber security.

Dr. Leandros A. Maglaras is a Senior Lecturer in the School of Computer Science and Informatics of De Montfort University conducting research in the Cyber Security Centre. He is an author of more than 120 papers in scientific magazines and conferences and is a senior member of IEEE.

Isabel Martins, holds a Ph.D. in Organizational Behavior. She is currently an Associate Professor in Organizational Behavior at the University of KwaZulu-Natal, School of Management, IT & Governance, South Africa. Her scholarship spans across different countries including, South Africa, UK, Germany Portugal, Hong Kong, Middle East as well as the Gulf Countries.

Angela Mison is a Research Student at the University of South Wales. Her current interests are in cyber security of the road transportation system. She is the winner of the Automotive Electronics Innovation Cyber Student of the Year in Automotive.

Paulo Simões received the Doctoral degree from the Department of Informatics Engineering, University of Coimbra, Portugal, in 2002, where he is Assistant Professor. He leads industry-funded technology transfer projects for companies e.g. telecommunications operators and energy utilities. He was founding partner of two technological spin-off companies. Research interests include network and infrastructure management, security, critical infrastructure protection, and virtualization of networking and computing resources.

Ms Thenjiwe Sithole is a PhD student at the University of Johannesburg. She holds a Masters in Information Technology (Information Systems) from the University of Pretoria and a Master of Engineering Sciences with a focus on Electronics and Telecommunications from the University of Stellenbosch. She also has Certificate in Cyber Security from the University of Johannesburg.

Professor Iain Sutherland is Professor of Digital Forensics at Noroff University College in Kristiansand, Norway. He is a recognised expert in the area of computer forensics and data recovery. He has authored numerous articles in forensics practice and procedure and network security. He has consulted on Cyberesecurity issues for UK police forces and commercial organisations

Syed Ahmed Ali is doing PhD in field of Cloud Forensics at Institute of Information and Communication Technology, University of Sindh, Pakistan. He did his MS in the virtualization from Information Technology Centre, Sindh Agricultural University, Tando Jam, Pakistan. His research interests are Software Engineering, Information Security, Digital Forensics and Cloud System.

Eleanor Taylor is the Program Manager for Cybercore's Workforce Development and University Partnerships at Idaho National Laboratory (INL). She is responsible for leading initiatives designed to develop the interdisciplinary talent pipelines to attract and retain industrial control systems workforce. Before joining INL, Taylor held leadership positions at the University of Chicago, Argonne National Laboratory and SAS Institute.

Bruna Toso de Alcântara is a Ph.D. student at the Federal University of Rio Grande do Sul. She holds a Master's Degree in International Strategic Studies and a bachelor's degree in International Relations. Currently, she is a fellow at the Alexander von Humboldt Institute for Internet and Society and a Ph.D. exchange student at Humboldt University in Berlin.

Dr. Zouheir Trabelsi is a Professor of Information Security at the College of Information Technology, UAE University. He received his Ph.D. in Computer Science from Tokyo University of Technology and Agriculture, Japan. His research interests include: Network security, Intrusion systems, Firewalls, Covert channels, Information security education and curriculum development.

Gulfarida Tulemissova, associate professor of Suleyman Demirel University, Doctor PhD.Research interests are mainly in the area of Artificial Intelligence, Multiservice Networks, Software Defined Networks, Internet of Things, FPGA, Embedded systems. Today has over 45 journal publications, more than 20 conference papers (11 in Scopus and others) and three book.

Ms Eda Tumer is a Master's of Science student studying Software Engineering at De Montfort University, coming from a background of Bachelor's of Science in Computing which she studied at Cardiff Metropolitan University.

Maija Turunen is a PhD Student at the Finnish National Defense University. Her main research areas consist of cyber warfare, Russia and strategic communication.

Mr. Petri Vähäkainu is a cybersecurity PhD student (MSc., BSc.) in Faculty of Information Technology at the University of Jyväskylä in Finland, and a researcher in Finnish Defence Research Agency (FDRA). His main research areas in the University of Jyväskylä have been utilization of Artificial Intelligence in cybersecurity, health care and Structural Health Monitoring.

Carien van 't Wout is an Industrial Psychologist, working in cyber operations research at CSIR. Her career includes 25 years in the military. She is a subject matter expert in military psychological operations. Carien holds an Honours degree in Clinical Psychology and a Master of Commerce degree in Industrial and Organizational Psychology.

include management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, Internet of Things, software defined networking, and network function virtualization.

Dr Didier Danet is a senior lecturer in Military Academy of Saint-Cyr (France), “Mutation of Conflicts” Research Department. Didier DANET is Head of Post-Master Degree In Cyber Operations and Crisis Management.

Lisa Davidson is a Signals Officer within the Australian Army. Lisa is undertaking a Ph.D at the University of New South Wales. Her research focus is designing a holistic Cyber workforce for the Australian Army based on a Middle Power approach.

Gareth Davies is a Senior Lecturer in Digital Forensics and Cyber Security at the University of South Wales. As Chairman of The First Forensic Forum (F3), Gareth has organised international conferences and regular yearly workshops to demonstrate new digital forensics research and cutting edge technologies to the law enforcement community.

Arno de Coning is a Systems Engineer in Facilities management at the University of Pretoria. He received his M.Eng in 2013 for Computer and Electronic engineering and is working towards his PhD in the same field. His main research is in optimising processes by implementing data driven system designs.

Arnold Dupuy is an Assistant Professor at the Virginia Polytechnic Institute and State University in Blacksburg, VA. He is also the Chair of the Energy Security in the Era of Hybrid Warfare project of the NATO Science & Technology Organization.

Dr. Petrus Duvenage served as an officer in the South African armed forces and in the intelligence services. He holds a Senior Research Fellowship at the Academy for Computer Science and Software Engineering, University of Johannesburg. He has PhD from the University of Pretoria and a PhD (D.Com) from the University of Johannesburg.

Peter Eden is a Lecturer in Digital Forensics and Cyber Security at the University of South Wales. He is Course Leader for BSc/MSc Computer Security courses. He has provided digital forensic consultancy services to UK law enforcement agencies and police forces and has a number of publications within SCADA forensics.

Dr. Jan Fesl is professor assistant at the Institute of Applied Informatics (University of South Bohemia in České Budějovice, Czech Republic). He received his PhD in informatics from Czech Technical University in Prague in 2018. His main areas of research are computer networks, computer networks security and application of artificial intelligence methods for computer networks, and distributed systems.

Tim Grant is retired but an active researcher (Professor emeritus, Netherlands Defence Academy). Tim has a BSc in Aeronautical Engineering (Bristol University), a Masters-level Defence Fellowship (Brunel University), and a PhD in Artificial Intelligence (Maastricht University). Tim's research focuses on offensive cyber operations and on Command & Control and Emergency Management systems. More details can be found at https://www.linkedin.com/in/tim-grant-r-bar/.

Ferdinand J. Haberl is a doctoral candidate at the Department of Oriental Studies at the University of Vienna, where he focuses on jihadism worldwide, cyberterrorism, and jihadi (counter-) intelligence activities. He he has furthermore engaged in terrorism research in the Middle East, North and East Africa and Southeast Asia.

Saïd Haddad, Ph.D in Political science (René Descartes University, Paris), is Senior lecturer in Sociology and member of the research team, Conflits in Mutation of the Saint-Cyr Research Center at the Saint-Cyr Military Academy, France. His current research focuses on the construction of cyber as a French national priority and the sociology of “cyber warriors”.

Clay Hampton is a Research associate and adjunct professor at IUPUI. With a background in networking and Information security. I enjoy continuously learning about new technologies and how cybersecurity is an important field to secure systems and information to ensure we are able to stay safe.