CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 1, No. 1
July 2022
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal. Currently the target acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C)

Jeff Greer
greerj@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Ulku Clark
clarku@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

Inspired by the U.S. military's levels of warfare model, we suggest a three-level cybersecurity model around which to orient strata of understanding, expertise, and education in the cybersecurity domain. Informal observation of the current cybersecurity education landscape appears to reveal an imbalance among the levels. We introduce the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) to encourage greater balance. IVLE4C is a tool and conceptual learning model based on six interrelated knowledge domains which, when aggregated, define a modern digital enterprise and its cybersecurity posture. IVLE4C can be used to teach inter-functional and/or intra-functional skills. We contend that IVLE4C can provide three key benefits: improve cybersecurity pedagogy, enhance cross-enterprise training, and advance cybersecurity technology development.

Keywords: Cybersecurity, Education, Virtual Learning Environment, Model, Paradigm

1. INTRODUCTION AND MOTIVATION

Consider how someone unfamiliar with soccer might begin to learn the game. Shown a match, the game's objective becomes rapidly apparent – a large field with one net at each end, one ball, 11 players on each side, and lots of running and kicking of the ball. Game understanding emerges naturally, simply through observation. We might call this "learning from a top-down perspective." Note: we eschew "top-down/bottom-up learning" to avoid confusion with those terms as used in cognitive systems research (Sun & Zhang, 2004).

If that same person wishes to become proficient at playing soccer, they will need to spend time learning skills from the bottom up – dribbling, passing, shooting, etc. Integrating their top-down understanding of the game, they will begin to see why their bottom-up-acquired skills are useful and when to employ them. As they watch and participate in matches, they will begin to make associations between in-game situations and the lower-level skills they need to further develop to become more successful.

Now, imagine trying to teach this same person the game of soccer by engaging solely in bottom-up learning activities and without revealing that the game is played 11-v-11 on a field 115 yards (105 meters) long for two 45-minute halves. How could they see the importance of training to kick a ball over 40 yards or understand the concept of offsides?

The idea of teaching someone soccer in this manner rightly seems absurd. Unfortunately, we believe this manner of teaching more closely reflects the present state of cybersecurity education than many are aware or might care to acknowledge. There is tremendous focus on technical cybersecurity skills and great computer network-centric awareness – and rightly so. However, opportunities for learning how cybersecurity fits into an organization's larger picture and how it links with inter/national-level guidance appears lacking.

In this paper, we generalize a conceptual three-level framework of cybersecurity perspective derived from the U.S. military model of warfare. This framework provides a useful paradigm for thinking about varied cybersecurity perspectives, needed full spectrum cybersecurity expertise, and broad-range complementary approaches to cybersecurity education. The model helps identify a gap in current cybersecurity education efforts for which we introduce and describe the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) to facilitate advanced skill development (Von Glasersfeld & Steffe, 1991). (*We pronounce IVLE4C as "I will foresee" with slightly German-accented English*).

2. EDUCATION MODEL GAP IDENTIFICATION

The U.S. Army's capstone operations manual, which endeavors to set forth fundamental doctrinal concepts, traces its roots back to Baron von Steuben's 1779 Regulations for the Order and Discipline of the Troops of the United States. The manual undergoes periodic review and revision to reflect the evolving needs of the U.S. and the changing nature of warfare. With the 1982 revision, the conceptual three-level warfare model (Figure 1) was introduced to modern U.S. military theory (Department of the Army, 1982). The model has been accepted, refined, and now occupies a central position in the joint doctrine for all services – Army, Navy, Air Force, Marines, and Coast Guard (Joint Chiefs of Staff, 2017a).

This unifying model was important and useful to the armed forces and the U.S. because:

> War is a national undertaking which must be coordinated from the highest levels of policymaking to the basic levels of execution. Strategic, operational, and tactical levels are the broad divisions of activity in preparing for and conducting war. While the principles of war are appropriate to all levels, applying them involves a different perspective for each. (Department of the Army, 1982, p. 2-3)

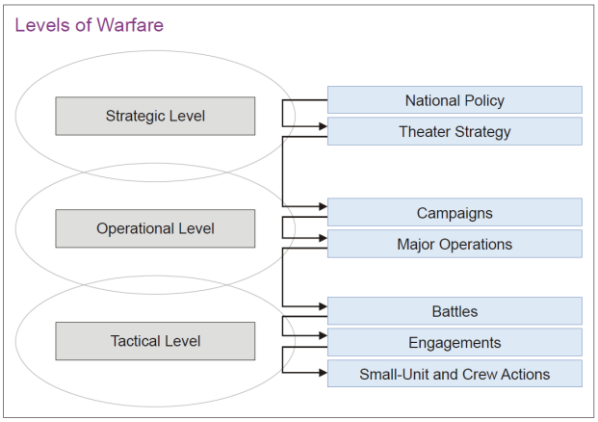

Figure 1: Levels of Warfare (Joint Chiefs of Staff, 2017a, Figure I-2)

This jointly-accepted, three-tier model provides a useful abstraction of warfare and offers a perspective that permits military units across the services and conducting various kinds of operations to speak a common language and act with unity of effort.

With modification, this model seems well suited for framing cybersecurity efforts at different strata and useful for thinking about how they tie together. Analogical and direct comparisons between war and cybersecurity have become common with journals and conferences devoted to or regularly featuring articles on cyberwarfare, including the International Conference on Cyber Conflict (NATO Cooperative Cyber Defence Center of Excellence, 2021), the Small Wars Journal (Small Wars Foundation, 2021), and the Cyber Defense Review (Army Cyber Institute, 2021). While levels of warfare are occasionally referenced, extending this model to cybersecurity education is, to our knowledge, new.

Luiijf and Healey (2012) added a policy level on top of the three-level military model to construct a four-level "generalized tool for analysis" (p. 111) that "can be applied as an instrument to study the much broader context of organizational decision-making structures in government." Raymond et al. (2014) referenced the three-level model when introducing the concept of key terrain at the four cyber planes: supervisory, cyber persona, logical, and physical (Raymond, et al., 2013). Schulze (2020) used the "three levels of warfare heuristic" (p. 184) to examine the utility of military cyber actions at each level.

In our derived model (Figure 2), we change the military-specific vocabulary to reflect the perspective from which cybersecurity efforts are being viewed: Government/Industry (GVI), Enterprise Leadership (EL), and Enterprise Employee (EE).

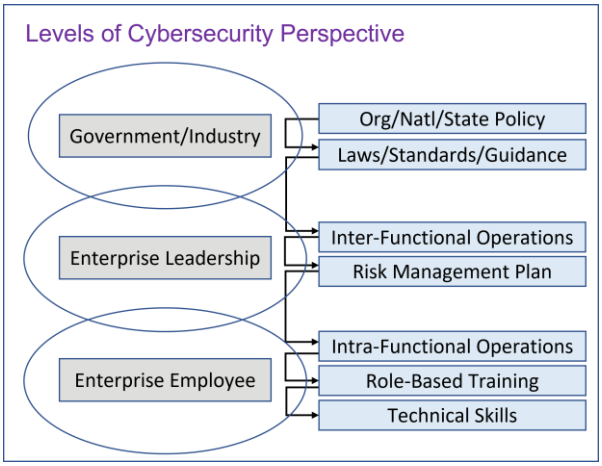

Figure 2: Cybersecurity Perspective Model

At the GVI level, political leaders issue directives, executive orders, etc. to set national/state policy, legislative bodies pass laws, and agencies/ industry bodies provide guidance on best practices/standards. Enterprise leaders at the EL level, whether government or commercial, for or non-profit, public or private, create enterprise policies, procedures, and processes that support inter-functional operations and comply with and/or are influenced by laws, standards, and other guidance. The enterprise risk management plan is a key product generated at the EL level. Enterprise employees at the EE Level fill specific roles and acquire technical skills to conduct intra-functional operations and securely install, configure, and operate digital devices.

While reasonable people might prefer different words to describe the levels, we believe many will find the Cybersecurity Perspective three-level model as useful for thinking about cybersecurity as the military has found their model for thinking about warfare.

Key to the military model's enduring usefulness, and the version we adopt for cybersecurity, is that the boundaries are not rigidly defined, but rather provide a flexible linkage of efforts from top to bottom. Accepting this model as an acceptable way to view the cybersecurity domain, we then recognize that we have a need for experts at all three levels that are heavily versed at their respective tier, but that are also capable of contributing to the other tiers.

Continuing with the three-level paradigm, we propose the complementary model, *Required Cybersecurity Expertise* (Figure 3). When thinking about the various kinds of cybersecurity expertise needed across the spectrum, we identify policy, management, and technical expertise. We change the shapes representing these concepts to reflect the need for robust expertise among the levels. For example, cybersecurity technical expertise is broadly required across the entire EE level, but also required to a lesser extent at the EL and GVI levels. Cybersecurity policy expertise reflects an inverse image – broad requirement across the GVI level and more narrow need progressing down through the EL and EE levels. Cybersecurity management expertise of enterprise leaders and functional leaders is broadly required at the EL level and to a lesser extent both up and down to the GVI and EE levels respectively.

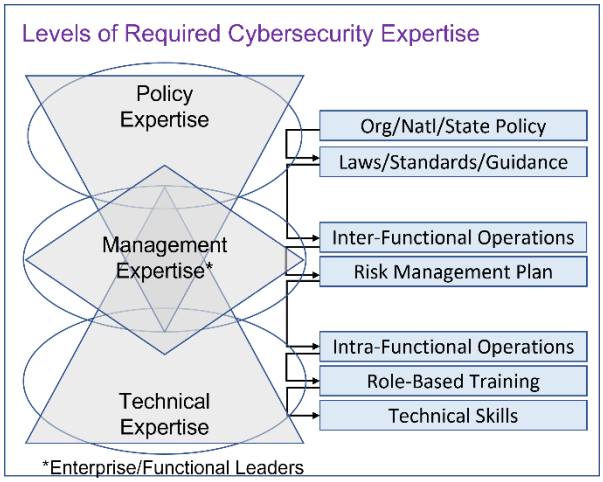

Figure 3: Required Cybersecurity Expertise

To create a stable of experts with the requisite expertise requires educational efforts across all levels; however, the current state of cybersecurity educational effort appears to have an imbalance that we believe is reflective of Figure 4 and that we will discuss in the next section. Figure 4 should be viewed as an abstract relative comparison. We are not suggesting that for every EE level workforce development course there should be one for EL and GVI development, but rather, that whereas it is plausible that current educational efforts are fully meeting EE level requirements, they are likely not meeting EL and GVI needs.

In this paper, we suggest that creating a conceptual learning environment will help grow and mature the cybersecurity pedagogy of the middle level – the EL view. It is at this level that

we will focus the paper starting in section 4. Just as the military's "operational level of warfare links the tactical employment of forces to national strategic objectives," (Joint Chiefs of Staff, 2017b, p. xi), we believe cybersecurity efforts at the EL level are vital for translating policy at the GVI level to actionable technical implementation at the EE level.

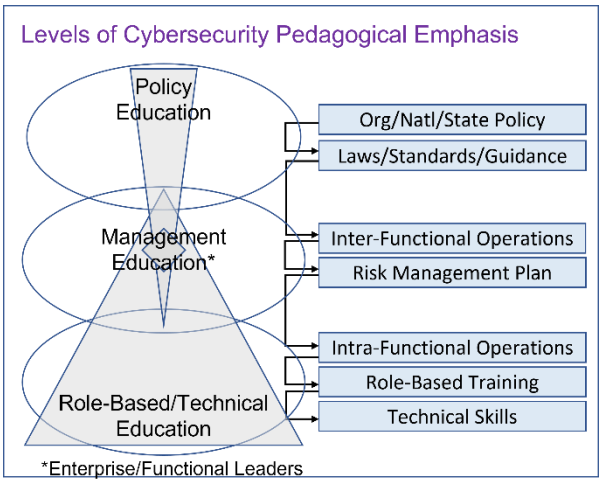

Figure 4: Current Levels of Cybersecurity Pedagogical Emphasis

3. CURRENT CYBERSECURITY EDUCATION LANDSCAPE

Traditional cyber ranges, by design, provide a computer network-centric viewpoint and focus on technical security. An early cyber range created to teach cybersecurity technical skills to college students is the IWAR laboratory (Schafer, Ragsdale, Surdu, & Carver, 2000). Created on premises at West Point, the isolated laboratory network fit into one classroom and consisted of machines built in the early-mid 1990s. This type of technically-focused cybersecurity learning environment proliferated rapidly – evolving and accelerating with the widespread adoption of virtual machines (VM) and web-based access.

Whether virtualizing a configurable network locally for computer science students (Du & Wang, 2008), providing non-engineering students exposure to hacking activities between two VMs on a laptop (Stoker et al., 2013), or hosting an open-source, publicly available, web-based learning platform on which anyone with interest can begin learning about cybersecurity (Kalyanam et al., 2020), technical-level cybersecurity educational innovations and opportunities abound. Outside of the physical and virtual classrooms, technical-level activity and competition-based cybersecurity events are seemingly everywhere and include, among other things, capture the flags (CTFs), tournament-structured events like the National Collegiate Cyber Defense Competition (CCDC) initiated in 2004, and CyberFIRE-type cybersecurity investigation training events (Frost & Stoker, 2020) established in 2009. Technical cybersecurity education at the EE level is deep, wide, feature rich, and continues to expand.

At the other end of the perspective hierarchy, cybersecurity policy education opportunities providing a GVI-level perspective exist but are smaller in number and seem to cater to a select group. Often, the education is embedded in traditional policy-style courses designed to give future policy makers a level of cyberliteracy that will allow them to "understand a particular issue and synthesize the ramifications into other aspects of national security" (Kessler & Ramsay, 2013). Events supporting policy-level cybersecurity education also exist, the first perhaps taking place in 1996, titled "The Day After… in Cyberspace" (Anderson & Hearn, 1996). Since 2012, the Atlantic Council has hosted "Cyber 9/12 Strategy Challenge" events where students compete in "developing policy recommendations tackling a fictional cyber catastrophe" (Atlantic Council, n.d.).

A good indicator of the imbalance we perceive at the EL level may be found among the data on the CyberSeek cybersecurity supply/demand heat map (2021) webpage. A comparison of certification holders to job openings indicates that the entry-level Security+ certification is ~300% oversubscribed, while the Certified Information Systems Security Professional (CISSP) population would need to increase nearly 18% just to meet current demand. And, while there are some, e.g., Jacob et al (2018), who appear, like us, to recognize that current cybersecurity education efforts are overly weighted at the technical EE level and have voiced concern, we are unaware of an existing effort/system that captures the cybersecurity perspective of the EL level for the purposes of providing a virtual enterprise-level cybersecurity view. The lack of learning environment support to the EL level motivates our work on IVLE4C.

4. CONCEPTUAL LEARNING ENVIRONMENT

Traditional K-12 and post-secondary students do not typically have enterprise-level experience, so we propose to bring the enterprise into the classroom. We believe the primary value of IVLE4C will be in helping students lift and shift their view from the parts to the whole. With much

of the cybersecurity pedagogy focused on transactions among digital devices, students unsurprisingly tend to develop a head-down, computer network-centric view.

Motivating the Idea

Our guiding precept – coined Greer's Truism – is that: *it is impossible to defend what cannot be visualized and described*. Therefore, it is essential to address the student enterprise knowledge gap before attempting to teach the means for assuring enterprise cybersecurity. Using IVLE4C will bring an EL perspective into the classroom, abstract away many of the technical details, and help students think about defending an enterprise rather than specific digital devices. Visualizing and describing an enterprise are challenging because of the operational scale, technical complexity, and geographic footprint involved. It is important to focus students on decision making for enterprise defense to achieve required cybersecurity objectives related to protection of assets and continuity of operations.

To help motivate and clarify this idea, consider the pervasive use of cloud-based services. Students contemplating threats & vulnerabilities to Amazon Web Services (AWS) might have only an abstract idea of AWS as virtual machines running "somewhere" out in the internet cloud. There is something about being able to see an actual AWS facility (Figure 5) that can make it feel real for students, capture their imagination, and expand their understanding of the enterprise that requires protecting.

Students need to see a modern digital enterprise from the viewpoint of an enterprise leader to properly understand enterprise cybersecurity. To our knowledge, there is no virtual learning user interface currently designed for this purpose.

In order to improve students' understanding of and classroom experience with enterprise cybersecurity (the EL level in Figure 2), IVLE4C will create and integrate six different enterprise views into a single environment as outlined in Appendix A and enumerated here:

1. ***Enterprise Operating Environment***: a 3D view of the world in which all enterprises operate.
2. ***Enterprise Being Defended***: a geo-located view of one or more enterprise buildings being defended.
3. ***Enterprise Digital Technology Stack***: a view of the digital technology (hardware, software, network communications, etc.) deployed in an enterprise's front office, back office, production operations, and field for mission achievement.
4. ***Enterprise Supply Chain***: a geo-located view of the enterprise/building's supply chain that is purpose built for fulfillment of enterprise needs.
5. ***Known Enterprise Threats & Vulnerabilities***: a web view of open-source intelligence needed for developing threat intelligence and identification of known vulnerabilities.
6. ***Enterprise Risk Management Plan***: a risk register for capturing identified risks, their assessment, treatment, and selected security controls for enterprise defense.

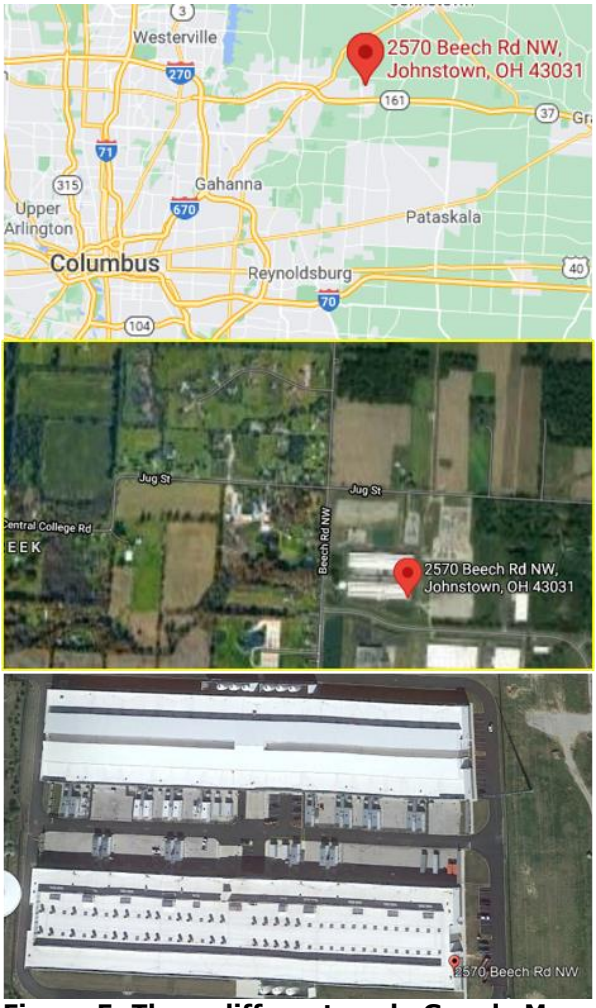

Figure 5: Three different-scale Google Maps views of the Johnstown, OH AWS facility (AWS facility, 2021)

Two-Level Conceptual Learning Model

Integrating all six enterprise views into a single virtual learning environment promotes conceptual learning at two levels. First, each individual view provides its own conceptual

learning opportunity for the topic matter contained within the view. For example, the notion of a digital technology stack, built for mission achievement, is an important cybersecurity topic in and of itself because students need to understand its architecture and inherent vulnerabilities. Second, the content in all six views is needed to create a conceptual learning opportunity for students at the enterprise or system level. There are relationships between the content in the discrete view topics that a student needs to understand before they can create a viable cybersecurity plan. For example, students need to develop an understanding of how cybersecurity controls are applied to an enterprise, its digital technology stack, and supply chain. Affording students with a two-level conceptual learning opportunity will accelerate their skill development and effectiveness. Further information on the views, their content, and use for creation of learning opportunities follows.

Learning Opportunities

Learning opportunities arise when all six views are integrated into a single virtual learning environment.

- Students will be able to see an actual image of a digital enterprise being defended and its operating environment versus imagining an abstract, nondescript enterprise.
- Students will better understand external versus internal threats once they draw a security demarcation boundary around the physical enterprise location(s).
- Students will develop better awareness of different digital technology stack designs based on enterprise type and strategy for mission achievement. Concepts like the Open Group's Architectural Development Method (ADM) will help students understand the functionality provided by digital technology in the context of enterprise requirements. Similarly, the Information Technology Infrastructure Library (ITIL) can be shown as a means for operating the digital technology stack for secure service delivery. Key to cybersecurity is the risk while using the digital technology stack which needs to be understood and treated.
- Students will be able to visualize an actual purpose-built supply chain that fulfills enterprise needs. Key is the number of suppliers and inter-action link types that exist between the enterprise being defended and its suppliers. This includes both traditional physical transport of goods and service technicians along with data transport over telecommunication circuits for remote delivery of digital services. A supply chain represents a large and porous attack surface that is increasingly being exploited. Rendering the supply chain will promote student awareness of third-party supplier risk and the need for treating it.
- Students will become more effective in assuring cybersecurity once they learn how to assess a modern digital enterprise and its operating environment. It is common knowledge that there is no one-size-fits-all approach to cybersecurity for all enterprises. Tailoring the cybersecurity plan to the enterprise is promoted as a best practice. To do this, a student needs to have a baseline understanding of the enterprise being protected, its digital technology stack, and its supply chain. With this knowledge, it is then possible for a student to review open-source intelligence for identification of motivated threat actors and their attack tactics, techniques, and procedures (TTPs).
- Students need to become more effective in assuring enterprise cybersecurity. This can be accomplished by recording specific identified risks in a risk register. These risks can then be assessed and ranked based on probability of occurrence and enterprise impact. Each identified risk provides an opportunity for a student to determine an appropriate risk treatment using one of the seven options identified in ISO 31000 (ISO/IEC, 2019a). When deploying a physical, technical, legal contract, or policy security control, it is important for a student to link the security control to the enterprise being defended, its digital technology stack, or its supply chain. The cost of a cybersecurity risk management plan needs to be further assessed in terms of its cost and the risk appetite of enterprise leadership.

Creating Six Views Leads to a Seventh

The underlying data set, developed while creating the six views, is valuable and useful for creating a seventh view that is important for enterprise leadership and student learning. The seventh view is a near real time dashboard with descriptive statistics useful for better understanding and communicating about the enterprise and its cybersecurity plan. This information is essential for identifying enterprise leader control points for mission achievement and differentiation of normal versus abnormal operating conditions. An example of supply chain descriptive statistics includes the number of cyber suppliers in the supply chain. Of this number, it is important to know the number of trusted

suppliers. If a supplier is deemed to be trusted then what is the basis of trust, etc.

IVLE4C Architecture

IVLE4C is logically depicted in Figure 6. Think of it as a special variant or analog of a traditional computer aided design or engineering workstation. Instead of being used to design products or buildings, it will be used to design or document a digital enterprise and its cybersecurity risk management plan. Intended IVLE4C users are students, teachers, researchers, and working professionals. Users will input information required for decision making and resultant output will create the six views described above. The seventh view, with descriptive statistics, will automatically calculate as information is entered. Analysis of an enterprise being defended will be saved as a file instance for future review and use.

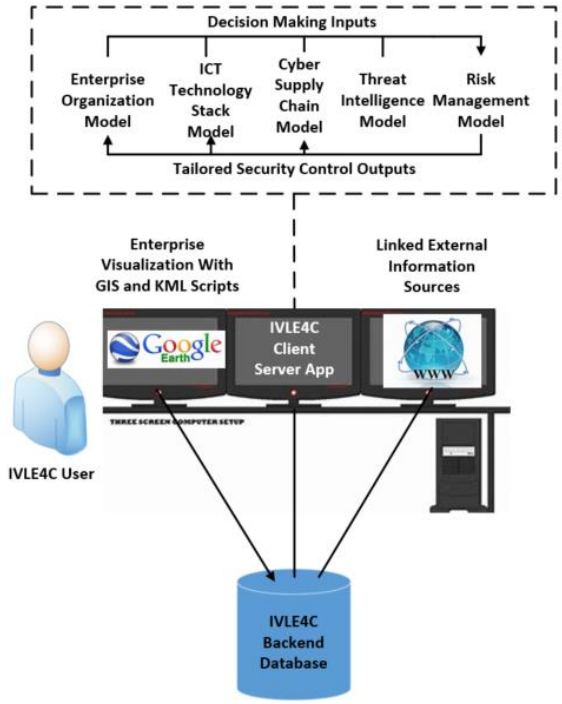

Figure 6: IVLE4C Logical Design

Expected Benefits

The expected benefits that will accrue to IVLE4C users include:

- Teachers will be able to create grade and class appropriate lessons using varying levels of input or description resulting in abstraction for delivery of key educational outcomes.
- As a client server web application, IVLE4C is extensible down to the student or working professional level as a VM session where they can participate in hands-on learning experiences. Working to secure a named enterprise will result in a richer student learning experience.
- Researchers will be able to comparatively analyze different enterprises in terms of their unique digital technology stacks, supply chains, and threat environments using a standard documented format.

5. DISCUSSION

With increasing frequency and impact, enterprises are being attacked and disrupted. In May 2021, President Biden issued an Executive Order on Improving the Nations Cybersecurity (Executive Order No. 14028, 2021). Shortly after signing the order, he called for greater private sector investment in cybersecurity. There is a limit to what government can do when partnering with privately owned enterprises. It is one thing to write an Executive Order and suggest greater private sector investment for cybersecurity; however, intelligent action is necessary along with continuity of effort to achieve enterprise cybersecurity and resilience.

An important question to consider is how IVLE4C can be used to promote enterprise cybersecurity. At a high-level there are three opportunities worthy of consideration and action. First, is the use of IVLE4C to help achieve the National Initiative for Cybersecurity Education (NICE) roadmap objectives. Second, is the use of IVLE4C to help working professionals implement the National Institute of Standards and Technology (NIST) cybersecurity frameworks along with others like the recent Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) requirements for defense industrial base (DIB) suppliers. Third, is use of core IVLE4C capabilities as an enabler for developing new digital and cybersecurity technology.

In 2008, the U.S. Government created NICE in response to a recognized need to expand the cybersecurity workforce and improve its effectiveness ("National Initiative for Cybersecurity Education," 2021). Over time, NICE needs to evolve if it is going to be maximally effective. The threatscape is constantly changing along with the application of new digital technology for enterprise mission achievement and changes in enterprise operating practices. With IVLE4C, NICE will be better able to expand the mission scope to include better enterprise leader development including both senior executive leaders and senior functional leaders who need to provide critical leadership for

enterprise cybersecurity. IVLE4C will facilitate team inter-action and skill development. K-12 and secondary students exposed to IVLE4C will develop an appreciation for the importance of cybersecurity, career opportunities, and the means for assuring enterprise cybersecurity. Early enterprise exposure will provide a broader learning context when a student is taking technical cybersecurity courses. This approach will promote greater skill development and help reduce the time for an enterprise employee to qualify for promotion into an enterprise-level leadership position.

In 2014, NIST released the Cybersecurity Framework (CSF) for enterprise use (NIST, 2020). While useful as a risk management framework, working professionals frequently comment on the framework's complexity and the resulting difficulty in implementing it. The same holds true for other cybersecurity frameworks and standards. The challenge then is how to simplify the complex for greater effectiveness. IVLE4C can play a key role in simplifying cybersecurity risk management frameworks. This includes both improved understanding and greater clarity in deployment. With IVLE4C it is possible to virtually architect and communicate a risk management and resiliency plan. Typically developed by a team of professionals working collaboratively in a conference room, having the ability to project the key views of IVLE4C in the conference room will help promote common understanding and better decision making. IVLE4C will be a repository which will document all assumptions, decisions, and actions. This is valuable information for computer incident response teams and development of after-action reports.

As a concrete example, consider the recent ransomware attack on Colonial Pipeline ("Colonial Pipeline," 2021) that shut down 5,550 miles of pipe and disrupted the daily delivery of ~100 million gallons of gasoline, diesel, and jet fuel to much of the east coast (Testimony of Joseph Blount, 2021). Though details are not yet fully known at the time of the writing of this article, Joseph Blount, Colonial's president and CEO, stated at a senate committee hearing that the current working theory is that the attackers exploited a legacy virtual private network (VPN) profile. We could imagine, given the history of DarkSide (Shakarian, 2021), that one of the avenues of exploitation might have involved the SonicWall VPN vulnerability, CVE-2021-20016. And, we might further imagine a technical-level discussion of this SQL-injection vulnerability that "allows a remote unauthenticated attacker to perform SQL query [sic] to access username password and other session related information" (NIST, 2021).

Contrast that thought with the idea of discussing the attack in the context of IVLE4C with the ability to link to CEO testimony video, a pipeline map (Figure 7), Google Earth views of injection stations, delivery facilities, booster stations, etc.

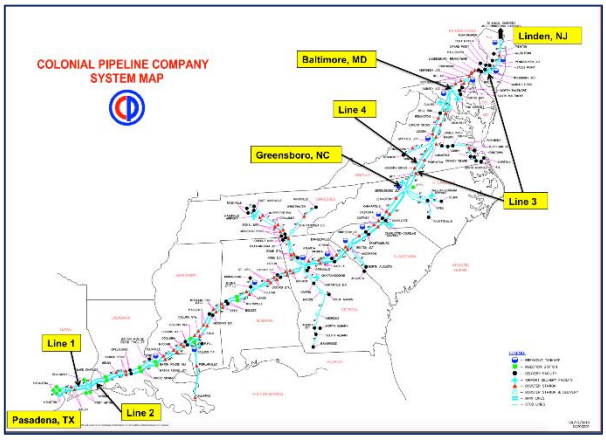

Figure 7: Colonial pipeline image (RBN Energy LLC, 2021)

Imagine IVLE4C users getting a deeper understanding of how business systems and operational systems interact and acquiring new insight into how errors and missteps at the EE level (software flaws, weak passwords, misconfigurations, clicking malicious links, opening dangerous e-mail attachments, etc.) can trigger a chain of events that disrupt the lives of tens of millions of people.

It is commonly acknowledged that early digital technology employed by enterprises was never designed for security. Over time, with successful cyber-attacks causing material damage, action was taken to create secure digital technology and operating environments for enterprise use. This trend is still ongoing and expected to carry forward into the future to address enterprise needs.

IVLE4C has a core capability that is needed for next generation cybersecurity technology. Its virtual enterprise model, views, and analytical data are essential for creating a state machine identifying normal and abnormal enterprise digital operations using AI. The notion of creating a secure digital operating environment is a top priority for an enterprise. Once the secure digital operating environment is established, applications can then be deployed to address enterprise needs. It is anticipated that intelligent

networks and smarter digital devices will communicate and interact with the state machine. IVLE4C will enable the cybersecurity focus to shift from the network or digital device to the enterprise being protected.

6. CONCLUSIONS & FUTURE WORK

In this paper, we introduce a paradigm, derived from the U.S. military three-level model for warfare, which is useful for thinking about cybersecurity understanding, expertise, and education. Analogical to the military's strategic, operational, and tactical levels of warfare, we designate three levels of cybersecurity perspective: Government/Industry (GVI), Enterprise Leadership (EL), and Enterprise Employee (EE) (Figure 2). Each level has different educational needs if government/industry leaders are going to effectively achieve policy objectives, enterprise leaders are going to assure enterprise security, and enterprise employees are going to securely employ systems and equipment (Figure 3).

To help close the education gaps identified above the technical level (Figure 4), we introduce IVLE4C, an Integrated Virtual Learning Environment for Cybersecurity Education. The IVLE4C creates a two-level conceptual learning opportunity the primary value of which will be to raise students' eyes and cybersecurity perspective from the parts of an enterprise to the whole.

IVLE4C development is ongoing. In parallel, research is being conducted on the use of IVLE4C for enterprise continuity planning as specified in ISO 22301 (ISO/IEC, 2019b). Continuity planning for resiliency runs parallel to cybersecurity and is essential for enterprise recovery as called for in the NIST Cybersecurity Framework. As IVLE4C becomes more fully developed, we anticipate that its use in a classroom environment for delivery of educational objectives will grow over time. Key will be IVLE4C's impact on the delivery of NICE K12 roadmap outcomes and cybersecurity pedagogy. Finally, as IVLE4C becomes more fully developed, exploratory work is planned for the development of a more secure enterprise and digital operating environment using new technical capabilities.

7. REFERENCES

Anderson, R. H., & Hearn, A. C. (1996). An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After... in Cyberspace II". RAND CORP SANTA MONICA CA. https://apps.dtic.mil/sti/pdfs/ADA319848.pdf

Army Cyber Institute. (2021). Cyber Defense Review. https://cyberdefensereview.army.mil/About-CDR/

Atlantic Council (2021). Cyber 9/12 Strategy Challenge. https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/

AWS facility. (2021). Google Maps. https://goo.gl/maps/Q3g9K5RsYXJuRyzK7

Colonial Pipeline cyber attack. (2021). In Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack

Cybersecurity Supply/Demand Heat Map. (2021, August). CyberSeek Project Web site. https://www.cyberseek.org/heatmap.html

Department of the Army. (1982, August 20). Operations (FM 100-5). https://cgsc.contentdm.oclc.org/digital/collection/p4013coll9/id/976/

Du, W., & Wang, R. (2008). SEED: A suite of instructional laboratories for computer security education. Journal on Educational Resources in Computing (JERIC), 8(1), 1-24. https://dl.acm.org/doi/pdf/10.1145/1348713.1348716

Exec. Order No 14028. (2021, May 12). Improving the Nation's Cybersecurity. https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

Frost, N. & Stoker, G. (2020). Novice Cybersecurity Students Encounter TracerFIRE: An Experience Report. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 4901). http://proc.iscap.info/2020/pdf/5337.pdf

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 31010:2019 (2019a, June). Risk management - Risk assessment techniques. https://www.iso.org/standard/72140.html

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 22301:2019 (2019b, October). Security and resilience - Business continuity management systems - Requirements. https://www.iso.org/standard/75106.html

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T.A. (2018). Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors? Proceedings of the 16th International Conference on Scientific Computing (CSC'18). https://par.nsf.gov/servlets/purl/10095246

Joint Chiefs of Staff. (2017a, July 12). Doctrine for the Armed Forces of the United States (JP 1). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Joint Chiefs of Staff. (2017b, January 17). Joint Operations (JP 3-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

Kalyanam, R., Yang, B., Willis, C., Lambert, M., & Kirkpatrick, C. (2020, October). CHEESE: Cyber Human Ecosystem of Engaged Security Education. In 2020 IEEE Frontiers in Education Conference (FIE) (pp. 1-7). IEEE. https://aic-atlas.s3.eu-north-1.amazonaws.com/projects/e7299991-eb2b-4764-a849-4909e01fb07d/documents/THwopx8k3piBVcoXolb6jvstZa8bvlWHPspCJ59B.pdf

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. Journal of Homeland Security Education, 2, 35. https://commons.erau.edu/cgi/viewcontent.cgi?article=1006&context=db-security-studies

Luiijf, E. & Healey, J. (2012). Organisational Structures & Considerations. In National Cybersecurity Framework Manual (pp. 108-). Tallinn: NATO CCDCOE. https://www.researchgate.net/publication/261984614_Political_Aims_Policy_Methods

National Initiative for Cybersecurity Education (NICE). (2021). In Wikipedia. https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education

National Institute of Standards and Technology (NIST). (2021, February 4). CVE-2021-20016. https://nvd.nist.gov/vuln/detail/CVE-2021-20016

National Institute of Standards and Technology (NIST). (2020, November 16). NICE Framework Resource Center History. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history

NATO Cooperative Cyber Defence Center of Excellence. (2021). International Conference on Cyber Conflict. https://www.cycon.org/

Raymond, D., Conti, G., Cross, T., & Fanelli, R. (2013, June). A control measure framework to limit collateral damage and propagation of cyber weapons. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (pp. 1-16). IEEE. http://www.rumint.org/gregconti/publications/130324_CyCon_Malware_Full.pdf

Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the high ground. 2014 6th International Conference on Cyber Conflict (CyCon 2014), 287-300. http://www.rumint.org/gregconti/publications/Cyber_Key_Terrain_v14.pdf

RBN Energy LLC. (2021). Colonial Pipeline Image. https://rbnenergy.com/sites/default/files/field/image/figure1_299.png

Schafer, J., Ragsdale, D. J., Surdu, J. R., & Carver, C. A. (2000). The IWAR range: a laboratory for undergraduate information assurance education. https://apps.dtic.mil/sti/pdfs/ADA408301.pdf

Schulze, M. (2020, May). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In 2020 12th International Conference on Cyber Conflict (CyCon) (Vol. 1300, pp. 183-197). IEEE. https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf

Shakarian, P. (2021, May 24). Colonial Pipeline Breach: Vulnerabilities Used by DarkSide CYR3CON. https://blog.cyr3con.ai/colonial-pipeline-breach-vulnerabilities-used-by-darkside

Small Wars Foundation. (2021). Small Wars Journal. https://smallwarsjournal.com/

Stoker, G., Arnold, T., & Maxwell, P. (2013, October). Using virtual machines to improve learning and save resources in an introductory IT course. In Proceedings of the 14th annual ACM SIGITE conference on Information technology education (pp. 91-96). https://dl.acm.org/doi/pdf/10.1145/2512276.2512287

Sun, R., & Zhang, X. (2004). Top-down versus bottom-up learning in cognitive skill acquisition. Cognitive Systems Research, 5(1), 63-89. https://www.sciencedirect.com/science/article/pii/S1389041703000470

Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company, U.S. Senate Committee on Homeland Security and Governmental Affairs, 116th

Cong. (2021). https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf

Von Glasersfeld, E., & Steffe, L. P. (1991). Conceptual models in educational research and practice. *The Journal of Educational Thought (JET)/Revue de la Pensée Educative*, 91-103. https://www.jstor.org/stable/23767267?casa_token=k50ylvFfHwcAAAAA%3A2ntSGivNDgvk4i6F_IY4L5J3atM4gR4quf5tRnv6uZTD9RLCc9Mqz0OFCjmwdwHXowf5SOmht6qiHglPGH8cylV-8yAizoh6zbzFml6tBp-f0Ooq3lin&seq=1&socuuid=5c07442f-543a-4da1-afe1-8acf3007b596&socplat=email#metadata_info_tab_contents

Appendix A – Six Enterprise Leader (EL) Level Functional Views

(*Alt + Left arrow to return to hyperlink location*)

Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) Enterprise Leader (EL) Functional View Elements						
EL View-point	**Enterprise Operating Environ-ment**	**Enterprise Being Defended**	**Enterprise Digital Technology Stack**	**Enterprise Supply Chain**	**Known Enterprise Threats & Vulnerabilities**	**Enterprise Risk Mgmt. Plan**
Content Shown	3D Earth view	View of building located on the Earth's surface.	View of building ICT deployed for mission achievement.	View of supply chain vendors fulfilling enterprise needs.	View of motivated threat actors, potential attack vectors, & known vulnerabilities	View of identified risks, their assessment, treatment, and security control deployment