# A Layered Model for Building Cyber Defense Training Capacity

Erik L. Moore, Steven P. Fulton, Roberta A. Mancuso, Tristen K. Amador, Daniel M. Likarish

# A Layered Model for Building Cyber Defense Training Capacity

Erik L. Moore[1[0000-0003-1566-526X]] and Steven P. Fulton[2[0000-0001-6962-8558]] and Roberta A. Mancuso[1[0000-0002-1486-5748]] and Tristen K. Amador[1[0000-0003-0622-8877]] and Daniel M. Likarish[1[0000-0001-5654-710X]]

[1] Regis University, Denver CO 80221, USA
{emoore,rmancuso,tamador,dlikaris}@regis.edu

[2] USAF Academy, Colorado Springs CO 80840, USA
Steven.Fulton@usafa.edu

**Abstract.** As technology proliferates and becomes indispensable to all functions of society, so does the need to ensure its security and resilience through cyber defense training, education, and professional development. This paper presents a layered model that supports cyber defense training progressively through the development of technology services, digital context, performance assessment, and impact analysis. The methods used were applied to college laboratories associated with cybersecurity classes, defense training exercises, cyber based competitions, and graduate research program designs. The service layer presents methods for developing the technical infrastructure and agile deployment necessary to support cyber defense training. This then is layered with conceptual frameworks to guide teams as they immerse into scenarios within cyberspace. To enhance team performance in this space and to enhance the value of the training process itself, psychometric feedback, Agile methods, and quantitative assessments are used to track efficacy and facilitate future development. The final layer represents active incident response and ongoing collaborative efforts between institutions and across disciplines. The work is presented as a progression and illustrates a decade of research from 2010 to 2020. The context has been updated here with the intention that it can be used as a guide for designing a broad range of collaborative cyber defense and cyber range programs. The influence of socio-behavioral factors increasingly illuminates the path forward.

**Keywords:** Cyber Defense, Cybersecurity, Psychometrics, Agile, Cyber Range, Collaborative, Training, Education, Behavioral, Teams, Societal, Capacity

## 1 Introduction

This paper describes a path of increasing cyber defense capability that has demonstrated significant benefits within and across the layered model for cybersecurity students, faculty, practitioners, and partnering organizations. The framework describes layers that represent both new levels of capabilities and underlying technological and organizational foundations. In early 2001 the authors were building laboratory infrastructure for university information technology

programs. The pivot to using this space for cyber competitions started occurring by 2005. The authors started publishing the underlying work for this framework by 2010 and the resultant modeling is still used in their work currently. This layered approach ensures a robust model of collaborative services among peer institutions that are working to build cyber defensive capabilities, including all levels of government (federal, state, and local), academia, industry, and cyber defense organizations. The origin of this work was an effort to build laboratory environments, using Agile development techniques to provide immersive, hands-on experiences to Regis University students anywhere on the Internet. In 2005, Regis University started the process to obtain authorization as a National Security Agency Center for Academic Excellence (CAE) in Cybersecurity Defense, adapting curriculum and mapping to federal standards. The Regis team worked to attain this designation in 2007, partially inspired by the cyber competitions that were occurring in the area.

Several related publications describe the general national trend toward cybersecurity competitions and inter-collegiate collaboration at that time [1,2,3,4]. While this work influenced the authors, our research focuses on describing, in a way designed to be replicable, the method of building capacity at multiple layers that has led to agile and collaborative communities of cyber defense training. Further, our work and these communities are uniquely informed by socio-behavioral and psychometric based training.

**Table 1: CyCap** A layered model for building cyber defense training capacity that illustrates the range of affecting technical infrastructure to societal norms for sustainable cyber defense [5]

| | | | | |
|---|---|---|---|---|
| **L4** | **Societal** | Collaborative Response Communities | Interdisciplinary Collaboration | Risk Reduction |
| **L3** | **Programmatic** | Psychometric Feedback | Multi-Agency Collaboration | Technical Training Evaluation |
| **L2** | **Contextual** | Digital Identity | | Cyber-Influenced Reality |
| **L1** | **Infrastructure** | Service Development | Immersive Virtual Scenarios | Agile Service Provisioning w/ Unknowns |

By 2007, several universities in Colorado had initiated significant collaborative cyber competition efforts, particularly the United States Air Force Academy, Colorado State University, and the University of Colorado, Boulder. This led to coordinated work in both the Computer and Network Vulnerability Assessment Simulation (CANVAS) competition beginning in 2007 and the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) beginning in 2011. This context provided the motivation that led to a rapid capacity-building program as described in the model presented here.

By 2016, collaboration with Regis faculty regarding behavioral analytics and psychometric instrumentation allowed the team to add capacity to include support for team behavior during training and actual incident response.

Our framework is built on the experiences of the authors as we navigated the challenge of maturing and adding technology-based services, providing digital context, ensuring assessment, and developing analytical capabilities. On reflection this was much in the same way that the Capability Maturity Model Integration (CMMI) represents progressive development of technical capabilities [6]. It was actually based on our progressive effort over time, which allowed for the creation of a robust Collaborative Training and Response Community (CTRC) within an empowering socio-technical environment. The compounding capabilities illustrate how a roadmap of progressive development can be built, offering value as each new layer of capacity is added, as seen in Table 1.

**Table 2:** Matrix of cyber defense capacity building efforts mapped to the CyCap model.

| Focus | Differentiating Traits | Overlap with The Cyber Defence Training Capacity Building Model Presented Here | Model Examples | Relates to CyCap Layers |
|---|---|---|---|---|
| Cyber Range computing platform, infrastructure provisioning, software provisioning, and scenario engine, describing a used build | Cloud-ready, or hardware/software-driven scenario deployment, can be used for exercises, training, and research & development | Models of infrastructure dependencies designed to describe cybersecurity training for multiple professions to meet scenarios of multi-organizational collaboration. | AIT Cyber Range [7]<br>NCR, Michigan, Virginia, IBM, CRATE, Cisco, UD, NATO, DOD, Raytheon, Baltimore, Florida [8] | L1-L2 |
| Institutional program-oriented effort for role preparation | Skill, knowledge, competence-driven, merging multiple standards | Layered model, success expectations | Finnish Cyber Security Degree Program Model [9] | L3 |
| National scale multi-model collaboration architecture for coordinated response | Holistic approach to solutioning that includes societal action implemented through multi-sector rapid reaction teams | Contextualizing/situational models, collaborative modeling at the organizational level | Cyber Resilient Bulgarian National Model [10] | L3-L4 |

A review of literature suggests that the CyCap layered model presented in Table 1 appears to be relatively unique in that it illustrates a span of concerted effort starting at the technical infrastructure level (L1), providing cyber contextual level (L2) for participants in the immersive experience, adding a layer (L3) for tuning and evaluating the programmatic output, and sets a layer (L4) for establishing organizational and societal structures is both the result of training, and a structure that can maximize how cyber resources are leveraged. A representative sampling of work represented in Table 2 suggests the the focus of most cyber defense capacity generally addresses at only a single layer, either at the national (societal L4) level structure, the curricular structure of institutions (programmatic L3), the changing experience of an

immersive digital experience (contextual L2), or the technical challenges of creating a robust cyber environment (infrastructure L1).

Table 2 maps several models that illustrate cyber defense training capacity building to the various layers of the proposed CyCap model which refers to four interdependent layers of cyber capability or capacity. The categorized models offer focused value in specific areas such as cyber ranges, curricular models, hands-on defense training scenarios, or inter-organizational cyber defense collaboration modeling. Across a review of US and international efforts to bolster cyber defense, this compartmentalization of efforts into the CyCap layers is a commonality. This is reflected in the use of standardized modeling at each layer, such as facilitating workforce skill, knowledge, and ability development based on standards such as the US National Initiative for Cybersecurity Education (NICE) [11]. The cyber range row in Table 2 owes a significant debt to Priyadarshini [8] who provided a broad survey of cyber range activity across the US.

## 2 Research Methodology

This work uses a case study methodology. This methodology was selected because the quantitative and qualitative research methods in the underlying papers varied as appropriate for the individual challenges at the time, but do not aggregate well as a single research method except through treatment of the entire effort as a case [12]. The work is summarized here as a multi-year effort that led to the development of the CTRC. The analysis presented here draws on a series of published works produced by the authors and their peers over a span of 10 years as well as extant material from the described events. The research question addressed by this case analysis reflects on this decade-long effort, asking "What components can be used to create a collaborative training and response community, and can they be added incrementally to support an effective cyber defense capability for society?"

The methodologies of the underlying published work, and the strategy of application, are described below. This list includes the rationale for using methodologies and a critique of appropriateness. This review of research methodologies of the earlier work is offered as part of the decade-long case analysis presented here as a reference for those engaged in similar lines of research.

### 2.1 Primary Research Methodologies

**Case study:** As the authors were describing events and projects where they did not have sufficient control to establish quantitative measures, the case study methodology provided the ability to describe events and projects while analyzing actions and outcomes of large groups that were collaborating in less structured efforts. The work represents more structured and finite events, the level of formality of the methodology increases. For instance, a less formal application was in early use of the SCRUM framework to produce competitions [13] where many participants were temporary and goals fluctuated. The most formal application of case study was later in the body of work when a more formal effort to develop multi-agency collaboration was facilitated

using Agile methods [14]. The level of structure of the events was a limiting factor on the formality of case study methodology.

**Quantitative pre-post testing** methodology [15] was used to measure technical skill of cyber defense training participants, evaluating variance in objective capability and self-evaluation of confidence with the technologies [16]. The tool was also used to determine the efficacy of a 3D virtual world training experience to determine how much students learned about physical security risks in a datacenter [17]. In both cases, the confidence level of the results was limited somewhat by either the sample size or by variance between sampled groups.

**Creswell's interrelating themes** methodology [18] was used when different types of data were gathered, from live observation of cyber defense events, post-event interviews, etc., and the authors had less control over the environment. This method was used to analyze how a gathering of institutions formed into a CTRC [19].

**Creswell and Clark's explanatory design mixed methods research** methodology [20] was used when significant quantitative data had been gathered and analyzed, and qualitative analysis could enhance the value and add context to the work, particularly where psychometric analysis was performed [16].

### 2.2 Secondary Research

**Secondary research** [21] was used by the authors to support the primary research and to support the development and application of theoretical models and frameworks in the developing contexts that were being formed in the virtual environments [22,23]. While this work was driven by observation of students' needs as they worked in immersive digital contexts and is applied there to teaching and coaching, the basis of the model development relied heavily on synthesizing extant research.

## 3 Infrastructure

The initial needs that drove the development of the service layer in Table 1 included online coursework-associated laboratory space, graduate students' need for research lab facilities, faculty need for infrastructure to support research projects, and the regional need for multi-institutional cybersecurity exercises. The diagram in Figure 1 illustrates the complexity of the challenge while also offering one of the analytical techniques developed through whiteboard troubleshooting and brainstorming sessions. The diagram uses the pipeline analysis model, nesting virtualized systems as they present to users and aggregate processing load across a broad range of technologies. The initial goal was to provide an immersive, engaging, and sustainable education experience across a broad range of client systems and internet connections while mixing a complex range of technologies like QuickTime Streaming, Second Life® virtual world immersive experiences, and active, hands-on keyboard challenges on live machines provisioned agilely to the students. Other technologies used to create a rich community at that time included TeamSpeak, Citrix, VMware, GNS3, RDP,

VNC, and SAN technologies orchestrated in small clusters so as not to overwhelm students in an individual course, but customized to the delivery of each course topic.

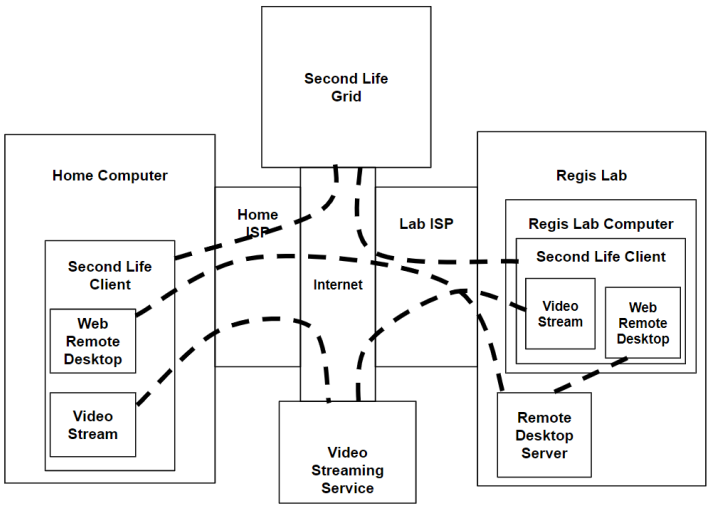



**Fig. 1.** Service Pipeline Modeling demonstrating clients both at home and in university labs

One of the greatest challenges that existed in this work at small to medium sized universities was the ability to offer this type of environment while working with limited, donated equipment, volunteer graduate students and adjunct faculty, and budget constraints all while much of the early work occurred before universities were making strong pushes into the cybersecurity space. Without this Agile methodology, the longer-term vision of building the program likely would not have been sustainable in this resource-lean environment. Because of this agile approach, Regis University was able to regularly host RMCCDC effectively for a decade, even though it was not one of the larger or significantly resourced institutions in the region.

Initially the infrastructure for these virtualized environments was based on donated equipment cobbled together by graduate students and adjunct faculty. Once the capability was demonstrated on-site, the program began to apply for grants to expand capacity. Within two years, the infrastructure was infused with sufficient servers, Internet bandwidth, and SAN storage to sustain a local cloud environment capable of projecting entire competitions over the Internet, or hosting on-site labs with each team in different classrooms.

In addition to the projection of a live "console experience" and collaborative spaces that simulate network environments, Regis also started a Second Life® campus that included a security operations center, complete with computer forensic lab, server room, conference rooms, and live workstations that included interactive consoles embedded in the virtual world as shown in Figure 2. Students could enter the world to gain more immersive experiences in Security Operations Center environments. The models developed in this world contributed significantly to the design of the Regis University Denver Technical Center (DTC) campus that was built in 2011 in Greenwood Village, Colorado. In both the physical world and the virtual world, the idea was to offer the immersive professional experience.


**Fig. 2.** Regis Security Operations Center in Second Life®.

In these virtual worlds, students faced several challenges that were not evident when engaging in a cybersecurity lab on a college campus. In order to accomplish tasks in the virtual world, students had to first overcome the idea that this environment was only a game. This distracted them from engaging fully with the scenario. It required coaching from the faculty to keep the students focused on the relevant learning tasks. Another barrier to entry was that students had to have a computer with sufficient capabilities, so some students needed to use the university computer labs when their computers at home did not meet the minimum hardware requirements.

## 4 Contextual

As Regis started providing significant numbers of immersive digital experiences in online labs, cyber competitions, training events, and collaborative events, the authors began observing variance in the way participants were behaving and relating to each other in the space. Of the two models presented here, one is a reference framework for digital identity, and the other is a matrix for analyzing the impact of cyber-influenced reality, also called “Bit Induced Reality.”

At collegiate cyber competitions, each student takes on the role of a team member in a given competition working with their teammates to successfully secure their systems. They may be further given a technical role in the environment to gain experience that they would not normally obtain in the classroom — for example, a "firewall engineer" for a fictitious company becoming responsible for all the tasks that a firewall engineer would be responsible for in a given company. This creates next identities which can cause conflicting behavioral motivations.

The goal of introducing contextual models to cyber trainees and challenge participants is to provide an orienting context for participants as they take on nested identities within events and experiences. This enables a participant’s behavior to be motivated by the right layer of identity. For example, a person may be a student at the university with the primary intention of learning from an experience. His or her

identity is nested by a team member in a scenario-based game trying to win, and within that game scenario they may be a firewall administrator attempting to defend against a cyber attack.

Many immersive digital scenarios presented in Table 3 were developed initially for CANVAS or RMCCDC and later repurposed for professional development, graduate course experiences, cyber defense training, and research laboratory support. As the authors participated in working groups designing these workshops, the driving factor was that the scenario should be taken from contemporary events and concerns, so the scenarios were similar to challenges the participants were likely to face in their professional careers. Year after year the competitions became more complex in both the scenario and in the technical challenge as teams became more prepared for the challenges.

**Table 3:** Immersive digital scenarios and their contemporary sources

| Scenario | Contemporary source | First use |
|---|---|---|
| Voting Protection | Diebold Hack | CANVAS |
| Myface.com on ELGG | Facebook Popularity | CANVAS |
| Smart Electric Grid | US Infrastructure Protection Efforts | CANVAS |
| Medical Records, Open EMR | Anthem Hack | CANVAS |
| Medical Device Defense | Donated Medical Devices | RMCCDC |
| Banking Security on Cyclos/Citadel | Western Union Hack | CANVAS |
| SCADA Defense | Target Hack | CANVAS |
| Regis HMO - medical Device Hack | Team Member worked in Hospital | RMCCDC |
| Hotel Management | Team Visit to Casino SOC | RMCCDC |
| Traffic Signal “Regis City” | City of Denver recommendation | RMCCDC |
| Regis Global Financial Services | Equifax Hack | RMCCDC |
| Online Gaming Companies | 2011 STEAM® Hack | RMCCDC |
| Electric Dam Tampering | Cyber attack on Dam in Rye, NY | CTRC |
| Town Electrical Grid | National Guard | CTRC |

In cyber competitions, the digital identity of the participants is created by providing the participant with a role, a goal, and a context that is valid in that virtualized experience. In one such scenario, some of the authors witnessed a student who had taken on the role of a cyber defender and responded to a barrage of exploits from the competition hosts as part of the scenario. The student became emotionally invested in this identity, similarly to a belief structure, and this role affinity drove the student to rapid defensive actions in the digital world. While this was going on, a member of the event host team who was simulating the cyber attack attempted to perform an in-person view of the defending team’s whiteboard in their classroom through a hallway window. The defending student responded by racing out the door and beginning a physical scuffle with the attack team member. The digital identity in-scenario had become high-stakes as the student felt both a strong affinity for the cyber defender role, and allegiance to his team. The exuberance at that moment began

to violate basic assumptions of the competition and of orderly conduct on a college campus. The effects of this immersive digital identity within the scenario may have had a significant impact on the motivating frame of reference of the student.

**Table 4.** The B/K-A/E model representing Belief/Knowledge and Allegiance/Ethics.[22]

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

Explaining the experience from the Belief/Knowledge (B/K-A/E) model in Table 4, students can become more self-aware of their investment or "belief" in a frame of reference and "allegiance" with and motivated by that role. Using the model they become more able to discern how much that frame of reference is driving their behavior. "Belief" is used in a specific way here to refer to the level of motivational engagement in a particular frame of reference. We can think of it as "How real in this moment is it that I'm the firewall defender?" If the participant is high in the Belief/Allegiance (B/A) scale for a nested identity of "firewall defender," this can affect the coherence of their primary role in the competition as a student. To counteract this issue, students are reminded through this model to self-assess with critical thinking what knowledge should drive their behavior, and the appropriate ethical framework that should set boundaries on that behavior on the Knowledge/Ethics (K/E) side of the model [22]

A very different example occurred when the competition was held at the United States Air Force Academy and illustrated the impact of cyber-influenced reality. All arrangements for the conference had been made digitally with the competing universities, primarily using email and telephone communications. When participating teams and coaches arrived at the US Air Force Academy, they were met by two student greeters who were dressed in civilian clothes, carrying a clipboard, and offering guidance to the student participants and faculty alike. No introductions were made, but the student greeters presented confidently in their role. The opening for deception occurred since the trust of the digital relationships transferred to the greeters, even though no participant team had met them before. This remained true even though the students did not wear military uniforms (unlike other US Air Force Academy cadets), nor did they present credentials. Each team trusted the greeters with an extended excursion before ending up at the competition; no students or faculty

questioned them. Fortunately they were operating under the guidance of the sponsoring faculty as part of a study in social engineering [24].

In Figure 3, the Bit Induction Scale shows the range of how digital systems influence objects in the real world. At level zero a person in civilian clothes is observed. At level 2 a computer-printed photo ID might have been printed on a computer and used for physical identity confirmation. At level 5 email communications would not even exist in a meaningful way without the Internet. Figure 3 displays how the dominant mode of security that shifts from a primarily digital context of email establishes trust to the physical situation of being greeted at an institutional entrance. When the student greeters were confronted in a physical mode, the trust established in email should not have automatically transferred without a digital authentication linked to the email. Because of this disconnect in the scenario, the physical modes of establishing trust have been undercut. If the student greeters' contact information had been presented in the email, physical trust could have been established with more assurance, rather than relying on insufficient trust established via email.

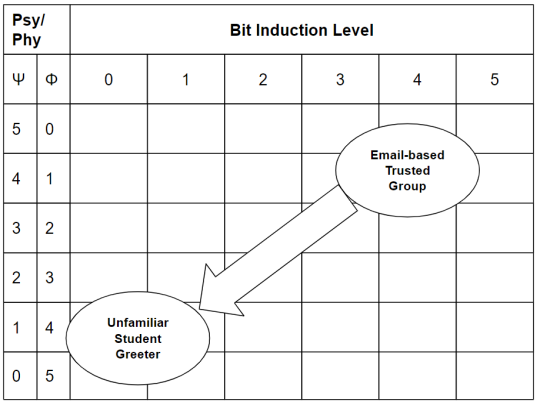



**Fig. 3.** The Bit Induction Level set against the physical/psychological significance of an object.

These brief examples represent a significant number of observations during digital challenges and stressful training that suggest a need to address cyber identity and the shift in security postures that accompanies immersive cyber experiences. Models of this type become necessary to support participants in these experiences, where the evolutionary instinctual responses and previous interpersonal experiences that participants bring to the event may not have prepared the participant for immersive interaction in cyberspace. While the frameworks presented here were applied to the immediate situations, the observations suggest that more work on these types of cognitive dissonance and disconnect from the most relevant social frames of behavior is necessary.

The leadership of the CTRC engaged across disciplines at the university, discussing what was happening in the cyber defense exercises. Based on these discussions, in 2015 the CTRC leadership invited socio-behavioral experts to observe what was

happening in these digitally immersive experiences. The scenario at that event was the defense of medical devices in a hospital from a cyber attack. The socio-behavioral experts observed the digital role-based behavior in this scenario first in a competition, and then when it was used in a cyber defense exercise, and then in the formal planning group of the CTRC.

## 5 Programmatic

As cyber competition and training events progressed, questions emerged among the training leadership team such as, “What can we do to extend and add value in terms of effectiveness to the training and response experience?” and “What are the needs of the teams we are training?” These questions initiated a collaborative effort to identify individual and team characteristics that could elevate team performance. The goal was to create awareness and build knowledge and skills among individuals and teams with regard to their strengths and limitations. This was done in order to develop more effective and efficient teams during training and in actual incident response. Further, the goal was to fully develop individuals and teams that were prepared to respond rapidly and deliberately to incidents. In the past, the authors trained cyber defenders to narrowly focus on highly technical skills used individually. We shifted our training of cyber defenders into a more comprehensive and holistic approach that continued to include highly technical skills but were utilized by all individuals as a cohesive and unified team. More recently, the focus of this work included socio-behavioral factors rather than solely technical factors.

As the mission of cyber defense teams formed, additional activities identified that could be facilitated by socio-behavioral support included cross-institution team training for rapid collaboration, tabletop exercises to work out playbooks, and strategic leadership planning sessions for expected cyber attacks. The authors facilitated the performance assessment and advancement through the use of psychometric instruments and a feedback and coaching process. The authors included specific psychometric instruments such as the Myers-Briggs Type Indicator (MBTI) [25] to evaluate individual personality traits, the Parker Team Player Survey (PTPS) [26] to evaluate team player roles, and the Crew Cohesion Scale (Crew) [27] to evaluate cohesion of team members. These psychometric instruments provided a comprehensive method for assessing individuals and teams and then advancing their ability to utilize their individual strengths in personality and leverage role diversity to the benefit of the entire team.

The choice of psychometric instruments grew out of the authors’ realization that one of the most significant barriers to cyber defenders was team members’ reluctance to communicate with each other during training exercises. The stereotypical cybersecurity team is composed of IT introverts who prefer interaction with computers over human colleagues. Yet, the authors’ real-time observations of the most effective cyber defense teams have consistently shown that open communication between members is linked to greater success [28]. Not only does the MBTI identify the degree to which individuals prefer introversion over extraversion (which often translates into a preference for written versus verbal communication), but it also recommends strategies that introverts can adopt in order to increase effective

communication when the context demands it. Moreover, the MBTI identifies individuals who prefer to attend to the smaller building blocks of a problem versus the "big picture"; the ability to tackle an incident by utilizing both of these perspectives is critical to cyber defense.

Additionally, a review of research on highly-effective teams indicates that role diversity within teams is associated with better performance. The PTPS was then selected as a well-known, reliable, and brief assessment of the roles that people adopt in team settings. This would also allow the authors to test their assumptions about greater role diversity in the context of cyber defense: When team members adopt all four of the roles identified by the PTPS, and create maximum role diversity, teams are most effective.

A measure was then needed that would provide a more holistic assessment of the team and its members' ability to work as a unified front, so the Crew was chosen as a global measure of team cohesion. This measure is most commonly used to assess the cohesion of first responders in crisis situations, particularly firefighters. The Crew is well-suited to assess teams in the crisis environment that emerges as the result of a cyber attack.

As more data were gathered, it became clear that the best course of action was to design an instrument that focused on the key variables of interest in the context of cyber defense while leaving extraneous variables behind. For this reason, the authors have begun to build and test a specialized instrument that will identify the trait preferences, team roles, levels of cohesion, and additional factors that are most consequential to cyber defense. The ultimate goal in this endeavor is to use the data to create a plug-and-play type of coaching mechanism so that at a moment's notice, cyber defense teams can be composed of available technical experts with a range of trait preferences who receive strategic directives that maximize their leadership capabilities, communication effectiveness, and role diversity.

This work focused on organizational relationships with and between cyber defenders as team members and also with and between multiple agencies including industry (private sector), government (federal, state, and local), and academia (Regis University and the United States Air Force Academy). This multi-agency collaboration was based on long-standing, cooperative relationships and mutually beneficial partnerships that leveraged the interdisciplinary nature of the teams and a more coordinated and strategic response. This kind of comprehensive response to developing cyber defense teams within and across organizations for mutual benefit is powerful and can only be achieved through a true CTRC. A CTRC builds bridges within and between cyber defense teams in industry, government, and academia in order to provide training and incident response that will be strong and sustainable over time in a rapidly growing world of cybercrime.

Quantitative Pre-Post assessment of the efficacy of the cyber defense challenge events was another significant basis for determining how to advance the effectiveness of the CTRC. [16] The Pre-Post assessment used both objective testing of skills as well as self-assessment as measures to determine participant readiness. Covered skills included things like the network scanning utility NMAP, network traffic analyzer Wireshark, and a suite of forensic tools. While the sample sizes in this work were relatively small, as limited by the size and participation of the team being assessed, the work suggested increases in skill level, particularly across multiple events. Some

increased skill levels can be attributed to the additional training in certifications required by employers. As discovered in discussion, some individuals' personal intensive studying and practicing between events also contributed to their overall improvement.

The results of this work suggests that across a three year longitudinal assessment, participants self-perceived skills did not consistently advance across a technical range. Yet their actual capabilities as demonstrated in a longitudinal pre-test doubled in capability over the same period. The quantitative results in specific categories are available in previous work by three of the authors [16]. Based on discussions with participants, this variance between self-perception and capability may partially be attributed to a growing understanding of the related body of knowledge and their changing perception of where they sit within that discipline. Also, the participants may not be accounting for growth in relation to self-study. The previous work also presents the Personalized Education learning Environment (PELE) is designed to account for these variances while tracking participants across institutions.

## 6 Societal

Once the first three layers were functioning and the CTRC had formed, new functions needed to be added as the CTRC: responded to actual cyber attacks; engaged a range of interdisciplinary subject matter experts; began to analyze the organizational risks inherent in the cyber defense preparation work itself. The authors began to analyze these new functions to offer the CTRC a more fluid team engagement with external entities and to evaluate its role and risks as part of the cyber defense capacity building sector.

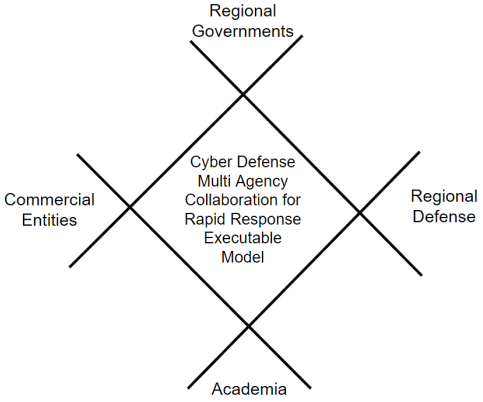
The reason that the Societal Layer (L4) of the CyCap model (Table 1) was developed was to develop the capability to address the inter-institutional interest in leveraging the first three layers (L1, L2, L3). The dynamic tension of this challenge is illustrated in Figure 4 as the interaction between four different types of entities.

The initial live cyber defense response that occurred was in reaction to a highly disruptive attack on the Colorado Department of Transportation (CDOT) in early 2018. The Colorado National Guard responded as an integral member of the CTRC. A primary advantage was that the response team had trained with many responders from other agencies, so that command structure, team formation, and strategic assignments could happen more rapidly than with usual incident response. Because many jurisdictional and logistic issues had been resolved in that training, they were even able to give a significant number of defenders at CDOT an opportunity to rest and recover as they took over defensive operations resulting in a successful network defense [29].

After the CDOT event, an interdisciplinary model was created to clarify how psychometric support for cyber defense teams could be incorporated into both cyber defense training and response to enhance team effectiveness. One exercise involved pulling the leaders out of each team to determine the adaptive capabilities of the team. Another included assembling response teams across institutions in order to analyze their rapid team formation and develop strategies and coaching methods. The authors see this work as opening up a range of interdisciplinary opportunities and have

therefore created models for forming fluid teams within the CTRC to allow interdisciplinary work to expand [30].

**Figure 4:** an executable model (X-model) representing the partners in a multi agency collaborative for rapid response. [14]




With trained students, professionals, and cyber defense teams actively engaged in cybersecurity and cyber defense, the authors began focusing on a new need, reducing risks for institutions that perform cybersecurity training and cyber defense. The first aspect of this work addressed the risks associated with the behavior of students and the professionals engaged in training and the potential culpability of the training organization if skills were misused [31]. The initial value of this model is the identification of key programmatic risk controls in the teaching, training or competition. The model is used across public education cyber challenges, college education, professional development, and cyber defense training. The institutions analyzed as the initial cases where these methods were applied included Adams 12 Five Star Schools (representing the public sector) and Regis University (representing higher education, research, professional development, and cyber defense training).

The areas of control are: 1) curricular limits, 2) technical controls such as firewalls, 3) ethical engagement with participants in curriculum, and 4) institutional behavioral policies and agreements. The particular controls vary widely across each of the groups considered, but hold their value across that range. A good example was that for minors in public education, teaching proactive cyber defense attack skills should be assessed as potentially causing too much risk for the student, the teacher, and the institution.

A second value of the work is a set of models tracking participant behavioral risk across different situations. The risk case analysis extended beyond the direct relationship with the institution and on-campus technical controls, and includes potential behavior of participants after the training at home, work, and other locations where the training and motivation might be tracked back to the institution. With a broad set of risk controls, an institution can mitigate off-site risk that may not be anticipated in traditional cybersecurity risk analysis [31].

## 7 Conclusion

The layered model for building cyber defense training capacity is an empirical framework derived from a series of quantitative and qualitative studies of a decade long effort. This analysis of a long-term program development represented in the layered model offers an example and some ready methods for those engaged in similar work. The authors continue to focus on the development of cybersecurity programs using this layered model as a reference when creating course focused lab exercises. As a new cycle of capacity building starts, however, developing a more systematic and agile approach using this or a similar model could help to define the overall challenge more clearly. Our approach is intended to further the incorporation of human-centric psychometric instruments and behavioral coaching tools designed to enhance participant experience in the potentially disorienting world of immersive technical cyber training and defense. It also adds a significant layer of inter-organizational and interdisciplinary structure to facilitate collaboration.

The CDOT incident represents a new level of capability in society in regard to cyber defense, in that it is the first time in the United States that a National Guard unit came to the cyber defense of a state government. They did this in conjunction with other participants in the CTRC. The CyCap model lays out how this new level of capability was achieved.

The authors publish this in the hopes of finding common vocabulary for such efforts that will lead to new forms of collaboration. Detailed analysis of each section of this work are available in papers previously published by the authors [5]. Currently the authors are working to expand these research interests to larger scales of collaboration. As cyber ranges, cyber defense training programs, and cyber defense collectives grow in popularity and scope across the United States and across the world, the models and details of progressive development presented here are designed to help reduce risk and systematize their work, thereby enhancing the stability of our modern digital society.

## References

1. Carlin, A., Manson, D., Zhu, J.: Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). Information Systems Education Journal, Vol. 8, No. 14. (2010).
2. White, G. Ph.D., Williams, D.: Collegiate Cyber Defense Competitions. The ISSA Journal, October (2005).
3. 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), 27–33 (2005).
4. Fulton, Steven, Dino Schweitzer, and Judson Dressler.: What are we teaching in cyber competitions?. Frontiers in Education Conference Proceedings. IEEE (2012).
5. Moore, E.: Building Cyber Defense Training Capacity, doctoral thesis, University of Plymouth (2020).
6. 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, (1993).

7. Leitner, M., Frank, M., Hotwagner, W., Langner, G., Maurhart, O., Pahi, T., Reuter, L., Skopik, F., Smith, P. and Warum, M.: AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research. In Proceedings of the European Interdisciplinary Cybersecurity Conference, pp. 1-6 (2020).
8. Priyadarshini, I.: Features and architecture of the modern cyber range: a qualitative analysis and survey. Masters Thesis, University of Delaware (2018).
9. Saharinen, K., Karjalainen, M., & Kokkonen, T.: A design model for a degree programme in cyber security. In: Proceedings of the 11th International Conference on Education Technology and Computers, pp. 3-7 (2019).
10. Sharkov, G.: From cybersecurity to collaborative resiliency. In: Proceedings of the ACM Workshop on Automated Decision Making for Active Cyber Defense, pp. 3-9 (2016)
11. Newhouse, W., Keith, S., Scribner, B., & Witte, G.: National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, 800, 181 (2017).
12. Smith, C.: The case study: a useful research method for information management. In: Journal of Information Technology 5.3, pp. 123-133 (1990).
13. Novak, H., Likarish, D., & Moore, E.: Developing cyber competition infrastructure using the SCRUM framework. In: Information Assurance and Security Education and Training (pp. 20-31). Springer, Berlin, Heidelberg (2013).
14. Moore, E. and Likarish, D.: A cyber security multi agency collaboration for rapid response that uses agile methods on an education infrastructure. In IFIP World Conference on Information Security Education (pp. 41-50). Springer, Cham (2015).
15. Gall, M., Gall, J., Borg, W.: Educational research: An introduction, 8th Ed. Pearson (2006).
16. Moore, E., Fulton, S. and Likarish, D.: Evaluating a multi agency cyber security training program using pre-post event assessment and longitudinal analysis. In: IFIP World Conference on Information Security Education, pp. 147-156, Springer, Cham (2017).
17. Nestler, V., Moore, E.L., Huang, K.Y.C. and Bose, D.: The Use of Second Life® to Teach Physical Security across Different Teaching Modes. In: Information Assurance and Security Education and Training, pp. 188-195. Springer, Berlin, Heidelberg (2013).
18. Creswell, J. W., & Creswell, J. D.: Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications (2017).
19. Moore, E., Fulton, S., Mancuso, R., Amador, T. and Likarish, D.: Collaborative training and response communities - an alternative to traditional cyber defense escalation. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). pp. 1-8, IEEE (2019).
20. Creswell, J., Clark, V.: Designing and conducting mixed methods research. Sage publications (2017).
21. Thorne, S.: Secondary analysis in qualitative research: Issues and implications. In: Critical issues in qualitative research methods 1. pp. 263-279 (1994).
22. Moore, E.: Managing the loss of control over cyber identity. In: 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC). IEEE (2016).
23. Moore, E.: A vulnerability model for a bit-induced reality. In: ICIW 2013-The Proceedings of the 8th International Conference on Information Warfare and Security (2013).
24. Kvedar, D., Nettis, M. and Fulton, S.P.: The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. In: Journal of Computing Sciences in Colleges, 26(2), pp.80-87 (2010).
25. Briggs-Meyers, I., Hammer, A., McCauley, M. and Quenk, N.: MBTI Manual: A guide to the development and use of the Meyers-Briggs type indicator. CPP Incorporated (2003).
26. Parker, G.: Team player and team work: The new competitive business strategy. Jossey-Bass Inc, San Francisco (1990).

27. Wildland Fire Leadership Development Program: Toolbox: Crew Cohesion Assessment Tool, April 16. 2018 (www.fireleadership.gov, accessed October 20, 2018).
28. Zarya, V., These Mormon women are some of the best cyber security hackers in the U.S. In: Fortune.com April 27 (2016).
29. Moore, E., Fulton, S.P., Mancuso, R., Amador, T., Likarish, D.: A short-cycle framework approach to integrating psychometric feedback and data analytics to rapid cyber defense. In: IFIP World Conference on Information Security Education. pp. 45-58. Springer, Cham (2019).
30. Amador, T., Mancuso, R., Moore, E., Fulton, S. and Likarish, D.: Enhancing cyber defense preparation through interdisciplinary collaboration, training, and incident response. In: Journal of The Colloquium for Information Systems Security Education Vol. 8, No. 1, pp. 6-6 (2020).
31. Moore, E., Likarish, D., Bastian, B. and Brooks, M.: An institutional risk reduction model for teaching cybersecurity. In: IFIP World Conference on Information Security Education. pp. 18-31. Springer, Cham (2020).