2020

Building Cyber Defense Training Capacity

Moore, Erik

http://hdl.handle.net/10026.1/16608

http://dx.doi.org/10.24382/984
University of Plymouth

UNIVERSITY OF PLYMOUTH

Building Cyber Defense Training Capacity

By

Erik Moore

A thesis submitted to the University of Plymouth in partial fulfillment for the degree of

Doctor of Philosophy

School of Engineering, Computing and Mathematics

July 2020

Copyright Statement

Table of Contents

Building Cyber Defense Training Capacity i

Copyright Statement ii

Table of Contents iii

List of Figures v

List of Tables vi

Author’s Declaration vii

Acknowledgements viii

Glossary of Abbreviations ix

Abstract xii

Building Cyber Defense Training Capacity xii

1 Introduction 1

1.1 Background 1

1.1.1 Cybersecurity Laboratory, Training, and Challenge Environments 2

1.1.2 System Virtualization in Education 2

1.1.3 Virtual World Usage in Education 3

1.1.4 Cyber Defense Collaborative Training 3

1.1.6 Background Summary 4

1.2 Research Context 4

1.3 Research Aims and Methods 5

1.4 Thesis Structure 7

2 - Service Development 10

2.1 - Multi-Method Virtualization - A Pipeline Model for Service Tuning 10

2.2 - Agile Service Provisioning 12

2.3 - Physical Datacenter Virtualization 13

3 - Providing Digital Context 14

3.1 - Modeling the Impact of Virtualization 15

3.2 - Managing Digital Identity 16

4 - Tuning Performance 18

4.1 - Evaluating Multi-Agency Cybersecurity Training 18

4.2 - An Agile Joint Collaborative Training Model 19

4.3 - Short-Cycle Psychometric Feedback 20

5 - Analyzing Impact 22

5.1 Collaborative Response Communities 22

5.2 Institutional Risk Reduction for Teaching Cybersecurity 23
6 Current Impact and Relevance 26
6.1 Service Development 26
6.2 Providing Digital Context 27
6.3 Tuning Performance 27
6.4 Analyzing Impact 28
6.5 Building Cyber Defense Training Capacity as an Integrated Focus 28
7. Conclusion 30
7.1 Research Contributions 30
7.2 Limitations 31
7.3 Future Work 32
References 34
Appendix A - Published Works 38
Appendix B - Confirmation Letters 48

List of Figures

Figure 1: Layered Cybersecurity Capacity Building Model 8

Figure 2: Service Line Pipe Model 11

Figure 3: Virtual World Datacenter Image 14

Figure 4: Psy-BIR-Phys Model of Virtual Command Post 16

Figure 5: Knowledge/Belief and Ethics/Allegiance Model 17

Figure 6: Xmodel of Collaborative Training and Response Community 19

Figure 7: Short-cycle Framework Model for Aggregate Analysis 20

Figure 8: Incident Response Load Model 23

Figure 9: Range of Participant Behavior Model 24

List of Tables

Table 1: Virtualization Layer Model (VLM) 12

Table 2: Matrix of Cybersecurity Program Deployment with Risk Mitigation 25

Author’s Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other university award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment. Word count of the main body of thesis: 13,669

Signed ______________________

Date July, 14, 2020

Acknowledgements

The earlier work was created while working in the roles of Technical Lead of Regis University's Academic Research Network laboratory and Faculty Advisor for the graduate students in the Systems Engineering and Application Development Practicum. A significant amount of the work was created while working as founding co-director of COFR-CIAS (Colorado Front Range Center for Information Assurance Studies) at Regis University in Denver, Colorado, USA.

Glossary of Abbreviations

3D Systems or technologies that render space in three dimensions to give a feeling of immersion in that space.

5ESS A 5th generation telephone switching system, the line of which was designed originally by Western Electric in the United States, becoming the first pervasive all digital switch in the telecom networks.

A/E A scale where *allegiance* and *ethics* are set in a scale of conjugate pairs (as in the chemical terms pH and pOH) to measure how much a decision is based on each type of moral context. *allegiance* and *ethics* have specific technical definitions in this model.

ANOVA ANalysis Of VAriance, a quantitative analytical method of dividing variation into components

ARN Academic Research Network at Regis University

ARPANET The Advanced Research Projects Agency Network is an experimental computer network that was the forerunner of the Internet. The agency that developed ARPANET in the late 1960s is an arm of the U.S. Defense Department.

CAD Computer Aided Design, a type of software method of designing 3D objects used by architects in building design, automated machining of parts, and elsewhere.

CANVAS Computer and Network Virtualization and Simulation, the name for a cyber challenge offered in the State of Colorado

CCDC Collegiate Cyber Defense Challenge, a national cyber defense competition in the United States.

CDOT Colorado Department of Transportation

CEO Chief Executive Officer of a company

CERN The Conseil Européen pour la Recherche Nucléaire, an organization of European states in Geneva for high-energy particle physics now known as the European Laboratory for Particle Physics

CIAC Colorado Information Analysis Center (also meaning Computer Incident Advisory Capability in the US Department of Energy)

CMMI Capability Maturity Model Integration as developed at Carnegie Mellon Institute

COFR-CIAS Colorado Front Range Center for Information Assurance Studies, at Regis University in Denver, Colorado, USA

COVID-19 A novel coronavirus that was identified in 2019 and spread into a global pandemic

CTRC Collaborative Training and Response Team, particularly in the case of teams that train together and respond to incidents together across multiple institutions

CVSS Common Vulnerability Scoring Systems

DDoS Distributed Denial of Service attack, meaning an attack generally over the Internet where servers or clients over a distributed geographic area

	simultaneously bombard a particular system with requests so that it is overwhelmed, thus denying services to its regular customers
F	Feedback from a Psychometric Monitor during training or incident response
GNS3™	A brand name of an open source network emulator whose name is an acronym for Graphics Network Simulator, the third version
HTTP	HyperText Transfer Protocol, used to transmit web pages and other data over the Internet
I	The Internet, meaning the global Internet and not internetworks that are separate or a subset of the global Internet
IFIP WG 11.8	International Federation for Information Processing, Working Group 11.8 on Information Security Education
IRL	Relative Incident Response Load measured across a cybersecurity incident timeline
ISP	An Internet Service Provider, such as a cable or phone company that provides wired or wireless connections to provide access to the Internet
K/B	A scale where knowledge is set in a scale of conjugate pairs (as in the chemical terms pH and pOH) to measure the context in which human beings rely on these types of information for motivation and decision making. Knowledge and Belief have specific technical definitions in this work.
LMS	Learning Management System, a type of application that is generally web-based to hold curricular content, assessment tools, and interaction space for student engagement
MBTI	Myers-Briggs Type Indicator, a psychometric instrument for determining personality traits
n	Number of participants in a statistical sample
OSI	Open Systems Interconnect Model, a product of the International Organization for Standards
PELE	Personalized Experiential Learning Environment, as developed and presented in the author's research
pH	The measure of hydrogen ion concentration in a solution, the conjugate pair to pOH
PM	Psychometric Monitor
pOH	The measure of hydroxide ion concentration in a solution, the conjugate pair to pH
Psy-BIR-Phys	A cartesian coordinate model. On the Y axis the double scale is conjugate pairs (as in the chemical terms pH and pOH) with psychological significance increasing in importance vertically and physical significance decreasing. On the X axis the scale is the level of Bit Induced Realty. An example of levels of bit indication is in how a coffee cup moves from handmade to computer designed, then to a virtual coffee cup in a virtual world where its continued existence relies on digital bits.
PTPS	Parker Team Player Survey, a psychometric instrument for determining team structure and interaction characteristics
SCADA	Computerized systems designed for the Supervisory Control and Acquisition of Data, used to automate and control industrial systems such as oil refineries and municipal drinking water systems

SCRUM Not an acronym, but a reference to an intense moment in the sport of Rugby, used in information systems practice as a reference to intense recurring periods of focused development in agile business and technology

SDLC Systems Development Life Cycle as used in this work, or used commonly as Software Development Life Cycle or Security Development Life Cycle

SLB Second Life® Browser, a 3D Viewer for an avatar-based virtual world accessible from a regular computer screen without headsets.

SNIA™ Storage Network Industry Association

TCP/IP A suite of protocols that make the Internet function, represented in the acronym by Transmission Control Protocol (used for simulating a connection over a packet network) and Internet Protocol (used for addressing devices and routing packets from local network traffic across large blocks of addresses such that the Internet became possible)

VLM Virtualization Layer Model developed by the author, is a layered model that starts at the bottom of the stack with technological layers like the virtualization of networks, and near the top of the stack has environmental and social virtualization layers.

VPL Visual Philosophy Language, a visual technique of understanding philosophical questions, developed by the author

VPN Virtual Private Network, a set of authentication and encryption technologies designed to tunnel data more securely over the Internet

VR Virtual Reality, a 3D virtual space experienced generally using digital binocular headsets as though the space is all around the user

Abstract

Building Cyber Defense Training Capacity

Erik Moore

As society advances in terms of information technology, the dependency on cyber secure systems increases. Likewise, the need to enhance both the quality and relevance of education, training, and professional development for cybersecurity defenders increases proportionately. Without a continued supply of capable cyber defenders that can come to the challenge well-prepared and continuously advance their skills, the reliability and thus the value of information technology systems will be compromised to the point that new information-driven societal structures in commerce, banking, education, infrastructure, and others across the globe would be put be at risk.

The body of research presented here provides a progressive building of capacity to support information technology, cybersecurity, and cyber defense training efforts. The work starts by designing infrastructure virtualization methods and problem modeling, then advances to creating and testing tunable models for both technical and social-psychological support capabilities. The initial research was designed to increase the capacity of Regis University in education simulations and cyber competitions. As this was achieved the goals evolved to include developing effective multi-agency cyber defense exercises for government and private sector participants.

The research developing hands-on computer laboratory infrastructure presents novel methods for enhancing the delivery of training and cyber competition resources. The multi-method virtualization model describes a strategy for analyzing a broad range of virtualization services for making agile cyber competition, training, and laboratory spaces that are the technical underpinning of the effort. The work adapts the agile development method SCRUM for producing training events with limited resources. Parallel to agile training systems provisioning, the research includes designing a 3D virtual world avatar-based resource to help students develop spatial skills associated with physical security auditing. It consists of a virtual world datacenter and training program.

The second category of contributions includes the presentation of new models for analyzing complex concepts in cybersecurity. These models provide students with tools that allow them to map out newly acquired skills and understanding within a larger context. One model maps how classical security challenges change as digital technologies are introduced using a concept called “bit induction.” The other model maps out how technology can affect one’s sense of identity, and how to manage its disruption.

The third area of contribution includes a rapid form of psychometric feedback, a customized quantitative longitudinal capability assessments, and an agile framework that is an extension of the earlier agile method adaptations.

The most recent category of contribution extends the training analysis to analyzing the resultant training capabilities and providing new models to describe live operation using operational load analysis to describe characteristic behaviors along an incident timeline.

The results of this research include novel cybersecurity frameworks, analytical methods, and education deployment models along with interpretation and documented implementation to support education institutions in meeting the emerging risks of society. Specific contributions include new models for understanding the disruptiveness of cyberattacks, models for agilely and virtually deploying immersive hands-on laboratory experiences, and interdisciplinary approaches to education that meet new psycho-sociological challenges in cyber defense. These contributions extend the forefront of Cybersecurity education and training in a coordinated way to contribute to the effectiveness and relevance of education solutions as society’s cybersecurity needs evolve.

1 Introduction

This body of work focuses on the development of new capabilities for cyber training programs whose functions support laboratory work associated with university classes, cyber competition spaces, and professional training program development for cyber defense teams. In the context of these served groups a particular military team was prepared for live cyber defense incident response, which is described in detail in the last paper. The work was completed at Regis University, where the author held a range of technical and research leadership titles, the highest being founding co-director of the cybersecurity center.

1.1 Background

A significant challenge of moving humanity to a cyber-empowered global society is addressing the concomitant cyber vulnerabilities. Significant advances in our communications and computing capabilities have led to a highly connected and automated environment where the need for ensuring cyber defense capacity continuously increases. To consider the increasing risks that humanity faces as its dependencies on digital technologies increases, a timeline going back to the 1980's is helpful.

A landmark of transition that suggests this new cyber world is the establishment of the Internet in 1983 when ARPANET switched to TCP/IP as its primary host protocol (Leiner *et al*, 1997). At that time, the US was just starting to digitally connect across all markets with the introduction of new digital telephone switches like the Western Electric 5ESS (Marterstek *et al*, 1985). Information assurance was often more about controlling human behavior related to talking in person and controlling the sharing of paper. Since then, the High-Performance Computing Act sponsored by Senator Albert Gore (US Congress, 1991) created funding and authorization that expanded the Internet to civilian use. And while at CERN, in Geneva Switzerland, Tim Berners-Lee created a technology to allow non-technical individuals easy access to the Internet's data as the World Wide Web (Berners-Lee, *et al*, 1992). Based on these and many other contributions, computers have expanded beyond government and telecommunications operations to facilitate commerce and personal activities to create the Internet we know today around the world. This transformation has created an increasing reliance on technology and a need for pervasive cybersecurity within each company, each home, and each individual's affairs. It's been only 40 years since the days of wired analog phones and cardboard library catalogs.

As the pace of underlying information technologies accelerates (Kurzweil, 2005), cyber defense is not possible without preparing people to successfully sustain this rapidly changing world. Society needs these learners fluent in new technologies to design new cyber defenses and to become cyber defenders able to wield contextually relevant technical skills in action. Beyond technical skills, these professionals need to participate effectively in teams and across institutions, operating in a new type of engagement space that includes digitally enabled and in-person human interaction. It requires mental self-awareness to adapt agilely as rapidly evolving digital environments detach from the natural environmental cues where intuitive and instinctive responses have relevance.

Four lines of innovation are presented here that converged to allow for the rapid development of cyber defense capabilities when they are integrated to create coherent ecosystems of growth and capacity development. These include the creation of cyber challenges, the virtualization of digital systems in laboratory environments, the creation of immersive virtual scenarios where new ways of cyber-relevant thinking can evolve, and the creation of new inter-institutional organizational collaboratives that can prepare and respond rapidly to cyber incidents.

1.1.1 Cybersecurity Laboratory, Training, and Challenge Environments

Preparing cybersecurity professionals for these challenging careers and environments requires building new institutional capabilities at universities. These capabilities need to be agile enough to keep up with the ever-accelerating pace of innovation described above, and engaging enough to rapidly provide empowering skills and psychological astuteness in newly emerging domains of information systems resilience and cyber defense. This rapidly rising discipline goes by multiple names such as computer security, information assurance, and cybersecurity and is in the process of causing a significant shift in academia particularly since the year 2000 (Cooper *et al*, 2009).

In 2005, structural and resource issues were a strong indicator of preparedness as the survey of university cyber competitions indicates (Cooper *et al*, 2009). This generally meant heavy investment in hardware that needed to be deployed separately from standard university information technology operations along with the logistics and administrative work needed for physical deployment and maintenance. The exception was virtual private network tunneling (VPN) that could allow terminals distributed around a building to ride over the university's production network to a competition network (Hoffman *et al*, 2005). To address this challenge: new types of agile education infrastructure needed to be developed. New technologies need to be able to deliver hands-on cybersecurity experiences through the Internet to online students. New relevant digital environmental contexts in which to acclimate to cyber-driven environments became a requirement. New frameworks with which to orient oneself and team goals needed to be developed. And new psychological feedback methods to guide participants through this new digital landscape of learning, competition, and work were called for to help them become self-aware enough to adapt as traditional interaction cues faded into the past.

Examples of multi-institutional cyber competitions (Carlin *et al*, 2010) reflected a focus on Network Systems Analysts in 2010 when the Collegiate Cyber Defense Competition (CCDC) began to move to regional competitions. Select universities within each region of the United States were selected to host regional competitions that would lead to the national CCDC. At the time of the prior work presented here there were several groups moving in parallel to innovate cyber training, laboratory, and competition facilities (Carlin *et al*, 2010).

1.1.2 System Virtualization in Education

The popularization of microcomputer-based virtualization in education laboratories commenced around the year 2010, when this body of prior works begins. Early studies involved remote access of virtualized systems (Border, 2007). The challenge of selecting and using virtualization solutions was being explored by other groups in 2010. Li's work and that of Stackpole (Stackpole *et al*, 2008) (Li, 2010) generally focused on deploying sets of virtualized computer operating systems to deliver a variety of environments. The goals were often oriented towards rapidly instantiating machines that were customized to perform particular laboratory exercises. Stackpole particularly makes the assumption of high bandwidth availability as he defines the requirements from lab to lab in a campus environment. Li's work represents efforts to use systems virtual machines as a way of offering remote hands-on experiences, comparing VirtualBox™ and VMware™.

1.1.3 Virtual World Usage in Education

In 2004, Cyberceige was introduced at the Naval Postgraduate School as a flat space immersive game available on CD-ROM, and provided an experience interacting in an office environment with specific cybersecurity tasks (Irvine *et al,* 2005). It helped popularize the idea that scenario-based learning for cybersecurity could introduce more human factors and social/business context for cybersecurity learners. Parallel to this was work in 3D virtual worlds in a range of disciplines to leverage the immersive experiences that were becoming possible. By 2010, SecondLife® hosted a thriving community of education resources rendered by various institutions in 3D spaces. All of these virtualization tools were being used in corporations as well as many in education settings. However, organizing them across vendors and technologies was generally left in the institutions and end users. The US National Oceanic and Atmospheric Administration's Earth Systems Research laboratories offered an extension to learning management systems with an experiential immersion in a virtual space (Hackathorn & Explorer, 2006). Medical and Health librarians and educators offered a significant range of virtual world experiences on topics like nutrition, genetics, cardiology, and psychology. The US National Library of Medicine provided a $40,000 grant funding significant work in the SecondLife® region called Healthinfo Island. (Boulos *et al*, 2007). The physics community also had an extensive presence including the NASA's CoLab Island (Smith, 2008). Specifically, in regard to cybersecurity education, an open source 3D world similar to SecondLife® run on the OpenSim platform was used by Ryoo to allow students to experience a cyber attack in a game-based learning scenario (Ryoo *et al*, 2011). It could simulate packet flow with blocks lined in sequence and had a range of objects to simulate both technology and social experience. Preparatory experiences for certifications were also being offered in Second Life® specific for laboratory challenges like the Caesar cipher. encryption, and packet analysis (Choi *et al*, 2010).

1.1.4 Cyber Defense Collaborative Training

In the United States around the year 2010 at a state level, such as Colorado, the bulk of collaborative joint training exercises in preparation for societally disruptive incidents were being conducted by first responder institutions such as fire departments, police departments, and state National Guard units. The focus was on preparing for large scale events like forest fires and floods. Joint cyber training activities including government, military, and civilian entities in cyber defense generally have several challenges, whether hosted by universities or otherwise, because of the jurisdictional boundaries and scope of action limitations between participants and the need to independently protect the sensitive information of each party (Shider, 2011). The literature of cyber defense training of the time does not present psychometric evaluation of cyber defense teams, even though there is significant research on the use of cyber technologies in behavioral psychology as evidenced by the 15 years of publication of the Journal of Cyberpsychology, Behavior, and Networking (Wiederhold, 2020).

Some related psychometric evaluation is used starting around 2016 in relation to cyber threat deterrence (Adebiaye *et al*, 2016). By 2018 Sullivan indicated the significance of psychometrics as a future area of research in creating cyber resilience (Sullivan *et al*, 2018).

1.1.6 Background Summary

The background in each of these related areas can be viewed as converging synergistically in support of new areas of capability in cyber defense training capacity. When combined, they can lead to the development of new digital laboratory experiences, and authentic immersive virtual world training scenarios. Institutions can then leverage these virtualized systems to agilely deploy just-in-time learning environments and facilitate cyber defense collaboration and psychological support methods to expand this capacity and resilience.

1.2 Research Context

The author began personally developing significant cyber defense research aims while participating in communities focused on cyber defense education. Many of the theories and models in the prior works were first envisioned and presented by the author at those conferences. From 2005 to 2017, the author attended 9 conferences in the United States at The Colloquium for Information Systems Security Education, where institutions were setting up centers of academic excellence in cybersecurity and moving to rapidly accelerate the effectiveness and pervasiveness of cyber security education programs. The author is now the Editor-in-chief of the Journal of The Colloquium. Also in the United States, the author contributed to running the Rocky Mountain Division of the Collegiate Cyber Defense Challenge (CCDC) for 6 years from 2012 to 2017. The CCDC leadership worked vigorously to enhance the realism, relevance, and engagement of cyber competition exercises to help popularize, build, and validate cyber security programs across the US. The author designed competition scenarios and participated on live attack teams, competition infrastructure teams, and monitoring teams. Internationally, the author participated in the International Federation for Information Processing Working Group 11.8 on Information Security Education. Associated with that, the author presented in 5 World Conferences on Information Security Education since 2013. Currently the author is the Co-Vice Chair of IFIP WG 11.8. Other conferences of note where participants had influence on the author's research aims include the International Conference on Information Warfare, The Hawaiian International Conference on Systems Sciences, and CyberScience, organized in the United Kingdom.

Leading participants at these conferences were looking for ways to leverage emerging technology paradigms like virtualization, cyber challenge events, immersive instructional technologies, and collaborative opportunities. This general drive to advance the discipline was then carried over into the infrastructure and program development work at Regis University.

The 18 years of the author's work at Regis University teaching at the graduate level offered significant opportunity to make substantive contributions at the forefront of the field. The author led students in a variety of roles including advisor of the systems engineering and application development practicum for about 5 years, technical lead of the graduate research laboratory for about 5 years (as the exemplar for the current project scientist position), and Co-Director for the Front Range Center for Information Assurance Studies at Regis University for 3 years. These roles afforded relationships and opportunities to engage in experimental testing of hands-on instructional methods, testing of theoretical models, and first hand participatory observation of major multi-institutional efforts to enhance regional cyber defense training. These observations and collaborations raised a strong awareness of the new theory and practice that needed to be developed in order to increase the capacity of cyber defense training.

1.3 Research Aims and Methods

In the context of the above efforts to rapidly transform cybersecurity education and training, this research aims to advance the field of cybersecurity education in order to provide new capacity to meet emerging education needs in the face of greater societal dependence on information technologies and greater potential for disruptive cybersecurity events. The research aims to contribute to the body of knowledge at the forefront of the field by contributing theoretical structure and new methods in an area that must be integrated in order to help institutions achieve new capabilities. As learners use these theories methods to operate in reliable and authentic virtualized learning environments that simulate the challenges of cybersecurity work, they also need the intellectual tools to effectively function in this evolving space of operations.

The primary aim of this research can be divided into several goals necessary to agilely offer cybersecurity learning and performance enhancement experiences so that participants can respond to emerging challenges well prepared. These challenges include deploying technical environments that can rapidly change to maintain relevance, creating theoretical frameworks that can provide coherence and understanding in this changing environment, designing socio-psychological methods to enhance the potential of individuals and teams, and organizational challenges to mitigate risk and maintain relevance that are both inherently dynamic in contemporary cybersecurity education. The goals below directly address these challenges:

1. Devise new models of rapidly developing and deploying virtualized technology environments for education, professional training, and challenge events.
2. Create conceptual frameworks that enable learners with better modeling of the ways in which cybersecurity risks evolve, particularly where new risks are emerging through the transformation of traditional cybersecurity situations
3. Design novel methods for preparing and supporting cybersecurity experts to operate in an evolving digital landscape increasingly disconnected from the intuitive social, psychological, and physical situations where humans evolved.
4. Formulate new conceptual approaches and analytical methods for tuning cybersecurity learning environments, so that institutions can create programs that effectively bridge students to cybersecurity careers while minimizing both student and institutional risk.

How these goals are integrated can be seen as a set of common required inter-dependent functionalities and needs. As students move into immersive digital environments for their learning interactions, they will need new conceptual frameworks to understand the landscape. The use of these new virtual environments calls for some type of contextual frameworks to understand them. When a framework sets a new context for digital behavior in the virtual landscape, it’s easier to recognize that it is somewhat detached from the normal physical context. So, new tools of behavioral self-awareness naturally become the next goal, to help students better operate as individuals and teams within that space. When students are operating effectively in this virtual training environment, institutions will be responsible for

ensuring that the program maintains a strong synchronization to societal expectations, cyber defense roles, and the evolving digital landscapes where cyber defense actually occurs.
Because this work employs multiple allied disciplines, different approaches and research methodologies are selected within each published paper. The research methodologies include:

1. **Case Study:** Case Study is the most used research methodology in this body of work, primarily because a large portion of the work is based on the development of actual laboratory environments where particular events led to new conceptual modeling and understanding. Across the body of work it is used with varying degrees of formality. In the works that introduce models for analyzing identity or reality, a series of cases are analyzed using the introduced method in order to set broad coherence of understanding across the cases. In works where research relies on first-hand analysis of development within an operations environment, as in the work analyzing an innovative use of the SCRUM framework, the paper [P01] covers one case. The most formal usage in this body of work is in the analysis of a multi-agency collaboration using Agile methods on an education infrastructure [P02] (Smith, 1990).
2. **Quantitative Pre-post testing:** This method uses assessments for skill and understanding before and after a training event to look for differentials in student comprehension or performance where the events are expected to yield results with specific outcomes. It was used in this research to analyze the learning of students experiencing an exercise auditing a datacenter in the virtual world SecondLife® [P03] and in evaluating the technical advancement of participants in a multi-agency cyber security training program [P04] (Gall & Borg, 2007).
3. **Creswell's Interrelating Themes** is used where the primary data includes a range of different types and sources that can provide insight through cross-reflection. In this work the data sources include observation of a live cyber defense event and post-incident interviews. This method is used and described in detail in the research using collaborative training and response communities (CTRCs) as an alternative to traditional cyber defense escalation [P05] (Creswell & Creswell 2017).
4. **Creswell and Clark's two-phase explanatory design mixed methods research** is used where context contributed significant understanding of the quantitative results. Particularly this is used in evaluating a multi-agency cyber security training program [P04] to amplify the value of quantitative data about skill levels. In reviewing the initial results the author used follow-on qualitative methods that enhance understanding (Creswell & Clark, 2017).
5. **Secondary research:** This method of research is used prior to the formation of new theoretical models to provide contextual references, to build on prior research, and to determine relevance and novelty. It is also used when performing exploratory research to find similar experiments to analyze with regards to the benefits and risks of their approaches. The practice of secondary research used here generally starts with building a standard review of literature and then referencing and analysing the key relevant work. This method is used throughout the body of work. A specific case of usage is in *Managing the Loss of Control over Cyber Identity* [P06], where secondary research plays a lead role in surveying the challenges of identity management and perception and is used to determine the relevance and application of a model (Thorne, 1994).

During the time of this research, business and software development methodologies like the SCRUM Agile methodology (Potter, 2010) and the Capability Maturity Model (Paulk *et al*, 1993) were also used to facilitate and characterize the laboratory and training operations being studied. In conjunction with the new knowledge presented here, these development models contributed to the capacity of an active cybersecurity training environment.

The novel contributions presented in this prior work enabled the Regis laboratory to be the originating host for the Rocky Mountain region of the United States for the Collegiate Cyber Defense Competition for several years. This was true even though Regis was one of the smaller institutions in the region, with significantly less human and technological resources. It also led Regis to become a technical training ground for the Colorado National Guard's cyber defense team. The cyber incident response team analyzed in this research was the first National Guard team in the nation to be deployed in defense of a state government facility in the face of a debilitating international cyber attack as described in the author's paper *A Short-Cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense* [P07].

Assumptions regarding the prior work that provide context includes the following:

1. A university network laboratory for research, teaching, training, and competitions was the primary type of environment being studied in the infrastructure papers, supplemented by other networked and internet-accessible virtual world resources. While some initial cloud resources were available at the time, they are not the focus of the work.
2. The work on multi-method virtualization modeling [P08] was built on a particular set of specific technologies including application virtualization, systems virtualization, virtual world scenarios, and other virtualized media, but the method is designed with awareness of a broader range of virtualization types and is intended for broader application.
3. Full VR immersion with headsets were not practically implementable for large numbers of students at the time of the 3D simulation research.
4. The primary perspective of the work is that of a leader of an information systems and cybersecurity research and education laboratory working to formulate and contribute novel capabilities and generalizable knowledge needed to meet emerging challenges.

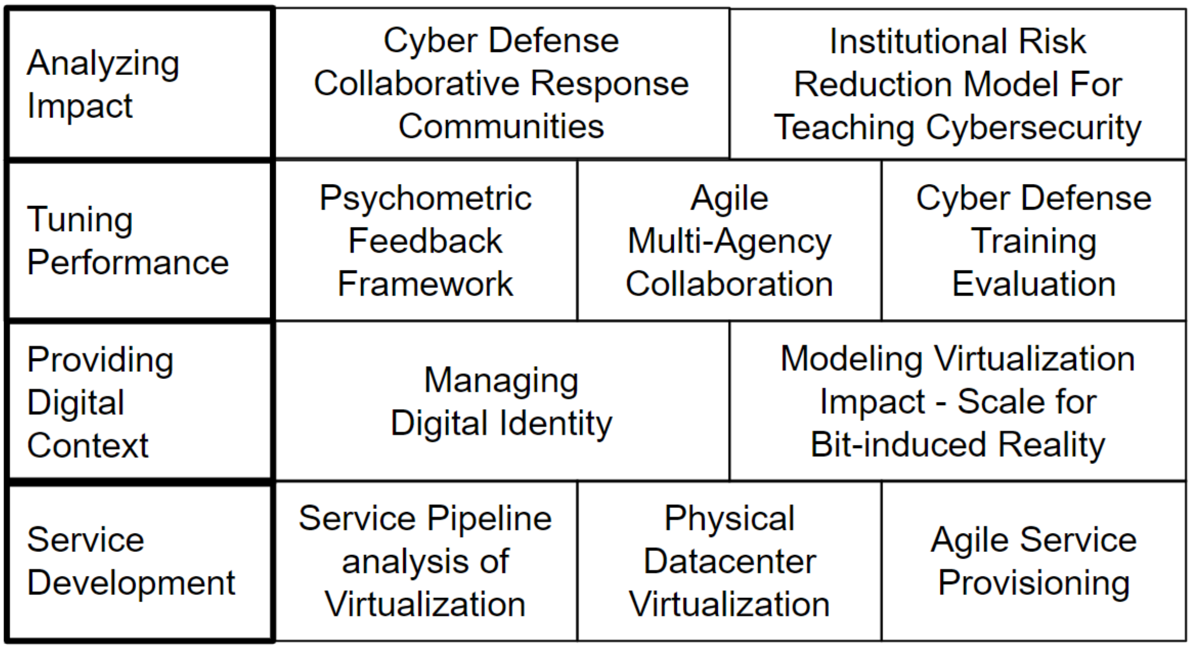
Given the research context, aims, and available methods, the research moved the capacity of cyber defense training forward incrementally, with different aspects of the work often in parallel as opportunities to innovate arose.

1.4 Thesis Structure

This integrative summary is divided into four layers of capability building, as illustrated in Figure 1. While the work is nearly sequential going from bottom to top, the design is intended to represent the higher layers' dependencies on the lower layers for functionality. The blocks within these layers represent new contributions to the field of cybersecurity as the work progressed to enhance the capabilities of institutions to deliver cybersecurity training.

The theoretical construct has conceptual similarity to the layered dependencies of the Open Systems Interconnect (OSI) model, where higher order protocols like HTTP run on lower order protocols and services like TCP and IP (Zimmerman, 1980). It also has similarities to the progressive capacity building structure evident in the Capability Maturity Model where new levels of capabilities are possible if prerequisite requirements are met (Marquardson & Gomillion, 2018).

Starting at the bottom, the *Service Development* layer is where technical systems and scenario building capabilities are established. As students immerse in virtual training systems, practical guides for dealing with the new virtual and digital contexts require models to help frame activities. This new digital context layer then became necessary work. As the range of work expanded to regional cyber competitions and joint agency training activities, the *Tuning Performance* layer work became necessary to expand capacity while maintaining quality outcomes with a very small team. In the *Analyzing Impact* layer, the researcher extended the analysis to a live cyber defense incident in order to provide an opportunity to tune the program design in relation to relevant outcomes. Additionally, creating a model to analyze the program for institutional risks provides a path to continue research.



Analyzing Impact	Cyber Defense Collaborative Response Communities	Institutional Risk Reduction Model For Teaching Cybersecurity	
Tuning Performance	Psychometric Feedback Framework	Agile Multi-Agency Collaboration	Cyber Defense Training Evaluation
Providing Digital Context	Managing Digital Identity	Modeling Virtualization Impact - Scale for Bit-induced Reality	
Service Development	Service Pipeline analysis of Virtualization	Physical Datacenter Virtualization	Agile Service Provisioning

Figure 1: Layered Concept Model that reflects a research structure of capacity building for cybersecurity education, training, and competition infrastructure

Regis University's cyber security program had students, professionals, government staff, and military teams training and competing on its cybersecurity training infrastructure. The cyber security training infrastructure became a place where students could meet challenges using both offensive and defensive components of cyber attacks. They used current digital tools in a way similar to what one might experience at a traditional munitions range in the military where new weapons are tested and new teams are trained. In the case of the Regis facility, teams are trained for cyber defense readiness. For about the last ten years in military environments, this type of active infrastructure space has been labeled a "cyber range" (Pridmore et al, 2010).

Section 2 provides an analysis of *Service Development* along with novel modeling from that work in a user-oriented and event-facing way. It provides a detailed narrative of the components of the published works. The Multi-Method Virtualization Strategy [P08] is the earliest paper in this body of work. Based on the metaphor of a pipeline, the modeling facilitates the creation of a stable environment built across a highly heterogeneous infrastructure primarily acquired by donation. Then the paper on agile provisioning of infrastructure services for cyber competition [P01] addresses both human resources and demand management in an unpredictable and resource lean environment. The final paper in Section 2 addresses virtual world infrastructure because a significant portion of the students were learning remotely on-line, and the tours of technical facilities that were customary earlier were no longer accessible due to the heightening of security around datacenter facilities at the time of the 9/11 World Trade Center disaster [P03].

Section 3 presents the ways in which this work is *Providing Digital Contex*t by introducing novel modeling methods for mapping out the new cyber landscapes in which participants learn and work. The work *Managing the Loss of Digital Identity* [P06] can apply as much to the unexpected system resets that students feel in a digital laboratory experience when work is lost, as it does on a societal scale when banks, universities, and credit agencies are hacked, leading to a loss of online communications and digital content. The work on modeling the impact of virtualization on changing vulnerabilities [P09] concludes this section by presenting an innovative model for dynamically tracking changes in technical and human systems as these systems' characteristics are increasingly "bit-induced" by digital manufacturing, electronic automation, software enhancement, and virtualization.

Section 4 examines contributions in the area of *Tuning Performance* of the training systems described in the first two sections by introducing specific cases where new methods are introduced to provide both real-time analytical methods [P07] and outcomes in relationship to multi-agency collaboratives [P04]. The context of analysis expands beyond earlier sections to include learner tracking across institutions and multi-institution goal-setting [P02].

Section 5 focuses on *Analyzing Impact* in relation to the outcomes of the cyber defense training efforts. First, a case is presented where a cyber defense team that trained using these techniques responded to a debilitating cyber attack on the State of Colorado [P05]. The analysis in this case uses a novel conceptual approach based on the team's ability to take over both incident response and operations load during the incident. Then considering the negative outcomes that can occur in cybersecurity training, the closing paper considers participant behavior in terms of individual and institutional risk [P10]. Two new analytical techniques are included, creating topological maps of participants' full range of behavior, and reviewing curricular content for appropriate curriculum-centric risk reduction given that range.

Section 6 provides analysis of the *Current Impact and Relevance* of this body of research, reviewing both direct impact with specific examples and the context presented regarding the current trajectory of related works.

Section 7 offers a *Conclusion* to the work, describing the specific research contributions, limitations of the work, and plans for future work.

Following the reference list, *Appendix A* lists the published prior works and includes bibliographic information, abstract, the time and location of the research, and the Ph.D. candidate's specific contribution. Appendix B, contains copies of the confirmation letters from co-authors, affirming the nature and level of the candidate's specific contributions to all of the co-authored works.

2 - Service Development

The three papers at the service development layer present innovative adaptations of emerging infrastructure technologies and methods that provide simulated cybersecurity scenarios.

- Multi-Method Virtualization: An Architectural Strategy for Service Tuning [P08]
- The Use of Second Life® to Teach Physical Security across Different Teaching Modes [P03]
- Developing Cyber Competition Infrastructure Using the SCRUM Framework [P01]

Some of the early challenges in developing cyber training and competitions involved the rapid deployment of whole virtualized network environments. Early on, the Regis University team saw advantages in moving to virtualization, even locally, instead of deploying systems directly onto new physical switches and servers. The local challenge for Regis was sustaining a consistent team capacity to agilely design, set up, and host large competition events on site with a relatively small number of faculty and graduate students involved in supporting the academic research network. The avatar-based virtual 3D scenarios providing physical security training did not rely on the laboratory infrastructure, except for robust clients with many students needing bandwidth as they logged in simultaneously. Together, these efforts created a rich environment of experience for academic students, professionals in training, and competitors in cyber challenges.

2.1 - Multi-Method Virtualization - A Pipeline Model for Service Tuning

To address the complexities of designing large sets of virtualized systems, this novel “pipeline” modeling system [P08] was developed as a multi-method virtualization model based on the functional requirements presented by the leadership of the information technology training lab. This pipeline modeling system is a way of representing the topological relationships of processing nodes, bandwidth vectors, and nested virtualization to consider the overall efficiency and capacity of a deployment design on a particular infrastructure. The author developed and used it to increase efficiency of the performance tuning of interactive training resources and in the design process of distributed virtualized systems given a large number of technologies and a complex underlying technological infrastructure. The infrastructure included varying user devices, network segments, and server system capabilities. The pipeline model in Figure 2 was primarily used to design delivery of services like cyber training and research laboratory experiences to remote students around the world, or to students competing on teams in separate rooms within the building. At the time of this work, multiple methods for virtualization existed such as remote screen rendering, client-based virtual networks, and server-based centralized systems of virtual machines where multiple parties could interact.

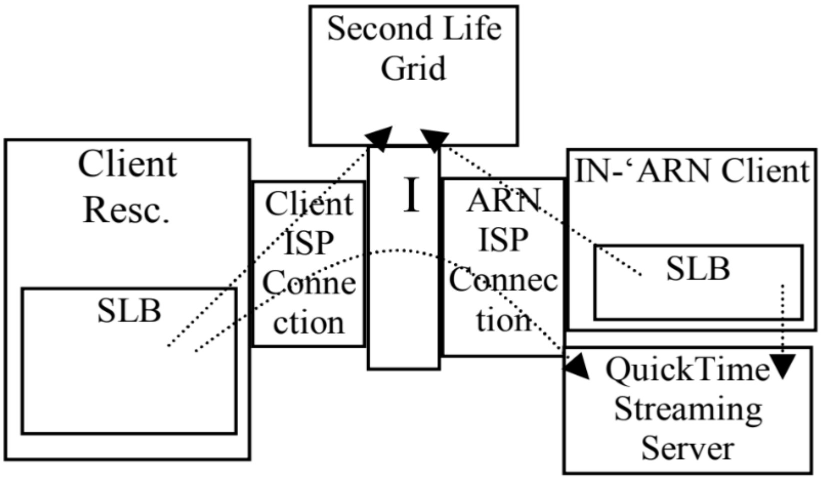


Figure 2: A Service Pipeline Model mapping a streaming teleconference feed from the Regis Academic Research Network (ARN) to a console embedded in a SecondLife® virtual world operations center using the SecondLife® browser (SLB) all connected by the Internet (I)

The author's research on the service tuning of virtualized services presents two innovative modeling methods that the author developed based on the use cases formulated by the co-author to describe educational needs. This pipeline model analysis is usually preceded by the Virtual Layered Model analysis in Table 1 that emphasizes a layered approach similar to the OSI network model (Zimmerman, 1980) and the SNIA storage model from the Storage Network Industry Association that is used to design and support large storage area networks (Yoder, 2001). Using these two modeling methods in a generalized approach, one can formulate a design to address particular questions of multi-product virtualization. Once layering is established, the design process introduces a novel "Service Pipeline" model that nests layered virtualization across the full path from the point of origin in the datacenter to the client workstation. A unique value of the models is the ability to represent the topological location of compute, virtualization, aggregate capacity, and connection speeds so that the virtual systems designers can better adjust processing locations and data transfer bandwidth to expected system performance requirements.

The Virtualization Layer Model (VLM) represents multiple layers of virtualization that are conceptually orchestrated as layers of potentially dependent functionality to create the training environment. A key characteristic of this model is the listing of technology options that is structured in the same way that laboratory designers access the work. For instance, SecondLife® has servers, storage and network systems underlying their technology, but the Regis University administrators need only list its server requirements at the Community Social Layer and then analyze the lower layers only in relation to the client. Other social layer technologies like learning management systems (LMS), may be run on local servers and require full stack analysis for the server. Other systems like a GNS3™ that emulate networks to support actual operating systems interacting over TCP/IP, may be accessed through virtualized applications at higher layers, such as the Citrix™ remote application virtualizer or SecondLife® where one's avatar might sit at a console in a virtual world to fix a network in a scenario in GNS3™ where the scenario suggests that an on-site service call is made by the learner.

Table 1: Virtualization Layer Model (VLM), This table represents a layered categorization of virtualization technologies providing services that build on the lower layers.

Layer	**Technology Options**
Community/Social	SecondLife® OpenSimulator™ Adobe Connect™ TeamSpeak™ Sharepoint ™ Portal Moodle™ LMS Angel ™LMS
Application	Citrix™ (XenApp™)
System	VMware™ Virtual Box™ Xen™
Storage	HDS Thunder™ HP EVA™ iSCSI software
Network	GNS3™ Cisco™ VLANning VMware™ Virtual Networks

2.2 - Agile Service Provisioning

The work to formulate a new agile training delivery method [P01] was performed on the Regis university infrastructure to deliver a cyber competition in the State of Colorado known as CANVAS (Computer and Networking Virtualization and Simulation). That existing infrastructure was designed using the service pipeline model. Based on the work preparing for CANVAS, the author worked collaboratively to establish a new application of the SCRUM (Schwaber & Sutherland, 2013) development methodology referencing the vision of the Agile Manifesto (Beck *et al*, 2001). The reason the SCRUM methodology was selected was because the author and others recognized the artifacts of standard project method dysfunctionality in the earlier similar work that is particularly addressed by the SCRUM design. The primary dysfunction noted was that the rate of requirement change and resource change was much faster than the planning cycle, so that the early CANVAS infrastructure development project work would often become desynchronized. The new development method based on SCRUM facilitates training event production in an agile way with a very lean staff of faculty and ever-changing set of student volunteers. The method is intended to help in the design of sustainable service assurances to regional partners such that Regis University could consistently hold quality training events even though human and technological resources were sparse. The primary goal of the research and training network at this point evolved from exclusively virtualized classroom laboratories for hands-on exercises to also include cyber competitions like the Rocky Mountain regional event for the Collegiate Cyber Defense Competition in the US.

This research introduces new methods to training infrastructure event deployment. The author's contribution was designing ways to adapt the new agile methods to the existing virtual environment and developing ways to incorporate it into the work that previously used the standard SDLC (systems development lifecycle). The agile SCRUM method allows for "chunking" work into reasonably sized components that could be performed in parallel by different teams, and at the end of each sprint when the chunk is complete an incremental completion check can be performed. This process enabled assignments, task completion, and the whole challenge of delivering a cyber event to be much more doable with less staff training in preparation for holding cyber events. Regardless of scale, the agile model is intended to facilitate adjustment, reassignment, and rapid rescheduling. Valuable aspects of this analysis includes consideration of how Potter's comparison of Carnegie Mellon Institute's CMMI (Capability Maturity Model Integration) and SCRUM (Potter, 2010) increased the ability to offer cyber competitions and how risk management can additionally be used to steer development in the face of hard deadlines.

2.3 - Physical Datacenter Virtualization

Outside of the virtual infrastructure of Regis, the author contributed to the development and analysis of a related virtualized learning environment, a virtual world scenario of a physical datacenter. This contribution [P03] was made in collaboration with co-authors from Idaho State University.

The Second Life® virtual datacenter project described here was instantiated in a temporary space called a "public sandbox" for the initial experiment in the avatar-based virtual world Second Life®, then moved to a space in SciLands hosted by the University of Denver near their nuclear reactor simulator. The datacenter project focused on achieving experiential similarity with the job of physical security auditing. The experience was designed to challenge learners to practice the spatial recognition of complex physical security issues. The scenario represents a novel contribution by addressing cybersecurity challenges where spatial recognition and experiential memory, acquired while walking through space, were the primary skill underlying the understanding.

This research aims to enhance the capacity to train students in physical datacenter security auditing by creating immersive cyber security learning experiences. With the advent of the 911 World Trade Center disaster in New York City, security across the US was tightened and it became hard to gain access to datacenters, particularly to teach students how to point out their security vulnerabilities. Thus there was a strong recognition that an alternative to actual datacenter access was necessary, and that a virtualized version of a datacenter might be able to fulfill the requirements of teaching requisite spatial recognition skills. An example of the type of spatial recognition is the location of a water pipe over a computer rack. Datacenters must have both water pipes and computer racks, but recognizing that the spatial situation as unacceptable is something the authors saw as problematic to teach using text-based, video, or photographic media that either point to the issue or overtly describe it in a way that prompt the learner too strongly in the discovery process.

The research team tested the efficacy of this scenario using the cyber training environments of Regis University and Idaho State University to access the models in the SecondLife® cloud.

The 3D model for the scenario is a virtual world data center building where students log in as avatars and walk through the space, taking on the role of a physical security auditor. It is designed to both train and test the activities of the participant in the role of a physical security auditor. Students participate in the virtual world by identifying risks in relation to access control, operations security, safety, business continuity, and resilience.

A professional physical security auditor in reality must call out spatial relationships between things like computer monitors with sensitive information being displayed facing windows, Halon™ fire suppressant nozzles installed in office areas. The intent of the model is to achieve a higher degree of validity of detection by requiring participants to use spatial recognition skills in a way prompted solely by the environment. An additional advantage of the virtual world version was that the author was able to make the exercise available to online classes and distributed groups in ways that tours through actual datacenters did not allow.

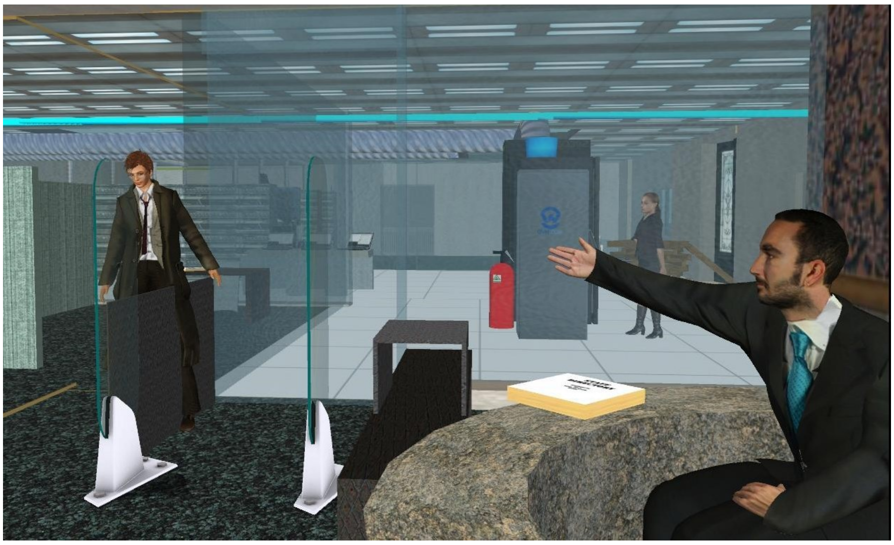


Figure 3: Looking from the lobby into the Virtual World Datacenter, where students train for the role of physical security auditor as they test their spatial skills

In this paper, the primary goal of the research is to compare efficacy across three different teaching modes, classroom-based learning, online learning, and a hybrid between the two. The participants assessed were from Idaho State University, Capitol College in Maryland, and Regis University in Colorado with an n=43 including all sites. Pre-tests and post-tests were used. The authors evaluated the resulting data with the one-way ANOVA analysis method, but the variance between group size was too great. While the quantitative results are presented in the paper, the qualitative analysis did add significant value, reflected in the descriptions of student behaviors within the virtual space.

3 - Providing Digital Context

Two papers with more theoretical content provide new frameworks for digital context and new tools for cyber contexts to help with interpreting the paradigm shifts experienced by students newly introduced to these new types of training environments that universities now call cyber ranges. In these spaces, instinctual responses and the intuitive responses developed in ordinary human life experience are less valid. This can lead to disorienting, desynchronizing, and potentially troubling responses to complex cyber environments (Aiken, 2016).

- A Vulnerability Model for Bit-induced Reality [P09]
- Managing the loss of control over cyber identity [P06]

The framing models presented in these papers also have application beyond the cyber range environment. A tank is an example of a military vehicle that can become more automated, and the bit Induction model may provide helpful insights into the changing risk. As physical tank becomes digitally enhanced it can incur new cyber vulnerabilities. For instance, a tank may be enhanced with an internal 3D metal printer to reduce the burden of a large supply chain requirement for many unique spare parts in remote locations of the world. Now the tank's CAD drawings of its parts become a target of attack. In the cyber range and in cyber defense, the context of engagement can be disorienting on multiple levels, and cause disruptive events. As observed by the author, in cyber competitions students can easily lose the frame of reference required to effectively "social engineer" or counterattack in-scenario during a competition and instead present behavior that is disruptive to the overall competition. Understanding these non-intuitive digital contexts is a significant part of succeeding in both cyber defense training and in similar immersive digital environments during actual cyber defense. To briefly mention an example of note, the attack on the Estonian banking system, where social sentiment and attack script distribution led to a massive human-caused denial of service attack (DDoS) that dramatically affected the economy of Estonia. The fact that it was incited by the move of a statue from one public square to another emphasizes how cyber contextual frameworks are becoming more important when considering the impact of societal events (Herzog, 2007).

In a cyber range, the initial cause of this disorientation is the introduction of the participants into the digital space of engagement itself. The sense of locality of action is compromised, objects and communications paths become ephemeral, and identities require different types of confirmation. This can have a negative impact on students. Thus the earlier work in virtualization produced the new requirement to build frameworks that could facilitate contextual awareness of the new risks within this environment and the self-awareness necessary to consider the implications of their actions and manage their triggered psychological responses as the digital context rapidly changed. The research is presented in a generalized format designed to provide value beyond training environments with the goal of supporting students as they take on cyber defense challenges in their careers.

3.1 - Modeling the Impact of Virtualization

This research on how virtualization impacts risk [P09] resulted in the development of a model that contextualizes the various types of virtualization. Coined in this paper is the term "bit-induction" which represents a quantitative measure for how much artifacts in any system or environment is induced, spawned, or created by digital information. The results of the research also includes a conjugate pair scale balancing physical and psychological significance. These scales help identify what emerging vulnerabilities might need to be considered because of an increase in bit-induction level. This idea of bit-induction levels provides a way to represent how an object's qualities increasingly rely on digital information for its characteristics and functionality as computers are introduced into its production. Starting at a low bit-induction level, a craftsman making a table by hand may be guided by a computer aided design (CAD). Moving up the bit-induction scale, a 3D printed gear is made by a digitally controlled machine without the craftsman's intervention. Further, a digital watch cannot display time without underlying active digital controls, and thus it is no longer functionally a watch. At the highest layer, a cup of coffee being used in a virtual world by an avatar cannot even exist without underlying active digital systems. The bit-induction model provides a framework for understanding these implications as functionality is moved from a lower level to a higher level of bit-induction. The model analysis both facilitates cyber training infrastructure design and provides students with better contextual understanding as they move through a range of virtualized and physical training environments.

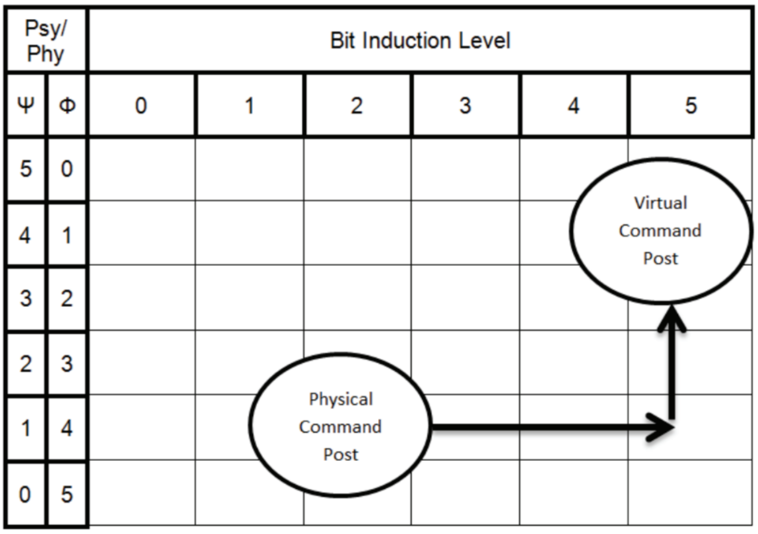
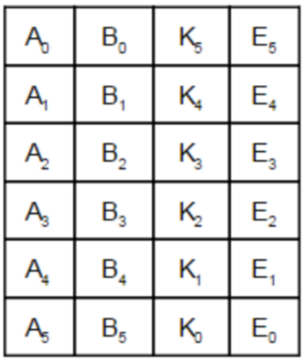


Figure 4: The Psy-BIR-Phys Model showing a case where a command post is virtualized and the resultant change from a dominant physical presence to primarily psychological functionality

Once the bit-induction and physical-psychological scales are introduced in the paper, they are used in a matrix to analyze a range of cases from 2013. When the analysis is complete, the variance is considered in relation to the Common Vulnerability Scoring System (CVSS) (Scarfone, 2009). In common practice CVSS is used to analyze a particular case at a single point in time to identify vulnerabilities along set characteristics like local network access, physical exposure, and Internet connectivity. The novel contribution of the bit-induction modeling is that a variation in vulnerabilities can be tracked when transformations occur even when classical vulnerabilities appear to be static. 3D printed gun laws in the United States for instance went through a four-year trial that could be tracked in this matrix, after which the distribution of 3D gun design files became legal until it became illegal again in November 2019 with a new injunction (Zaveri, 2019).

3.2 - Managing Digital Identity

The paper providing a conceptual model to assist with managing digital identity [P06] presents steps for addressing identity issues beyond the technology and beyond the process of authentication, authorization, and managing user accounts. This work is formulated as a curriculum-supporting resource to assist young cybersecurity professionals in managing the compromises of personal identity for their users, and in facing the risks inherent in their field. It also was used to address issues occurring on the cyber range. In addition, the work includes analysis of behavioral and societal implications of various ways of managing identity and the potential residual impact of those approaches.



A_0	B_0	K_5	E_5
A_1	B_1	K_4	E_4
A_2	B_2	K_3	E_3
A_3	B_3	K_2	E_2
A_4	B_4	K_1	E_1
A_5	B_5	K_0	E_0

Figure 5: Conjugate pair model for *Knowledge*(K_N)/*Belief*(B_N)with *Allegiance(*A_N)/*Ethics*(E_N)

The model was self-published by the author in "VPL1.0 Visual Philosophy Language, From Metaphysics to Metadata" (Moore, 2007). This general philosophy book is not included in the body of prior works. The VPL matrix represented in Figure 5 specifies technical definitions of each variable's level to make the quantification more accountable. Italization of the terms below indicates specific technical definitions briefly described in their application in the 2016 paper where it is then applied to a cybersecurity context to facilitate management of the disruption of digital identity.

The model aligns a *knowledge*/*belief* conjugate pair on the inner columns with a related *allegiance*/*ethics* conjugate pair on the outer columns. *Knowledge* is defined as an incremental rise from level zero to 5 representing increased effort and ability to comprehend complex patterns in evidence and observation, increasingly relying on larger communities of critical and scientific thinking. Running conjugate to that (similar to how pH runs in conjugate to pOH in acids and bases) is *belief*, which supports assertions with ever increasing insistence of surety from zero to 5, rationalizing its enforcement in the face of contradictory evidence and rational argument. The *belief* scale also requires ever greater personal and social effort as enforcement of belief approaches level 5. Moving to the outer columns, the level of rational *ethical* consideration is dependent on the level of *knowledge* of the consequences of an individual's actions, so moving outward in the grid suggests the level of potential moral consideration. Increased *belief* triggers greater deference to an authority for what to be *believed,* thus spurring increased intellectual dependence and *allegiance* as the resolving factor in the face of moral dilemmas. Historically, *allegiance* morality can be seen in the military structure of following orders at odds with what one might choose personally. The 2016 paper suggests how moving communications and user training up the *knowledge* scale could potentially de-escalate partisan or hostile tendencies in a population during incidents where cyber identity is disrupted.

The identity research of 2016 surveys the cybersecurity and psychology literature regarding the escalating dependencies and risks of digital identity as digital technologies pervade human interaction. The work includes evaluation of several psychological models that provide aligning insight into the management of identity. The result of that analysis suggests that the *knowledge/belief* model might help guide cyber responders to cue their users to more resilient behavior by de-emphasizing adversarial language and instead using knowledge-empowered collaborative language that focuses on creating greater cybersecurity resilience.

4 - Tuning Performance

The next three papers focus on tuning the performance of training, particularly the face of emergent cyber threats against regional and local governments.

- Evaluating a Multi-Agency Cyber Security Training Program Using Pre-post Event Assessment and Longitudinal Analysis [P04]
- A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure [P02]
- A Short-Cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense [P07]

With the assumption that context is provided at a lower layer of capability, the first paper in this section presents a model of research for analyzing technical performance of participant teams along with a method for tracking personal learning when multiple participating institutions are having an effect on individual progress. This accounts for training events, commercial certifications, and self-study. The research presented in the second paper in this section pushed agile methods from infrastructure resource deployment to joint development practices with collaborating institutions, leaders, and to a certain degree, the participants. Then Xmodels are introduced to illustrate the participant relationships. In the third paper, two new collaborators within the disciplines of psychology and sociology worked with the training teams and became co-authors, helping to develop psychometric feedback methods similar to those used in corporate management training programs. Those methods were customized to provide teams and individuals with both self-awareness and the ability to adapt behavior within timeframes that enable a new potential to yield feedback capabilities within the timespan of a single cyber defense incident or training event. The third paper then introduces a new integrative model to develop an aggregate timeline where psychometric observations, behavioral logs, and digital events can be better analyzed in a common context.

4.1 - Evaluating Multi-Agency Cybersecurity Training

The paper describing the development of a method of longitudinal analysis for cybersecurity training [P04] presents original work in a multi-agency collaborative context where governmental cyber defense is the primary objective. The primary goals of the training were logging and monitoring, coding and scripting, network and systems analysis, auditing and compliance, and interpersonal skills. These skills were tracked in the context of what a co-author named a Personalized Experiential Learning Environment or PELE. In the PELE framework each participant tracked learning from job-related certifications, professional development, and military training. As the data was analyzed over time, trends of improvement emerged that reflected the aggregate effort by the training community. The pre-post data to the cycle of training also allowed for rapid modification of the training activities where additional effort was needed. As will be seen in the sections below, this led to the inclusion of additional disciplines in training development and the introduction of Agile methods into the joint training development process.

This work was analyzed within the experimental structure of Creswell and Clark's "two phase explanatory design mixed methods research" where both qualitative and quantitative research contribute to the context and meaning of the analysis (Creswell, 2017). This method appeared to be more appropriate because n=30 was an insufficient population to account for the various institution-specific and individual-specific factors outside the joint events that led to skill enhancement over the three-year period. The authors then worked through the qualitative analysis to attribute and qualify the growth in capabilities of the training participants.

4.2 - An Agile Joint Collaborative Training Model

The earlier research to enhance training deployment agility [P02] began to involve participant institutions in the agile cyber defense training development cycle. The earlier agile work was used only internally in the Regis cyber range production group. In this new work the training leadership team, including some of the authors, developed a three sector model for engaging governmental entities, defense teams, and educators in rounds of development. This was later augmented with private companies and turned into a four corner Xmodel as the collaborative group acknowledged the large role that private companies play in actual incident response. After-action reports and gap analysis led to the rapid development of simulated events, tabletop exercises, and training goals. A critical finding was that the use of agile methods in training delivery initially had the negative effect of desynchronizing the participant team members' expectation of formal structure. After this realization, new emphasis was placed on sharing the agile methods with participants and tuning their expectations and attention to agile goal setting.

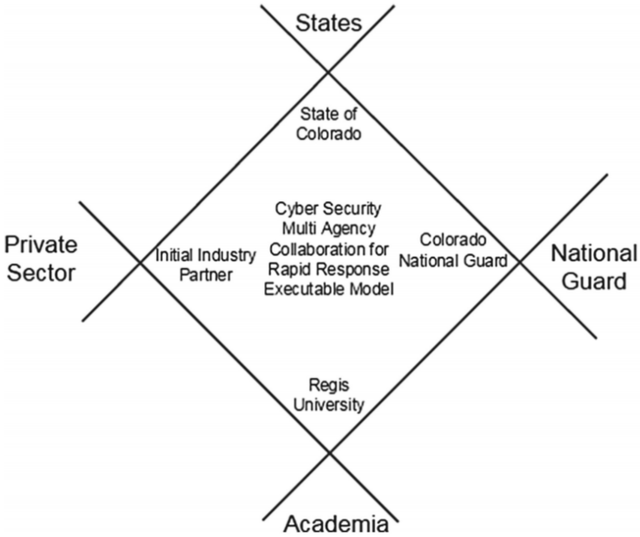


Figure 6: The second phase of the Xmodel of collaboration and cooperation, allowing for generalization and greater agility of peer forming and sector coverage

The research on agile methods for joint training development uses the case study research methodology and lays out a timeline of the application of the agile development methodology. Along this timeline is shown an increasing inclusiveness both within government sectors and across sectors like the later inclusion of private security companies. The models presented are designed to be extensible and generalizable to some degree for any institution wishing to engage agile methodologies in the development of broadly collaborative work.

4.3 - Short-Cycle Psychometric Feedback

Short-cycle psychometric feedback method [P07] represents a new direction for adding value to cyber defense training. Prior to its development, Regis faculty and National Guard leadership had been looking for new ways to increase training capabilities that were being developed for activities in the cyber range. A co-author, Likarish, suggested inviting faculty from the Regis University Rueckert-Hartman College for Health Professions and the College of Contemporary Liberal Studies to develop a new path that could leverage those disciplines. These new faculty collaborators performed psychometric analysis on the teams as they engaged in cyber defense training. Then when an actual cyber defense operation occurred, the defense team leadership offered the Regis psychometric analysts an opportunity to record observations on site during the defensive action. These observations along with the baseline psychometric analytics from training became the basis for the short-cycle psychometric feedback model presented in this body of work. It is designed to support actual cyber defense operations with pre-scripted coaching hints based on real-time observations. An example of a pre-scripted coaching hint directed towards a leader could be, “Make sure team members are reaching out to each other with updates since the group cohesion is dropping.”

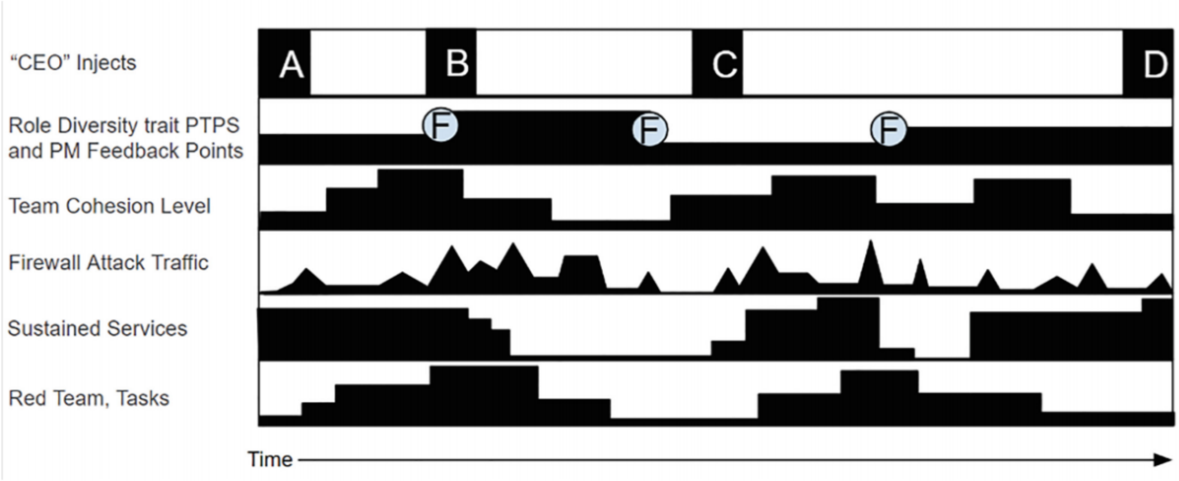


Figure 7: A model for the short-cycle framework, aggregating information types to facilitate relevant psychometric feedback during cyber defense training and incident response

A challenge with the psychometric data is how to rapidly respond effectively to the real time interpretation of changes in factors like team cohesion. Through collaborative efforts the timeline-oriented model for the short-cycle framework was developed so that it could be used to interrelate digital attack events with psychometric observations and other activities occurring in training events. Aggregation of the timeline is not yet automated, so it is currently intended to be first used for post-event analysis rather than feedback in support of active events. One research and analytical method chosen to collect the psychometric results here is based on the Myers-Briggs Type Indicator (MBTI) instrument for determining personality traits (Myers *et al*, 2003). The Role Diversity trait of the Parker Team Player Survey is another observable measure that is dynamic and can yield points of coaching feedback, labeled “F” in Figure 7, from the psychometric monitors (Parker, 1990).

Figure 7 presents “CEO” injections along the top where a competition staff member represents a chief executive officer in a fictitious company in scenario. During a training session students will be assigned a vulnerable system to defend and challenged with live cyber attacks. During this time, to simulate a real work environment, a staff member with the role of “CEO” will interrupt the team with “injects” (labeled A,B,C,D) that are ongoing business requirements such as generating reports, standing up servers, or responding to customers even in the midst of an incident. These injects are expected to show significant effects when tracked over time with other events and are generally scored in cyber challenge events. Setting up the aggregate timeline offers the possibility of seeing where injects, psychometric feedback, and live attacks can trigger changes in team both dynamics and individual engagement.

5 - Analyzing Impact

Beyond conceptual frameworks that describe the cybersecurity landscape for learners and professionals, another key requirement of building capacity in cyber defense programs is the need to confirm and sustain the effectiveness of the learner beyond education. Two papers present this analysis, introducing new tools designed to assist in understanding cyber defense training program effectiveness, objectives, impact, and relevance.

- Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation [P05]
- An Institutional Risk Reduction Model for Teaching Cybersecurity [P10]

These two areas of research differ in that the work on collaborative training outcomes is about enhancing intentional value while the work on institutional risk reduction is about mitigating unintentional negative outcomes of training. These two papers address a broad layer of research where more work is required in order to fairly assess the net effect of cyber defense training programs.

5.1 Collaborative Response Communities

This research into the efficacy and dynamics of collaborative response communities [P05] extended the scope of analysis to an active cyber defense operation composed of the cyber defense team that received training during the collaborative training events at Regis. The contribution also includes the development of a new model representing the impactful load on the operations team observed along the incident timeline of the event. It models the operationalized capabilities that collaborative cyber defense communities can offer. The cyber defense event described in this paper was the first time in the USA that a National Guard cyber defense team had been called to support a state agency, the Colorado Department of Transportation (CDOT). CDOT was under a sustained and debilitating strategic ransomware-based cyber attack when the state called on the Guard.

The research methodology used in this paper is Creswell's interpretation of meaning which defines how to interrelate a set of themes, along with gathered descriptions, to create a system of cross-validation and norming (Creswell & Creswell, 2017). Used in this approach is a set of interviews and modeling analysis to provide both specific event details and generalizable knowledge.

In Figure 8, the left side of the timeline represents normal operations for CDOT. When the incident occurs, incident response load (IRL) takes over the whole team's time, eventually minimizing the ability to do basic "Keep the Lights on" operations required to run the business. Then the CDOT operations team begins to work overtime and experience burnout fatigue. As the Collaborative Training Response Community's Colorado National Guard team engages they take over not only the overtime, but a significant portion of the CDOT incident response load, so that the team can recover and build some slack time into their efforts to keep the work sustainable. The Guard can do this because they have trained with CDOT.

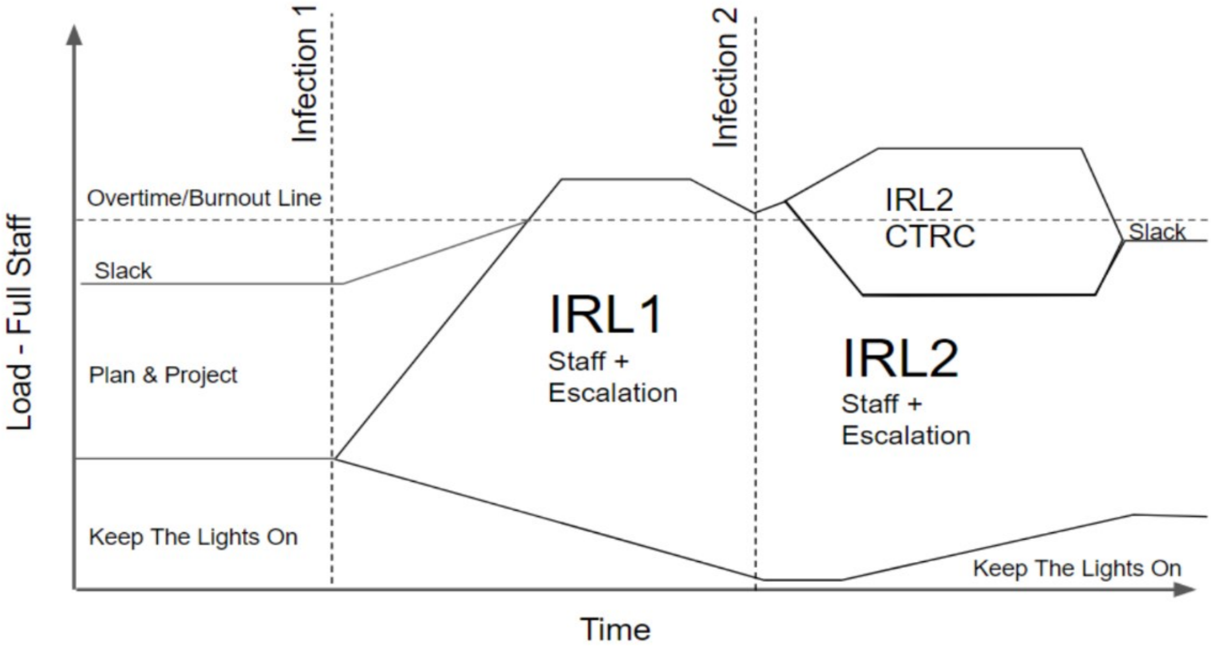


Figure 8: A cyber defense incident timeline reflecting relative load of tasks that are supplanted over time by the first Incident Response Load (IRL1) and how the Collaborative Training and Response Team (CTRC) provided relief after variants reinfected the institution

5.2 Institutional Risk Reduction for Teaching Cybersecurity

An emerging capacity requirement for all institutions teaching cybersecurity is the ability to recognize the risks inherent in teaching cybersecurity skills that have the potential to be used unethically against the institution or others (Marcum et al, 2014). While many institutions at the time of writing have implemented ethical components to their courses, the capability to broadly review institutional responsibility in mitigating this risk does not receive broad attention in cybersecurity literature. The contribution presented here [P10] includes two novel conceptual frameworks for addressing institutional risk across a range of technical and sociological controls. The institutional cases where these frameworks were applied included compulsory public education of legal minors, undergraduate and graduate college programs, and training for cybersecurity professionals and national defense teams.

The first conceptual model developed in this work maps out the range of behavior of the cybersecurity learner. This map initially appears to be a diagram of networks, but it represents domains of digital behavior where ethical choices must be made that are influenced by institutional practices. Education institutions incur multiple types of risk and responsibility as they teach invasive cybersecurity practices that, once in the minds of the learner, are not restricted to the laboratory where they were learned.

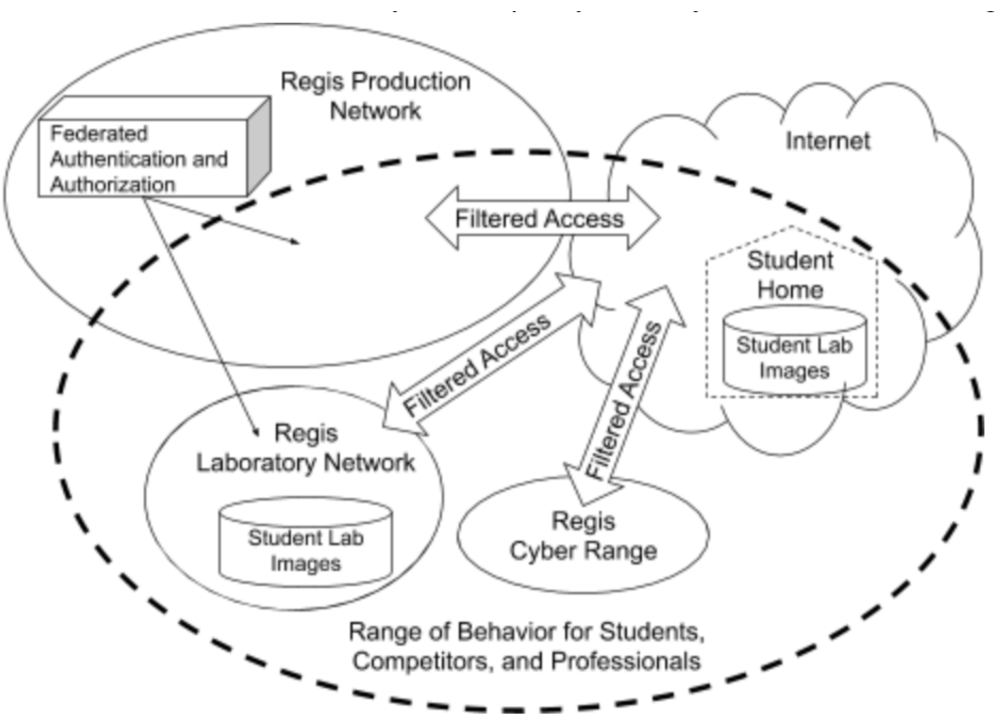


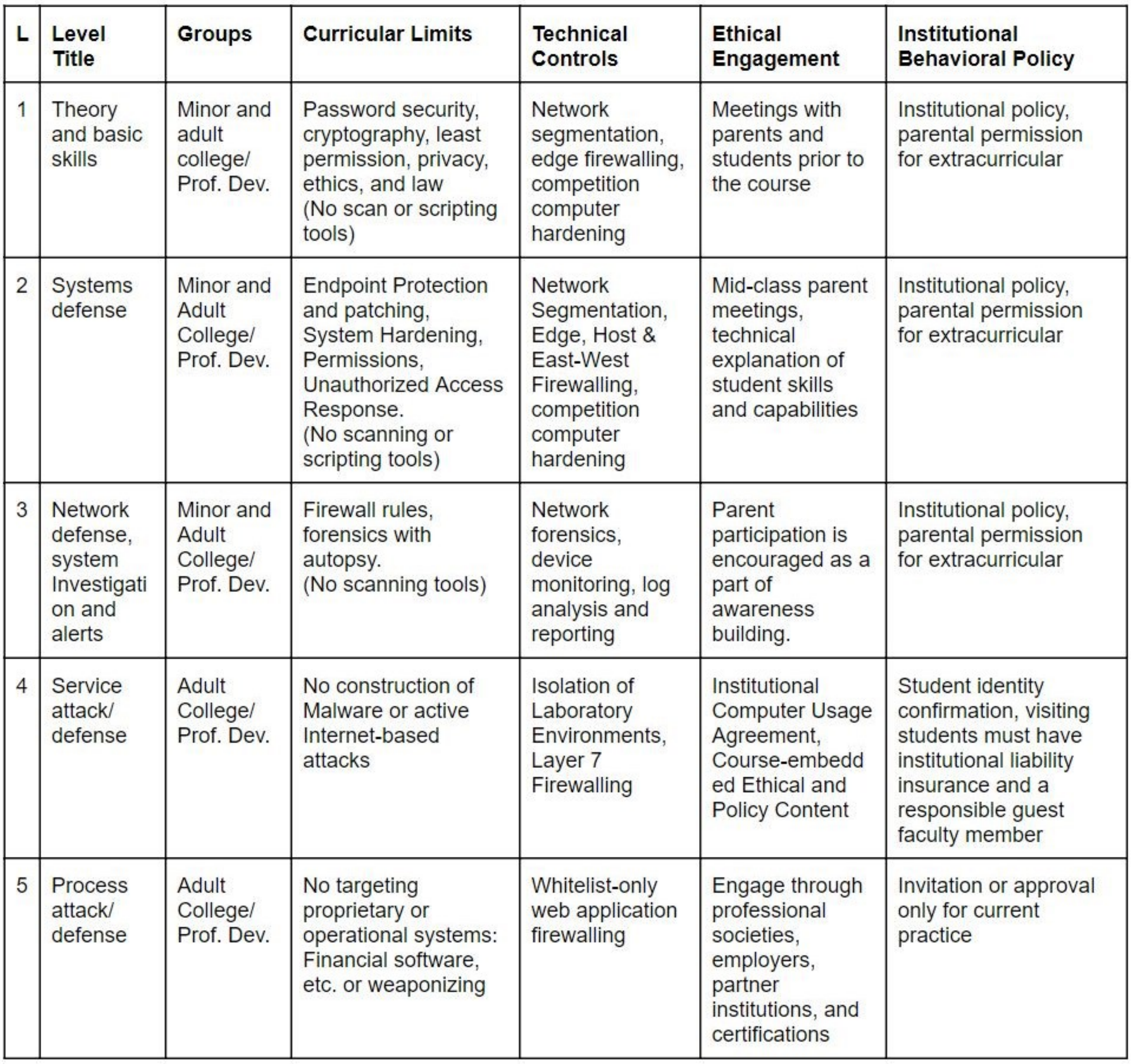
Figure 9: Range of Encouraged Student, Competitor, or Professional Behavior at Regis University

The Range of Behavior diagram in Figure 9 illustrates how multiple technical protections can mitigate risks. The thick arrows represent connections that may also introduce security controls between networks and to the open Internet. Separation of traffic, boundaries of authentication, and the various legal contexts in which student behavior occurs create a landscape of varying risk. Talking about ethics in classes and having firewalls in place are typical measures that education institutions use to reduce the risk of abuse and protect their own systems. But the risk of at least some portion of liability increases as the institution enables and encourages behaviors in the learning process like penetration testing, vulnerability scanning, reverse engineering, and malware design. The range of encouraged student behavior stretches well beyond policies that refer only to institutional systems and technologies that provide gateways at the borders of school networks. While these protective measures are very important, they do not cover the range of potential liability inherent in teaching invasive and proactive cybersecurity techniques.

In Table 2, the matrix of cybersecurity program deployment allows an institution to track the inherent risks in increasingly risk laden curricular content in a vertical column. Horizontally each level of instruction can track across technical controls, ethical engagement, and institutional policy controls. The underlying assumption is that these controls need to vary and adapt based on the types of capabilities that students acquire in the curriculum. Without this type of synchronized analysis, it would be hard to determine whether an institution's cybersecurity controls and ethical content delivery would be sufficient. Considering this inversely, an institution should consider limits on what it is teaching if it finds it is not able to sustain a broad range of proportionate risk mitigating measures across the behavioral ranges of the learner.

With policy, technical controls, and ethical training alone it is possible to mitigate some risk, particularly to institutional systems. But institutions still bear some responsibility and risk when a learner at home abuses cybersecurity techniques that were habituated and encouraged in a classroom. While this matrix begins to expose risks, the analysis alone will not cover institutional exposure in terms of responsibility to provide a learning experience that teaches behaviors that are risky off campus. But allowing academic leadership to thoughtfully deliver relevant levels of cybersecurity curriculum to learners based on their ability to bear risk and responsibility is one of the more significant benefits that the Matrix of Cybersecurity Deployment provides.

Table 2: Matrix of Cybersecurity Program Deployment with Risk Mitigation



L	Level Title	Groups	Curricular Limits	Technical Controls	Ethical Engagement	Institutional Behavioral Policy
1	Theory and basic skills	Minor and adult college/ Prof. Dev.	Password security, cryptography, least permission, privacy, ethics, and law (No scan or scripting tools)	Network segmentation, edge firewalling, competition computer hardening	Meetings with parents and students prior to the course	Institutional policy, parental permission for extracurricular
2	Systems defense	Minor and Adult College/ Prof. Dev.	Endpoint Protection and patching, System Hardening, Permissions, Unauthorized Access Response. (No scanning or scripting tools)	Network Segmentation, Edge, Host & East-West Firewalling, competition computer hardening	Mid-class parent meetings, technical explanation of student skills and capabilities	Institutional policy, parental permission for extracurricular
3	Network defense, system Investigati on and alerts	Minor and Adult College/ Prof. Dev.	Firewall rules, forensics with autopsy. (No scanning tools)	Network forensics, device monitoring, log analysis and reporting	Parent participation is encouraged as a part of awareness building.	Institutional policy, parental permission for extracurricular
4	Service attack/ defense	Adult College/ Prof. Dev.	No construction of Malware or active Internet-based attacks	Isolation of Laboratory Environments, Layer 7 Firewalling	Institutional Computer Usage Agreement, Course-embedd ed Ethical and Policy Content	Student identity confirmation, visiting students must have institutional liability insurance and a responsible guest faculty member
5	Process attack/ defense	Adult College/ Prof. Dev.	No targeting proprietary or operational systems: Financial software, etc. or weaponizing	Whitelist-only web application firewalling	Engage through professional societies, employers, partner institutions, and certifications	Invitation or approval only for current practice

6 Current Impact and Relevance

The works presented in the preceding chapters have made substantial contributions to a watershed of cyber defense training capacity building that can be assessed today in two ways. First, it is possible to review how much the specific contributions are being used. Second, a survey of related current trends of cyber defense can be used to determine what relevance these contributions have in the current context. The analysis will be divided into the four major sections below of the capacity building work with an emphasis on how these related to cyber defense in the specific areas of Service Development, Providing Digital Context, Tuning Performance, and Analyzing Impact.

Reflecting on the model as a whole, there are certain areas where efficacy is unsure. In terms of quantitative results, the work measuring the collaborative training community's technical performance did not achieve statistical validity. Nevertheless, surrounding qualitative analysis added value by described context, challenges, and methods of addressing that type of complex distributed training environment. Other models such as the psy-BIR-phys model, the Belief/Knowledge model, and the Incident Load model have so far only been used in the classroom as a conceptual approach for conveying critical aspects of cybersecurity issues. While anecdotal feedback there has been good, these models have not been rigorously tested as enhancing understanding in the cyber defense training context or demonstrated rigorously predictive capabilities. To make the work more valuable, these models could be tested in classroom environments for efficacy, and could also be tested for efficacy in the planning phases of cyber defense incident response, cyber infrastructure, and user population analysis.

6.1 Service Development

Since the research in these works was developed and put to use in the Regis labs, the Rocky Mountain Regional Collegiate Cyber Defense Competition has regularly chosen Regis University to be the host of the event. Regis continues to rely on new generations of these systems, originally designed using the pipeline service modeling and agile resource provisioning concepts. Because the service pipeline technique uses a model with a high degree of abstraction, it still has relevance for modern technical systems design in 2020.

The virtual world datacenter has been in operation every year as of 2019 in support of cybersecurity classes since it was introduced in 2012. Capital Technical University students are the primary users, joined in 2019 by students at the Higher College of Technology in the United Arab Emirates. The Association of College and Research Libraries Virtual World Interest Group also offered a tour of the facility in 2019 and related work in 2020. Beyond the original design, several other security scenarios have been designed including a Security Operations Center, Foreign Bureau Office, and Network Operations Center. Additionally, the introduction of VR (Virtual Reality) headsets into the market has re-invigorated development efforts in virtual environments. New development work in VR environments could transfer and use findings of the research presented here in the fulfillment of cyber defense training and actual operations requirements (Armstrong, 2016).

6.2 Providing Digital Context

The contributions in the prior works modeling bit-induced reality and digital identity management were published respectively in 2013 and 2016. While these particular methods have not seen significant application beyond the classroom, the relevance of these ideas has increased significantly given several trends in the use of technology. The Cambridge Analytics efforts using psychographics (also called psychometrics) exploited during the US presidential election (Risso, 2018) show that the effort used information with which individuals identify in order to influence their identity-based decisions. In the digital identity management modeling, identity reflects connections "with which individuals identifies" that have marked similarities to the type of "Like" data, group memberships, and meme forwarding behavior that was collected by Cambridge Analytics. Developing and applying models that manage digital identity in this manner is taking a place of increasing importance in defending the cyber identity of both individuals and groups, like voting precincts and nations. Regarding the vulnerability of elections and local sentiment in relation to government, the Psy-BIR-Phys matrix was used in 2013 to lay out the risks of moving from paper media to digital. The original text describes the possibilities as, "Unlike previous efforts in mass social engineering, it is possible to influence perceptions by controlling what an individual user sees while doing an apparently limitless search of the Internet," thus describing a significant function of the 2016 social engineering attacks on US elections. It is not as though the identity management modeling and Psy-BIR-Phys models presented in this body of work [P09] could have alone predicted or resolved these attacks. But the election is evidence that tools providing an initial context in developing defensive strategies against psycho-cyber attacks will be valuable in assisting cyber defense students as they enter careers.

6.3 Tuning Performance

Cyber defense is adapting as cyber attacks include significant intentional psychological components. They are now often intended to digitally manipulate a society (Gandhi *et al*, 2011), create a focused act of terrorism (Rogers, 2003), or target directly a company or defenders. In the cyber attack on the Estonian banking system (Hansel, 2018), understanding Russian public sentiment was key to using anti-Estonian feelings to convince Russians to trigger a script. In that context and closely related to the challenges being addressed in the work presented here [P07], a cyber attack can exploit a cultural weakness in a population of users or impact the cyber defense team (Halevi *et al*, 2016) (Finomore *et al*, 2013). In order to address this evident intentionality of exploiting psychological vulnerabilities as a component of cyber attacks, new designs in embedded user training are appearing (Finomore, 2013). The 2019 work on short-cycle psychometric feedback [P07] offers a method of facilitating mid-event psychometric coaching and baseline evaluations for cyber defense teams as a mitigating measure in psychologically disruptive events. This can be applied to the psychological resilience of teams engaged in training and incident response in ways that have yet to be broadly addressed in current cybersecurity literature.

Multi-agency and multi-institutional collaboration has also increased as is evident in the designs of the Colorado information Analysis Center (CIAC) facility, a center for aggregating cyber attack data so that broad attacks can be recognized and thwarted or minimized using aggregation technologies available in the US (Zandani, 2016). In addition to these more hierarchical approaches, the prior work presented here [P04, P02] contribute to the range of options that institutions at a variety of scale can leverage. While these types of joint response activities are just being implemented over the last few years, one of the authors of the 2019 paper was asked to present its content at JackVoltaic 2020, a US Army infrastructure readiness conference (Esquibel & Mitchell, 2019). Quantitatively measuring the capabilities of cyber defense training in multi-agency collaboratives over a span of years was an integral part of supporting this work.

6.4 Analyzing Impact

The most recent of the prior works are in the Analyzing Impact area, having publication dates of 2019 and 2020, thus post-publication trending and usage of the conceptual contribution has yet to be significantly observed. Contribution to the body of knowledge at the forefront of the discipline is evidenced in the uniqueness of the concepts. In the review of current literature, there are few works that address the topics of the institutional risks of teaching cybersecurity similar to what is presented in this body of work [P10]. Additionally, the paper on a joint National Guard based defensive response to a US state government coming under cyber attack [P05] describes the first defensive engagement of its kind in the US.

6.5 Building Cyber Defense Training Capacity as an Integrated Focus

Because cybersecurity and computer sciences are new disciplines in general, and capacity building for cyber defense training is a relatively new pursuit, when developing new concepts and methods to this work it is necessary to rely on sources from other disciplines that can bring in valuable context and tools.

While computer and information sciences fall naturally into this work in areas like virtualization, interdisciplinary work is where a great deal of the value has been revealed by this research. Regarding the social sciences, Creswell's mixed research designs (Creswell, 2017) provides a tool for working with smaller teams and highly diverse collaborations. The prospect theory and behavioral economics of Khanaman and Tversky as seen through McDermitt (McDermott, 2012) and Edward Bernays book, Propaganda, regarding the manipulability of the mind (Bernays, 1928), both lead to an understanding of how as a society we can address cyber disruption. Petress' work on active learning for pedagogical techniques (Petress, 2008) provides a method for enhancing the engagement of cybersecurity learning. Hatherington and Weiler's sociological work on authoritarianism and polarization regarding an individual's self-awareness of group posture (Hetherington, 2009) coupled with the brain-based studies of Kanai on political orientation (Kanai, 2011) elucidate both the risks and potential mitigating measures to cyber-social manipulation. Furthermore, the MBTI psychometric tools to facilitate interaction feedback (Myers *et al*, 2003) give us ways to respond to the psychotropic effects of cyber attacks at the scale of a team. While this cross-disciplinary work can be viewed as dabbling in a broad range of specialties, most work at the forefront of emerging disciplines are initially formed in a similar manner.

The integration of socio-psychological self-awareness and coaching enable this body of work to address some of the more problematic emerging challenges that cyber defenders will face in cyberspace (Aiken, 2016). Cyber defenders will need to go beyond technical skills and become more sensitive to and empowered within the socio-psychological world of cyberspace.

Perceiving when the environment and communications are being manipulated or set off balance is helpful as is expressed in the author’s prior work on managing identity. Using a cyber defense training program to build both technological skills and psychological resilience on the personal, team, and inter-institutional scale is an integrated goal of this work.

7. Conclusion

The prior works reviewed above represent a coherent effort of research producing progressive levels of capability all focused around cyber defense education, competition, and cyber defense training. It presents a progression of contributions to the body of knowledge at the forefront of cybersecurity capability development that has all been validated by peer reviews and the review of reputable editorial boards and continues to be available online through reputable listings such as Scopus.

7.1 Research Contributions

In summary, the main contributions of the research include:

- **Service Development and Training Models:** These include a novel pipeline analysis technique for analyzing virtualized systems, bandwidth, and processing within a distributed service system. Also included is a new virtualization layer model that presents social virtualization as an extension of the application layer, contributing to a focus on the experiential aspects of virtualization. A novel method of applying the agile SCRUM technique in support of technology events like cyber competitions is presented, offering methods for resource constrained groups to operate more efficiently. In concert, an innovative virtualized 3D datacenter model in a virtual world is presented that leverages an emerging infrastructure to offer immersive learning scenarios where spatial recognition and experience-based skill requirements are high.
- **New Frameworks for Digital Context:** Building on the digital environment of the services described above, unique contributions were made in providing more relevant perceptions of digital context, so that learners can perceive how their environments change when they become digitally dependent, and understand better their own identities as they too become digitally dependent. The Psy-BIR-Phys model provides a novel concept of mapping out the implications of "Bit Induction," which is the rising level of dependence on digital systems for functionality. This can manifest as the introduction of automation, virtualization, computer design and manufacturing, and visualization. Next a novel application of a layered Knowledge/Belief theory provides a novel way of understanding how individuals and societies react to the disruptive aspects of digital identity and how those might be addressed.
- **New Evaluative Instruments, Models, Methods, and Data:** Once the new context has been addressed for the learners, new evaluative instruments are introduced for tuning performance within the digital learning space. Spanning a multi-agency training collaborative, a unique application of the multi-method approach, mixing qualitative and quantitative research, is constructed to show individual progress within a larger emerging context of cybersecurity training. Then a new joint collaborative training model is introduced and used to evaluate an evolving multi-agency collaboration. Based on the evolving needs and resources within this collaborative, a novel analytical model is developed to aggregate participant behavior, psychometrics, and digital logs. The model enables a new conceptual approach for both mid-event intervention and post-event analysis of cyber defense activities.
- **Cyber Defense Training Program Performance Tuning Methods:** With some initial performance tuning systems in place, the focus of this research moves to the impact of the overall cybersecurity training program, addressing the outcomes of the learners

as they engage in international cyber defense incidents for governmental agencies and then evaluating the risks that are imposed on the institution and learner operating in this cybersecurity learning environment. The incident response performance of a set of trainees operating within a larger group are evaluated based on the load they are able to sustain as they engage in a new type of situation within the United States, a National Guard Unit responding to a US State experiencing a devastating attack on a major department. Next, a novel topological model is introduced to track the range of behavior of learners to consider the risks associated with the learning process. Then an innovative matrix is presented that allows for risk across that behavior range to be linked to mitigating actions.

In aggregate, these contributions represent a holistic advancement in cyber defense training. They were made with strong awareness of and participation in the academic communities engaged in cybersecurity and cyber defense training and were made at the forefront of the body of knowledge. The interdependent nature of each category of contribution reflects a need to integrate various focused disciplinary advances into a more focused discipline of cyber defense training. The result is a set of resources and data designed to allow significant advances in the capacity of cyber defense training.

7.2 Limitations

Reviewing the prior works presented here in light of the goal to build cyber defense capacity, several gaps appear in the research where further work is needed:

- Develop resilience and adaptability characteristics for the collaborative training programs, so that training programs persist with efficacy through participants' institutional change. Further, develop larger scale structures for joint operations so that disruptive cyber attacks can be handled collaboratively and rapidly. Resolve this by establishing better conceptual frameworks for measuring multi-institutional training value that achieves better determination of the most effective and least effective training components.
- Create characterizing frameworks and testing instruments to describe the psychotropic nature of cyber attacks, from DDoS attacks on institutions to disinformation and destabilization attacks on societies. Then work to develop technical and practice methods for responding to the negative psychotropic effects of cyber attacks based on recent clinical innovations in the use of cyber technologies for psychological conditions.
- Establish frameworks for rapidly including multi-disciplinary research that supports stable roadmapping for human society as it becomes increasingly dependent on cyber infrastructure.

These limitations in the research were each caused by different challenges. Collaborative relationship resilience in the emerging field of cyber defense has many skeptics because of the challenges of jurisdiction, the need to control confidentiality of data, and the preferences of changing leaders. This has proved to be challenging ongoing work, and is a significant part of engaging institutions as the research moves to new phases. The work supporting cyber defense teams with proactive psychological support has limitations on the speed that this can happen because the proactive psychological coaching of teams engaged in digital behavior is still in an emerging space. A somewhat distant example but a landmark moment is reflected in the first US Food and Drug Administration approved clinical use of a software prescription for a psychological condition (US Food and Drug Administration, 2020). As new knowledge in this field emerges, the author hopes to leverage it in cyber defense training and incident response environments. Multi-disciplinary work also faces cultural challenges in academia, where fields like philosophy, psychology, and journalism have operated at some distance from cyber defense operations. While interdisciplinary partnerships are currently maintained by the author by developing personal relationships across disciplines, professions, and institutions, efforts to create institutional structures that can encourage this type of cross-disciplinary work may be more sustainable.

7.3 Future Work

To be pragmatic, work planned over the next year addresses a very small subset of the above limitations of the work here in relation to the work that need to be addressed.

Planned research in the near-term includes:

- Advancing the psychometric work with an interdisciplinary team focused on the goal of making this type of work more accessible to other institutions. The intent is to develop methods to make the short-cycle psychometric feedback more automated and pre-planned. This will be designed to support collaborative studies.
- Developing pre-packaged resources to help make cyber challenge events more doable for smaller institutions is planned with the intent to regularize this type of training activity in cyber security and IT departments. It will be designed so that participants can choose to share their data, so that anonymized aggregated data can be analyzed in an effort to understand these types of activities more broadly.
- Testing the Psy-BIR-Phys, Incident Load, and Knowledge/Belief models for efficacy in the classroom and in cyber defense operations in order to validate, adapt, and tune the operational and analytical applications of these models.
- Design models that can lead to digital training environments with high levels of efficacy through engaging scenario development, increased digital environment seamlessness, psychometric guidance, and rapid “updatability” to achieve high levels of relevance in relation to the contemporary challenges of cyber defense.

The advances of technology and societal dependencies is likely to accelerate further. Specifically, the advances in virtualized and geographically distributed engagement are likely to advance and become more important as the COVID-19 pandemic has made clear with many institutions moving to remote learning and work. The research presented here will need to be advanced at each layer, but the move to where innovation is occurring in cyber defense training seems to be towards the higher layers because the underlying infrastructure is beginning to be operationalized into normal business practices and the underlying technologies are being commoditized in competitive markets.

As we see international election interference and sentiment manipulation, with meme-driven social influencing using AI and psychographic techniques emerge, protecting the intellectual process integrity of institutions, nations, and societies comes to the forefront of training needs as well as for active cyber defense. Cyber defenders will need greater ability to engage large systems that have psychotropic influence. And they will need to function at global scales of operations while engaging at very high degrees of granularity.

As the Internet of Things extends, compounding the reach of earlier SCADA and control systems that automated our buildings, our industries, and our traffic signals, the urgency of defending these systems will continue to increase proportionately. Developing the ability to be agile, aware of the implications of events, and able to operate agilely in both physical and cyberspace will likely emerge as a psychological requirement. Cyber defense training will need to provide these resources by developing frameworks, curriculum, and relationships that can span the breadth of civil engineering, social psychology, and analysis of the motivations of international politics.

Visions like these are what motivate the author to advance this work with all due speed. With a cyber-stable society, we can perhaps find our way to the stars. As H. G. Wells said in 1920 in his book, *The Outline of History*, “Human history becomes more and more a race between education and catastrophe... Yet, clumsily or smoothly, the world, it seems, progresses and will progress.”

References

Adebiaye *et al*, 2016 Adebiaye, R., Alryalat, H., & Owusu, T. (2016). Perspectives for cyber-deterrence: A quantitative analysis of cyber threats and attacks on consumers. International Journal of Innovative Research in Science, Engineering and Technology, 5(7).

Aiken, M. 2016 The cyber effect: A pioneering cyber-psychologist explains how human behavior changes online. Spiegel & Grau.

Beck et al 2001 Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R., Mellor, S., Schwaber, K., Sutherland, J., Thomas, D,. Manifesto for Agile Software Development, https://agilemanifesto.org/, retrieved: July 4, 2020.

Berners-Lee, et al, 1992 Berners- Lee, T., Cailliau, R., Groff, J. F., & Pollermann, B. (1992). World- Wide Web: the information universe. Internet Research.

Border, C. (2007). The development and deployment of a multi-user, remote access virtualization system for networking, security, and system administration classes. ACM SIGCSE Bulletin, 39(1), 576-580.

Boulos et al, 2007 Boulos, M. N. K., Hetherington, L., & Wheeler, S. (2007). Second Life: an overview of the potential of 3- D virtual worlds in medical and health education. Health Information & Libraries Journal, 24(4), 233-245.

Carlin et al, 2010 Carlin, A., Manson, D., Zhu, J. (2010). Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). Information Systems Education Journal, Vol. 8 No. 14. ISSN: 1545-679X, http://isedj.org/8/14/ISEDJ.8(14).Carlin.pdf, retrieved: July 4, 2020.

Choi *et al*, 2010 Choi, Y. B., Lim, S., & Oh, T. H. (2010, October). Feasibility of virtual security laboratory for three-tiered distance education. In Proceedings of the 2010 ACM conference on Information technology education (pp. 53-58).

Cooper *et al,* 2009 Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E., Hoffman, L., Perez, L., Pfleeger, C., Raines, R., Schou, C., Brynielsson, J.: An exploration of the current state of information assurance education. In:Impagliazzo, J. (ed.) Inroads - SIGCSE Bulletin, vol. 41, no. (4), pp. 109–125

Creswell, J. W., & Clark, V. L. P. 2017. Designing and conducting mixed methods research. Sage publications. https://books.google.com/books?id=BXEzDwAAQBAJ, retrieved: July 4, 2020.

Creswell, J. W., & Creswell, J. D. 2017 Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Esquibel & Mitchell, 2019 Esquibel, Judy and Mitchell, Erica, "Jack Voltaic 2.0: Threats to Critical Infrastructure," US Army Cyber Institute, Technical Reports. 36. https://digitalcommons.usmalibrary.org/aci_rp/36, retrieved: July 4, 2020.

Finomore *et al*, 2013 Finomore, V., Sitz, A., Blair, E., Rahill, K., Champion, M., Funke, G., Mancuso, V., & Knott, B. (September). Effects of cyber disruption in a distributed team decision making task. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 57, No. 1, pp. 394-398). Sage CA: Los Angeles, CA: SAGE Publications.

Gall et al, 2006, Gall, M.D., Gall, J.P., Borg, W.R., Educational research: An introduction, 8th Ed. Pearson.

Gandhi et al, 2011 Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P., Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1), 28-38.

Graham, P., 2016, Superdata Releases new VR Market Forecasts, Mar 10, 2016, VRFocus, https://www.vrfocus.com/2016/03/superdata-releases-new-vr-market-forecasts/, retrieved: July 4, 2020.

Hackathorn, E. J., & Explorer, S. L. 2006 Designing an educational island inside second life for the National Oceanic and Atmospheric Administration (NOAA) Earth System Research Laboratory (ESRL). In Second Life Education Workshop at the Second Life Community Convention San Francisco August 20th, 2006, p. 12.

Halevi *et al*, 2016 Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., & Chen, J. (November) Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services, pp. 318-324.

Hansel, M. 2018 Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks. Journal of International Relations and Development, 21(3), 523-551.

Herzog, S. 2011 Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49-60.

Hoffman *et al* 2005 Hoffman, L., Rosenberg, T., Dodge, R., Ragsdale, D.: Exploring a national cybersecurity exercise for universities. In: Donner, M. (ed.) Security and Privacy, IEEE, 3(5), p27–33

Irvine *et al*, 2005 Irvine, C. E., Thompson, M. F., & Allen, K., CyberCIEGE: gaming for information assurance. IEEE Security & Privacy, 3(3), 61-64.

Kurzweil, R., 2005, The singularity is near: When humans transcend biology, Penguin

Leiner *et al*, 1997, Leiner, B., Cerf, V., Clark, D., Kahn R., Kleinrock L., Lynch, D., Poste, J., Roberts, L, Wolff S., 1997, Brief History of the Internet, https://www.internetsociety.org/internet/history-internet/brief-history-internet/, retrieved: July 4, 2020.

Li, P., 2010 Selecting and using virtualization solutions: our experiences with VMware and VirtualBox. Journal of Computing Sciences in Colleges, 25(3), 11-17.

Marcum et al, 2014 Marcum, C., Higgins, G., Ricketts, M., & Wolfe, S., Hacking in High School: Cybercrime Perpetration by Juveniles, Deviant Behavior, 35:7, 581-591, DOI: 10.1080/01639625.2013.867721

Marquardson, J., Gomillion, D. 2018 Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience. Information Systems Education Journal, 16(5) pp 12-21. http://isedj.org/2018-16/ ISSN: 1545-679X. (A preliminary version appears in The Proceedings of EDSIGCON 2017)

Meyers et al, 2003 Myers, I., McCaulley, M., Quenk, N., Hammer, A.: MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator, 3rd edn. Consulting Psychologists Press, Palo Alto

Moore, E., 2007 VPL 1.0 Visual Philosophy Language From Metaphysics to Metadata, Seeing Through Press, Denver

Parker, G., 1990 Team Player and Team Work: The New Competitive Business Strategy. Jossey-Bass Inc, San Francisco

Paulk *et al*, 1993 Paulk, M., Curtis, B., Chrissis, M., and Weber, C., "Capability maturity model, version 1.1," in IEEE Software, vol. 10, no. 4, pp. 18-27, July 1993, doi: 10.1109/52.219617.

Potter, N. 2010 Comparing Scrum and CMMI, how they can work together. The Process Group.

Pridmore *et al*, 2010 Pridmore, P. Lardieri and R. Hollister, "National Cyber Range (NCR) automated test tools: Implications and application to network-centric support tools," 2010 IEEE AUTOTESTCON, Orlando, FL, 2010, pp. 1-4, doi: 10.1109/AUTEST.2010.5613581.

Risso, L. 2018 Harvesting your soul? Cambridge analytica and brexit. In Brexit means Brexit: Selected proceedings of the symposium (pp. 75-90). Academy of Science and Literature, July. http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, retrieved: July 4, 2020.

Rogers, M., 2003, The psychology of cyber-terrorism. Terrorists, Victims and Society: Psychological. Perspectives on Terrorism and Its Consequences, 75-92.

Ryoo *et al*, 2011 Ryoo, J., Techatassanasoontorn, A., Lee, D., & Lothian, J. (June). Game-based infoSec education using OpenSim. In Proceedings of the 15th Colloquium for Information systems security Education (pp. 101-106). Fairborn, OH: CreateSpace Independent Publishing Platform.

Schwaber, K., & Sutherland, J. 2013 The scrum guide-the definitive guide to scrum: The rules of the game. SCRUM. org, July.

Shnider, D, 2011 What makes cybercrime laws so difficult to enforce, IT Security, in CXO on January 26, https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/, retrieved: July 4, 2020.

Smith, N.C. 1990 The case study: a useful research method for information management. J. Inf. Technol. 5(3), 123–133 (1990), ISSN: 02683962. (Routledge, Ltd.)

Smith, S, 2008 July, Journal of virtual Worlds Research Vol. 1. No. 1, SSN: 1941-8477, “Virtual Worlds Research: Past, Present & Future”, Second Life Mixed Reality Broadcasts: A Timeline of Practical Experiments at the NASA CoLab Island, NASA JSC Learning Technologies

Stackpole *et al*, 2008 Stackpole, B., Koppe, J., Haskell, T., Guay, L., & Pan, Y. (2008, October). Decentralized virtualization in systems administration education. In Proceedings of the 9th ACM SIGITE conference on Information technology education (pp. 249-254) Journal of Computing Sciences in Colleges, 25(3), p11-17.

Sullivan *et al*, 2018 Sullivan, D., Colbert, E., & Cowley, J. (2018, August). Mission Resilience for Future Army Tactical Networks. In Resilience Week (RWS) (pp. 11-14). IEEE.

Thorne, S., 1994 Chapter 14 Secondary Analysis in Qualitative Research: Issues and Implications, found in Morse, J. M. (Ed.). Critical issues in qualitative research methods. Sage.

United States of America, Congress S.272 - High-Performance Computing Act of 1991, Senate Committees on Commerce, Science, and Transportation, S. Rept. 102-57, Law 102-194, https://www.congress.gov/bill/102nd-congress/senate-bill/272, retrieved: July 4, 2020.

US Food and Drug Administration, 2020 United States of America, Food and Drug Administration, Press Announcement: FDA Permits Marketing of First Game-Based Digital Therapeutic to Improve Attention Function in Children with ADHD, June 15th, https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-first-game-based-digital-therapeutic-improve-attention-function-children-adhd, retrieved: July 4, 2020

Wiederhold, B., 2020 (ed.), Cyberpsychology, Behavior, and Social Networking, online ISSN: 2152-2723, https://home.liebertpub.com/publications/cyberpsychology-behavior-and-social-networking/10/overview#aims, retrieved: July 4, 2020.

Zandani, S., 2016 U.S. Patent No. 9,426,169. Washington, DC: U.S. Patent and Trademark Office.

Appendix A - Published Works

Listed below are the ten peer-reviewed published prior works.

[P01]

Developing Cyber Competition Infrastructure Using the SCRUM Framework

Bibliographic Information - Heath Novak, Daniel Likarish, Erik Moore, pp. 20-30, in Ronald Dodge Jr., Lynn Futcher, (eds) Information Assurance and Security Education and Training, , Proceedings of the 8th International Federation of Information Processing working Group 11.8, World Conference on Information Security Education, proceedings of the conference, "WISE 8", Auckland, New Zealand, July 8, 2013 http://dl.ifip.org/db/conf/ifip11-8/ifip11-8-2013/NovakLM13.pdf, https://doi.org/10.1007/978-3-642-39377-8_3

Abstract - In March 2012, the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) was hosted at Regis University and attended by seven colleges from the region. CCDC was developed by the University of Texas in San Antonio to provide a structured environment for practical education tied to established information assurance learning objectives in the implementation of security techniques, strategies and processes. The Regis University infrastructure team designed the competition scenario to emulate an e-commerce web business. The pervasiveness of web application attacks resonated with the event developers at Regis University because of recent reported attacks against Valve™, Inc. and their Steam™ video game retail and social net- working service. This paper will outline at a high level the event architecture and technical infrastructure details, a discussion on Agile development methodologies (specifically SCRUM) and how they can be applied to competition infrastructure development.

Contributing Research Location and Time - This development work to leverage SCRUM methodology started in the fall of 2011. The author had been responsible for several preceding years for coordinating the technical designs of cyber training and competition events at Regis University's Denver Technology Campus. He had taken a position at another institution but came back to assist with the competition in March 2012. In 2013 where he provided contextual narrative regarding the cyber competition infrastructure, the CANVAS cyber competition, and the systems development life cycle (SDLC) methods previously used.

E. Moore's Contribution The operational work on this paper was developed in the research lab that the author ran day to day, designing infrastructure and assigning project work. The lead author is an expert in the SCRUM framework and all researchers including the author collaborated on developing an application method for that framework so that it could be applied to the specific needs of the institution's training and competition hosting objectives. The author wrote use case components in support of the work, but was not responsible for the overall structure or final edit of the paper.

[P02]

A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure

Bibliographic Information - Moore E., Likarish D. (2015). In: Bishop M., Miloslavskaya N., Theocharidou M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham, https://doi.org/10.1007/978-3-319-18500-2_4

Abstract - This study provides a summary and analysis of a cyber security multi agency collaboration for rapid response by Regis University (RU), in partnership with the Colorado Army and Air Force National Guard (CONG) and the State of Colorado (SOC), deploying AGILE methods to improve the ability of the CONG and SOC to respond to attacks against Colorado's critical infrastructure. The summary covers formative discussions and about a year-long series of physical exercises (hands-on digital challenges and in-person role playing), lectures and certification exams that advanced the study participants domain knowledge, awareness of SOC policy and communication with industry. Other states and territories can use the model to the benefit of their citizens. Events included multiple simulations, physical exercise scenarios, and tabletop exercises designed to give real-world substance to more abstract cyber security concepts and integrate physical world consequences to actions performed by the participants.

Contributing Research Location and Time - The author engaged in this research working collaboratively in a series of meetings from the fall of 2014 to January 2015 to formulate a case study and write this paper in Denver, Colorado with the co-author. Specifically related to this case, in 2013 the author contributed infrastructure resource design and training planning that were used in the events described.

E. Moore's Contribution - For 5 years prior to this paper, the author developed methods to scale a very small set of resources in a college computer science research laboratory to support recurring regional cyber training exercises. This is based in part on formative work in the paper Multi-Method Virtualization: An Architectural Strategy for Service Tuning where the author was the first author. The model presented in this work describes a new architecture of which the author was one of two designers in an equal collaboration. The research uses feedback from actual operations over 3 years as we adapted the methods.

[P03]

The Use of Second Life® to Teach Physical Security across Different Teaching Modes

Bibliographic Information - Nestler V., Moore E.L., Huang KY.C., Bose D. (2013). In: Dodge R.C., Futcher L. (eds) Information Assurance and Security Education and Training. WISE 2013. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-39377-8_21

Abstract - Teaching physical security can be difficult since classes generally do not have access to physical structures to assess. The purpose of this study was to investigate a new way of teaching physical security using Second Life® and to see if there is a difference in performance related to mode of instruction. The research question sought to determine whether there was a significant difference in student performance based on differences in modes of instruction for students evaluating physical security in virtual world environments. Three groups of participants situated in three geographic locations in the United States and belonging to three different modes of instruction – traditional, online, and hybrid were taught using Second Life®. The results were inconclusive in determining the best mode of instruction. However, the research suggested that Second Life® can be used as a teaching platform to teach physical security.

Contributing Research Location and Time - The author had engaged in virtual world scenario production at Regis University for several years prior to 2010 related to command center design with Regis University. The physical security auditing scenario work in the virtual space was presented by Vincent Nestler of Idaho State University's National Information Assurance Training and Education Center. Working with Nestler, Huang, and Bose from Idaho, the author met in the virtual world space of SecondLife® where, taking in their requirements in real time, the author formulated the design of the Virtual Datacenter over several sessions starting in the fall of 2010. It included their requirements for physical security flaws that could be discovered by students addressing the discipline of physical security auditing. As of publication, the scenario had been hosted within SecondLife® at the University of Denver's Science Island III, and the MASIE™ Center virtual space. Once the author designed the virtual world build, he worked with the others to architect an experiment using student participants at Idaho State University, Capitol College in Maryland, and Regis University in Colorado. Students participated online, in a hybrid online/classroom format, and as classroom-based students. The author managed the experiment in the virtual space in SecondLife® and the students at the Regis site who were classroom-based. Following publication it has been hosted at DeVry University and is now at the Adams 12 Five Star School site within SecondLife® where it is available for tours.

E. Moore's Contribution - Working as the second author on the project, the author contributed significant text characterizing the field trials of the virtual data center in addition to running trials. The author was also the primary designer of that virtual teaching space which has been used regularly by multiple academic institutions since it was made available. The idea came about as the the author and Vincent Nestler were discussing how at the time of the World Trade Center attacks on 9/11, data center access had become restricted and professors teaching cyber-physical security were no longer able to give tours of real datacenters to students on this topic. Other authors performed the statistical analysis and made contributions in the writer discussions and about the field trials on their site.

[P04]

Evaluating a Multi-Agency Cyber Security Training Program Using Pre-post Event Assessment and Longitudinal Analysis

Bibliographic Information - Moore E., Fulton S., Likarish D. (2017). Pp 147-156 in: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, vol 503. Springer, Cham https://doi.org/10.1007/978-3-319-58553-6_13

Abstract - This study presents the context and measured results of cyber security joint cyber defense training exercises. Building on previously published work by these researchers that introduced AGILE methodologies, this study analyzes the outcomes of that professional development and laboratory-supported environment. Analysis focuses on the development of specific individual skill levels and generally describes desired multi-agency collaborative capabilities. While all training events do not have sufficient pre-post data to isolate the particular causes of a rise in capabilities, competence in progressively harder levels of capabilities is observed over time in relation to the training components. A comprehensive Personalized Education Learning Environment (PELE) aggregate data of individuals is not presented here, indicators suggest that this would enhance outcomes.

Contributing Research Location and Time - Data was gathered from 2013 to 2015 on a cyber defense team in training at the Regis Denver Tech Center campus in Colorado. The analysis and preparatory work for the paper occurred at the same location or through distributed communications from fall 2016 to submission in January of 2017. Prior to the study, the author contributed to the design of the cyber training infrastructure where the training took place and to the training curriculum evident in the measured skills of the research. Co-author Likarish and the author constructed the Xmodels. The author provided categories of skill that contributed to the design of the survey questions and worked closely with Likarish in a series of meetings from the Fall of 2016 to January 2017. Then the author interpreted and applied a series of models to the data in order to maximize the generalizable value.

E. Moore's Contribution - The author contributed training content and objective design as a member of the design team for the training program described in this paper as well as contributing design components of the training space. Using data collected by the fellow researchers, the author jointly developed appropriate representations of the data and uncovered implications of data along with potential action items. The author collaboratively designed methods to improve both training and evaluative processes for this program and in ways that are generalizable. The author was the primary writer of the narrative.

[P05]

Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation

Bibliographic Information - Moore E.L., Fulton S.P. , Mancuso R.A., Amador T.K., and Likarish D.M., In: Eds. Onwubiko C., Belleens X., Erola A., Jaatun M.G., & Nogueira C., Cyber Science 2019, Cyber Situational Awareness for Predictive Insight and Deep learning, Multi Disciplinary Proceedings of the International Conference on Cybersecurity and Protection of Digital Services (Cyber Security 2019) at Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, Published by Center for Multidisciplinary Research Innovation and Collaboration (C-MRiC.org), pp 162-169, 2019 ISBN 978-0-9932338-4-5, https://doi.org/10.1109/CyberSA.2019.8899736

Abstract - In the United States, the State of Colorado's Department of Transportation successfully defended and recovered from a recent severe malware attack. The 2018 attack at the Colorado Department of Transportation was mitigated by a rapid multi-agency incident response. This is the first case in the United States where a state's National Guard responded to a governor's declaration of a cyber emergency response. In anticipation of advanced threats to Colorado citizens, Regis University has hosted collaborative exercises with government, organizations, and industry as part of a larger Collaborative Training Response Community (CTRC) effort to facilitate collaborative physical exercises, governmental policy development, and relationship building. The resulting capabilities allowed for an effective response to this incident. The authors present a new incident response model, based on this case in the context of existing cybersecurity organizations extant in the U.S., that may be useful to private and public sector communities where collaborative incident response is appropriate.

Contributing Research Location and Time - The author contributed ideas in several key discussions leading to the development of this paper with the Regis Faculty, all in and around Denver, Colorado starting on the day of the defensive engagement of the cyber defense team that the researchers had been training. The researchers developed the paper based on a relationship spanning more than a decade prior. The defensive engagement occurred in February, 2018. The author submitted the paper for peer review on January 22, 2019.

E. Moore's Contribution - The author invited this group of researchers to collaborate around several patterns of behavior that had surfaced during a cyber defense incident. The author was not at the Incident as were the others. But based on their notes and interviews with other participants, the author developed the model of load analysis used as the key component to describe new response strategies. The author jointly developed the response process models with one other researchers. While much structural and narrative work was done in real time in group sessions, the author was responsible for final paper edits and submission, working over about 4 hours a week on the project for a span of about four months, with an additional 20 hours the last week.

[P06]

Managing the loss of control over cyber identity

Bibliographic Information - Moore, E.L., 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), Moscow Conference Date: 6-8 July 2016, Added to IEEE Xprlorer: 04 August 2016, https:/doi.org/10.1109/DIPDMWC.2016.7529395

Abstract - Professionals entering the information security field need new models to manage user reactions to the loss of control over their digital identities. Escalations in authentication technologies like behavioral blocks and biometric data breaches are reducing the user's control over the management of their digital identities. Simultaneously, users are becoming more digitally dependent regarding financial transactions, buying food, emotionally connecting with loved ones on social media, managing personal information, and writing personal documents. This research presents a tool to address this issue pulled from the fields of education, political science, psychology, and cyber security. It is combined as a set of models to be delivered as part of information security curricula. Recent analysis of brain scans and population behavior studies have suggested that when people feel their identity at risk and feel disempowered they will have a stronger disposition towards authoritarianism, desire for retribution, and a desire for simplistic solutions instead of acting with reasoned and adaptive responses. Indicators in other fields suggest that the way professionals and educators characterize incidents that threaten digital identity can habituate different types of societal attitudes about the Internet and institutional data usage. The model presented herein should help cyber security educators characterize how users respond to digital identity threats, and provides a scale for evaluating those responses.

Contributing Research Location and Time - The bulk of the paper was researched and written in the spring of 2016 in Denver, Colorado, including the review of converging research related behaviors triggered by identity threats, increasing dependencies of identity on cyber resources, the desynchronization of identity from user control, and extant strategies for managing cyber identity. The author originally developed the model for forming identity automation and behavior queues as part of the philosophy book "*VPL 1.0 Visual Philosophy Language, From Metaphysics to Metadata*" written in Denver, Colorado between 2004 and 2007. The embedded models used in this context was developed by the author and included in a draft in 2005 of that book.

E. Moore's Contribution - Sole Author

[P07]

A Short-Cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense

Bibliographic Information - Moore E.L., Fulton S.P., Mancuso R.A., Amador T.K., Likarish D.M. (2019). In: Drevin L., Theocharidou M. (eds) Information Security Education. Education in Proactive Information Security. WISE 2019. IFIP Advances in Information and Communication Technology, vol 557. Springer, Cham, https://doi.org/10.1007/978-3-030-23451-5_4

Abstract - Following earlier research in demonstrating the significance of behavioral analysis in cyber defense, the authors developed a framework to incorporating multi-disciplinary datasets along a common timeline to increase incident response feedback for coaching. Currently this framework is being introduced in the state of Colorado, USA as a part of a joint government, industry and academic partnership. Upon project initiation, the feedback cycle had been a minimum of several months from observation to feedback. Presented here is a new framework that can shorten the cycle of psychometric feedback to multiple times in one training day. This Short-Cycle Framework, gathering psychometric and cyber data to provide direct feedback to cyber defense team leaders, was conceived when Regis University's psychometric evaluators observed a real multi-agency cyber defense response. The authors realized the psychometric data can be used in live cyber defense incidents alongside things like network firewall traffic analysis as the cyber defenders provide relief for organizations under active cyber attack. This work presents the context in which the framework was developed, the characteristics of the framework, and suggestions for further research. The framework implements a specific set of short- term state indicators based on well-known personality trait and state models. The coaching cycle was scripted to shorten the delay between observation and feedback so that it can be more useful in both training and live incident response.

Contributing Research Location and Time - The author performed all the research in or around Denver Colorado, primary at the Denver Technical Center campus of Regis University, just south of Denver, Colorado. One of the researchers, Likarish, invited the two psychometric analysts, Amador and Mancuso, to collaborate. The psychometric analysts began observing in May of 2016 and gathered data for this work from May of 2017 to February 2018. The author, in a series of meetings with Likarish, evaluated the potential generalizable value of the work in Fall of 2018. The author then led the broader collaboration structuring the work into the paper submitted in March of 2019.

E. Moore's Contribution - While the author was not present at the live fire cyber incident analyzed in this work, he was the primary author of this paper and a trainer for the defense team involved in the event. Psychometric analysis had been gathered independently on a traditional months-long cycle by the analysts on the research team during a training event. The research was in the context of a training series of which the author was one of the training designers. The author pulled the research team together around the transformational possibilities of a short-cycle goal and led model development that he envisioned, as well as leading the researchers in the design and editing of the paper. Beyond the authors named on this paper, several others made significant contributions to this work as indicated in the acknowledgements.

[P08]

Multi-Method Virtualization: An Architectural Strategy for Service Tuning

Bibliographic Information - Erik Moore, Daniel Likarish, in: IEEE Xplore: Proceedings of 2010 43rd Hawaii International Conference on System Science, 5 January 2010 https://doi.org/10.1109/HICSS.2010.281

Abstract - A wide variety of virtualization methods have recently come into common use. Using these methods as a suite of tools to tune service offerings has become a viable strategy for enhancing an Academic Research Network (ARNe) as it services a globally dispersed user population. This report will present a model for organizing and applying these virtualization methods to maximize service efficiency.

Contributing Research Location and Time - The technical and operations work described in this paper was performed in two locations. The primary location was the Regis laboratories in the Denver Technology Center just south of Denver, Colorado, where the author was the technical lead and responsible for day-to-day operations. The second location was the Storage Network Industry Association (SNIA) test bed, where the storage industry companies met to perform compatibility, standards, and integration work across platforms. This testbed was housed at the Hewlett Packard Rockrimmon Data Center facility in Colorado Springs, Colorado. The author managed a portfolio of storage technologies there and projected virtualized storage resources from there to the Denver location. The author developed the operations and virtualization modeling techniques over a span of several years from approximately 2001-2009, with model development, case study design, and writing occurring in 2009.

E. Moore's Contribution - While working in the Academic Research Lab at Regis University under the direction of the program coordinator for Master of Science in Information Assurance (MSIA) faculty, the author was responsible for deploying laboratory virtualization services including storage virtualization, network virtualization, system virtualization, and a physical scenario virtualization that included the Regis virtual world campus and virtualized command center. The need for capacity and performance was growing as the author prepared for cyber competitions and training exercises, developing new design methods. The institutional leadership provided requirements and use cases while the author developed the models and analysis for solving the problems that are presented in the paper. The author was the primary writer of the research paper**.**

[P09]

A Vulnerability Model for Bit-induced Reality

Bibliographic Information - Erik Moore, ICIW 2013, The Proceedings of the 8th International Conference on Information Warfare and Security, Editor: Douglas Hart, Venue: Regis University, Denver, Colorado, USA
https://issuu.com/acpil/docs/9781909507081_iciw_2013/183

Abstract - Professionals entering the information security field need new models to manage user reactions to the loss of control over their digital identities. Escalations in authentication technologies like behavioral blocks and biometric data breaches are reducing the user's control over the management of their digital identities. Simultaneously, users are becoming more digitally dependent regarding financial transactions, buying food, emotionally connecting with loved ones on social media, managing personal information, and writing personal documents. This research presents a tool to address this issue pulled from the fields of education, political science, psychology, and cyber security. It is combined as a set of models to be delivered as part of information security curricula. Recent analysis of brain scans and population behavior studies have suggested that when people feel their identity at risk and feel disempowered they will have a stronger disposition towards authoritarianism, desire for retribution, and a desire for simplistic solutions instead of acting with reasoned and adaptive responses. Indicators in other fields suggest that the way professionals and educators characterize incidents that threaten digital identity can habituate different types of societal attitudes about the Internet and institutional data usage. The model presented herein should help cyber security educators characterize user responds to digital identity threats, and provides a scale for evaluating those responses.

Contributing Research Location and Time - This research and analytical modeling was performed in Denver, Colorado. When this paper was written, the author had recently been hired at Adams 12 Five Star School District and had been teaching at DeVry University. So the author's institutional affiliation reflects the school district at this time. While the vulnerability assessment models were newly designed for this work, some of the cases represent earlier work where the author had designed a virtual world command center while transitioning from Regis to DeVry University in 2010. This virtual command center is based on an extensive photo archive the author created in the 1990's while touring inside NORAD, the North American Aerospace Defense Command inside Cheyenne Mountain, Colorado.

Author contribution - Sole Author

[P10]

An Institutional Risk Reduction Model for Teaching Cybersecurity

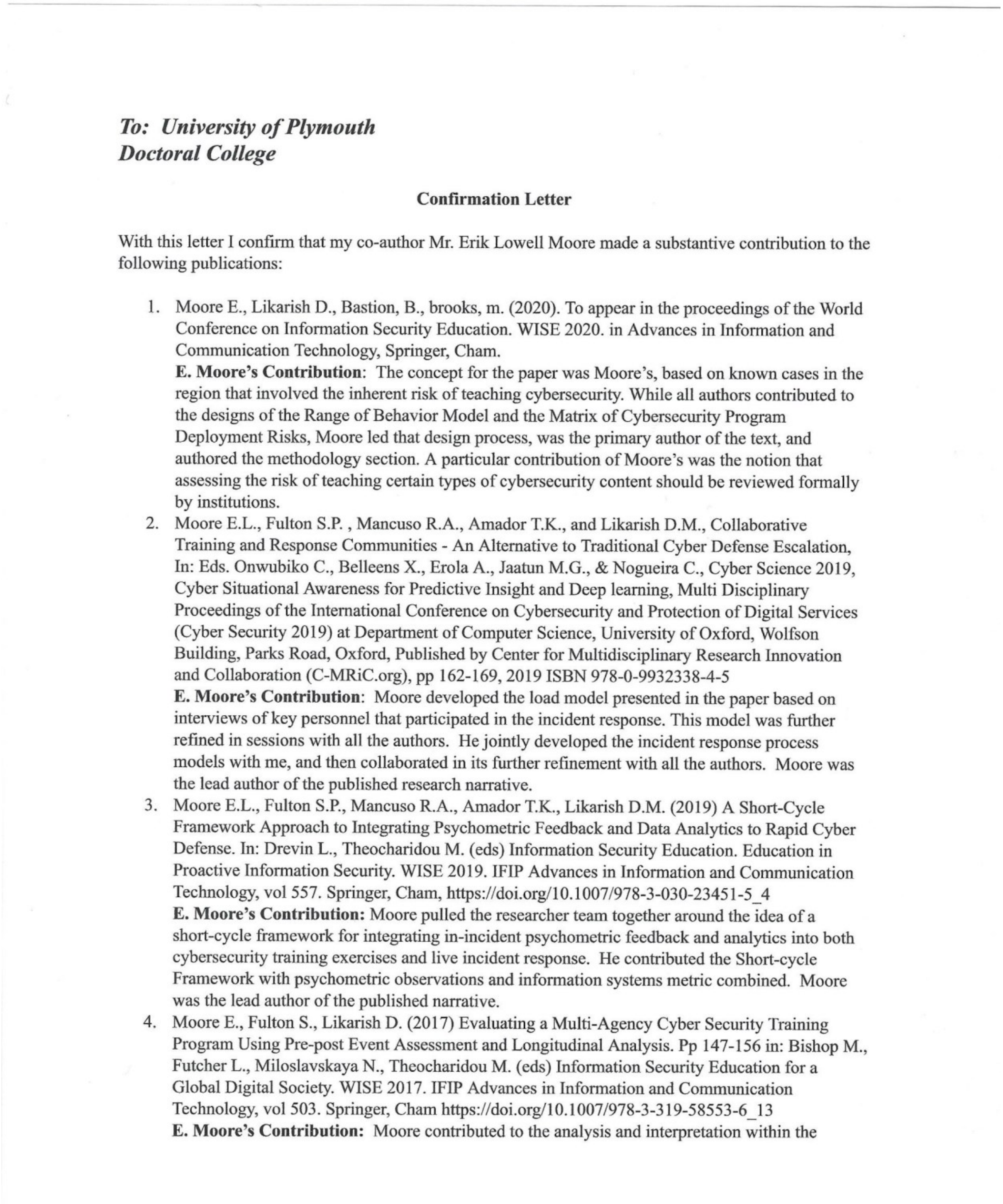
Bibliographic Information - Moore E., Likarish D., Bastion, B., brooks, m. (2020). To appear in the proceedings of the World Conference on Information Security Education,. WISE 2020. in Advances in Information and Communication Technology, Springer, Cham, https://doi.org/10.1007/978-3-030-59291-2_2

Abstract - This work presents a model for reviewing the risks of institutions teaching cybersecurity. The work is based on efforts in this direction at Regis University and Adams 12 Five Star Schools in Colorado. These two institutions are described in a comparative case study reviewing the following four aspects of addressing risk: policy, adjudication, infrastructure protection, and curricular boundaries. The model is presented in a generalizable framework to facilitate risk analysis across the education of children in public schools, university level education, and professional development programs. This framework is intended to supplement a traditional threat analysis program and not replace it. In addition to the specialized risks addressed here, institutions teaching cybersecurity are often perceived as potential targets for adversaries because of the schools as a pipeline to cyber defense activities, and because institutions teaching cybersecurity are part of societal long-term cyber defense strategies that confront criminal, nation state, and activist threats

Contributing Research Location and Time - 2019, collaboration between Adams 12 Five Star School District and Regis University in the greater Denver, Colorado area of the US. Work was primarily based on the author's experience in defending laboratory operations at these sites.

E. Moore’s Contribution - The author led the discourse used to formulate the risk reduction matrix and the Range of Behavior modeling. He provided requirements for institutional integrity, and provided policy and cyber event background that supported the relevance and usability of the models.

Appendix B - Confirmation Letters



To: University of Plymouth
Doctoral College

Confirmation Letter

With this letter I confirm that my co-author Mr. Erik Lowell Moore made a substantive contribution to the following publications:

1. Moore E., Likarish D., Bastion, B., brooks, m. (2020). To appear in the proceedings of the World Conference on Information Security Education. WISE 2020. in Advances in Information and Communication Technology, Springer, Cham.
   E. Moore's Contribution: The concept for the paper was Moore's, based on known cases in the region that involved the inherent risk of teaching cybersecurity. While all authors contributed to the designs of the Range of Behavior Model and the Matrix of Cybersecurity Program Deployment Risks, Moore led that design process, was the primary author of the text, and authored the methodology section. A particular contribution of Moore's was the notion that assessing the risk of teaching certain types of cybersecurity content should be reviewed formally by institutions.
2. Moore E.L., Fulton S.P. , Mancuso R.A., Amador T.K., and Likarish D.M., Collaborative Training and Response Communities - An Alternative to Traditional Cyber Defense Escalation, In: Eds. Onwubiko C., Belleens X., Erola A., Jaatun M.G., & Nogueira C., Cyber Science 2019, Cyber Situational Awareness for Predictive Insight and Deep learning, Multi Disciplinary Proceedings of the International Conference on Cybersecurity and Protection of Digital Services (Cyber Security 2019) at Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, Published by Center for Multidisciplinary Research Innovation and Collaboration (C-MRiC.org), pp 162-169, 2019 ISBN 978-0-9932338-4-5
   E. Moore's Contribution: Moore developed the load model presented in the paper based on interviews of key personnel that participated in the incident response. This model was further refined in sessions with all the authors. He jointly developed the incident response process models with me, and then collaborated in its further refinement with all the authors. Moore was the lead author of the published research narrative.
3. Moore E.L., Fulton S.P., Mancuso R.A., Amador T.K., Likarish D.M. (2019) A Short-Cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense. In: Drevin L., Theocharidou M. (eds) Information Security Education. Education in Proactive Information Security. WISE 2019. IFIP Advances in Information and Communication Technology, vol 557. Springer, Cham, https://doi.org/10.1007/978-3-030-23451-5_4
   E. Moore's Contribution: Moore pulled the researcher team together around the idea of a short-cycle framework for integrating in-incident psychometric feedback and analytics into both cybersecurity training exercises and live incident response. He contributed the Short-cycle Framework with psychometric observations and information systems metric combined. Moore was the lead author of the published narrative.
4. Moore E., Fulton S., Likarish D. (2017) Evaluating a Multi-Agency Cyber Security Training Program Using Pre-post Event Assessment and Longitudinal Analysis. Pp 147-156 in: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, vol 503. Springer, Cham https://doi.org/10.1007/978-3-319-58553-6_13
   E. Moore's Contribution: Moore contributed to the analysis and interpretation within the

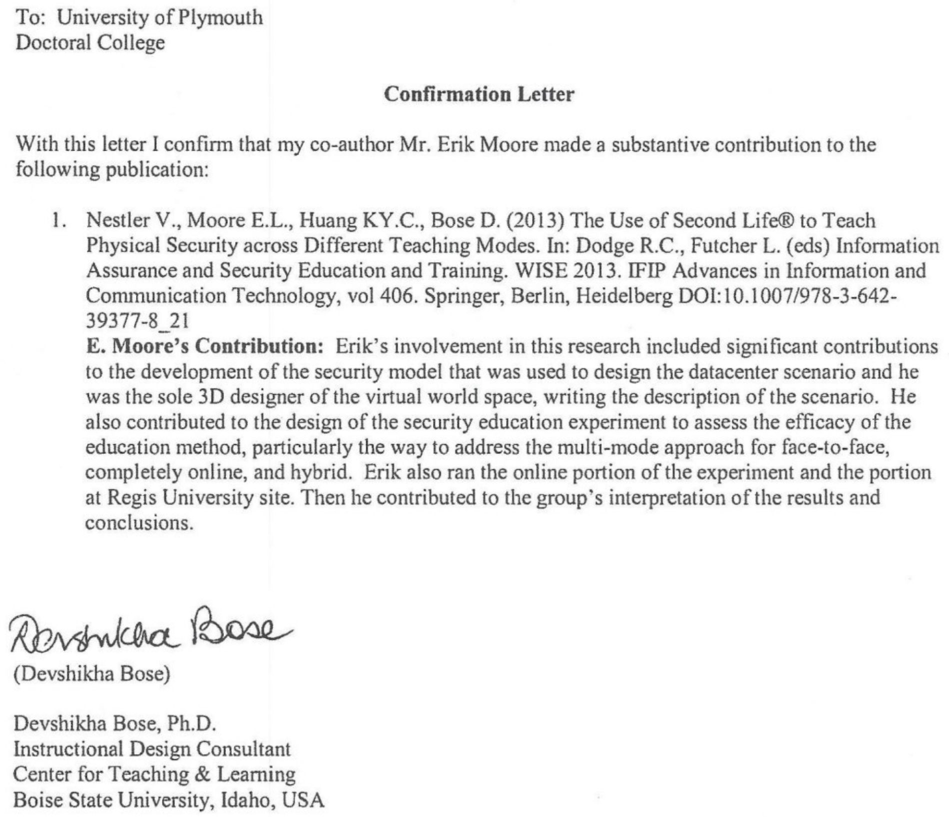
conclusions based on student tests for understanding and self examination. This led to an understanding of recommendations for experimental design and the potential impact to students. Moore was the lead author of the published research narrative.

5. Moore E., Likarish D. (2015) A Cyber Security Multi Agency Collaboration for Rapid Response that Uses AGILE Methods on an Education Infrastructure. In: Bishop M., Miloslavskaya N., Theocharidou M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham, doi.org/10.1007/978-3-319-18500-2_4
   E. Moore's Contribution: Moore developed the Framing Forward Model, characterizing operations processes and practices for an information systems and cybersecurity research laboratory environment that he developed over a period of multiple years. The techniques he described in the research resolved issues of unreliable resources and yet still offer a resilient program. Moore also contributed to refinement of the X-model design reflecting the shift of operations to multi-agency collaboration. He worked closely with me to perform the gap analysis and was the primary author of the narrative.
6. Erik Moore, Daniel Likarish, Multi-Method Virtualization: An Architectural Strategy for Service Tuning, in: IEEE Xplore: Proceedings of 2010 43rd Hawaii International Conference on System Science, 5 January 2010 https://doi.org/10.1109/HICSS.2010.281
   E. Moore's Contribution: Moore co-designed the Virtualization Layer models and developed individual virtualization models in the paper based on a set of technical solutions that had been identified by the co-author. Moore was the primary author of the research narrative.
7. Heath Novak, Daniel Likarish, Erik Moore, Developing Cyber Competition Infrastructure Using the SCRUM Framework, pp. 20-30, in Ronald Dodge Jr., Lynn Futcher, (eds) Information Assurance and Security Education and Training, DOI 10.1007/978-3-642-39377-8, Proceedings of the 8th International Federation of Information Processing working Group 11.8, World Conference on Information Security Education, proceedings of the conference, "WISE 8", Auckland, New Zealand, July 8, 2013
   http://dl.ifip.org/db/conf/ifip11-8/ifip11-8-2013/NovakLM13.pdf
   E. Moore's Contribution: In the narrative Moore described and analyzed practices that he had developed in the operations of the research laboratory that became the cases to which the Agile methodologies were applied. Moore also provided validation of the application of the AGILE model presented in the paper.

Professor Emeritus, Daniel M. Likarish

D. M. Likarish

Denver, Colorado, USA, May 28th, 2020



To: University of Plymouth
Doctoral College

Confirmation Letter

With this letter I confirm that my co-author Mr. Erik Moore made a substantive contribution to the following publication:

1. Nestler V., Moore E.L., Huang KY.C., Bose D. (2013) The Use of Second Life® to Teach Physical Security across Different Teaching Modes. In: Dodge R.C., Futcher L. (eds) Information Assurance and Security Education and Training. WISE 2013. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg DOI:10.1007/978-3-642-39377-8_21
   E. Moore's Contribution: Erik's involvement in this research included significant contributions to the development of the security model that was used to design the datacenter scenario and he was the sole 3D designer of the virtual world space, writing the description of the scenario. He also contributed to the design of the security education experiment to assess the efficacy of the education method, particularly the way to address the multi-mode approach for face-to-face, completely online, and hybrid. Erik also ran the online portion of the experiment and the portion at Regis University site. Then he contributed to the group's interpretation of the results and conclusions.

Devshikha Bose
(Devshikha Bose)

Devshikha Bose, Ph.D.
Instructional Design Consultant
Center for Teaching & Learning
Boise State University, Idaho, USA