Improving Cybersecurity Learning: An Integration of Cyber Offense and Cyber Defense

Completed Research Paper

Hwee-Joo Kam, D.Sc., CISSP

YanYan Shang, D.Sc.

Abstract

The critical shortage of cybersecurity talent urged the President of the United States to issue the Executive Order 13800 to bolster cybersecurity workforce. Unfortunately, higher education fails to cultivate cybersecurity talent that organizations are looking for. As a result, organizations have to invest their resources to provide on the job training to their employees. To enhance the quality of cybersecurity education, this study investigates how the learning of both cyber offense and cyber defense helps individuals to gain a more thorough understanding in cybersecurity concepts. Built on Activity Theory, this study examines individuals' cognitive learning in cybersecurity. Our key findings discover that cyber offense learning cultivates effective thinking, but cyber defense engages individuals in system thinking. We then suggest the research implications accordingly.

Keywords: Cyber Offense, Cyber Defense, Activity Theory, and Cybersecurity Education

Introduction

A dearth of cybersecurity talent urged the President of the United States to issue the Executive Order 13800 for growing the cybersecurity workforce (NIST, 2017). Unfortunately, the Center for Strategic and International Studies (CSIS) revealed that higher education fails to provide skillful cybersecurity workers (Crumpler & Lewis, 2019). At this moment, not only organizations are facing a short supply of job candidates for job openings, but also candidates with inadequate cybersecurity knowledge. Despite this pressing concern, many studies in the Information Systems Security (ISS) have largely neglected the topic of cybersecurity training. Most studies in the ISS literature examined individual security behavior, specifically using General Deterrence Theory (Hearth & Rao, 2009; D'Arcy, Hovav, & Galletta, 2009), Protection Motivation Theory (Boss et al., 2015; Posey, Roberts, & Lowry, 2015; Warkentin et al., 2016), Neutralization Theory (Siponen & Vance, 2010), and Control Balance Theory (Moody, Siponen, & Pahnila, 2018). Moreover, the literature of cybersecurity education reveals studies related to the implementation of cybersecurity programs in higher education (Conklin, Cline, & Roosa, 2014; Dark & Mirkovic, 2015; Schneider, 2013), the use of simulation for learning (Nagarajan et al., 2012; Pastor, Díaz, & Castro, 2010), and the effect of cybersecurity competitions on learning (Mirkovic et al., 2015; Tobey, Pusey, & Burley, 2014). However, there are very few studies addressing how to increase the quality of cybersecurity education for easing the critical shortage of cybersecurity talent and improving the qualifications of new graduates who will soon enter the workforce.

To fill the research gap, this study focuses on enhancing the quality of cybersecurity education. Using Activity Theory (AT) (Engerström, 1999), we investigate how the learning of both cyber offense and cyber defense promotes a better understanding in cybersecurity concepts. In a cybersecurity education context, cyber offense denotes ethical hacking wherein individuals learn how to exploit system vulnerabilities that later shed lights on how to patch vulnerabilities for system protection (NIST Special Publication 800-18, 2017). On the other hand, cyber defense includes protecting IT infrastructure through system monitoring, system configuration, incident response, and vulnerability assessment (NIST Special Publication 800-18, 2017). We selected cyber offense and cyber defense as our main focus for two reasons. First, the U.S. National Initiative for Cybersecurity Education (NICE), directed by the National Institute of Standards and Technology (NIST), revealed that the workforce must be able to design, develop, implement, and maintain both offensive and defensive cyber strategies (NIST Special Publication 800-18, 2017). This suggests that cyber offense and cyber defense are relevant and important to prepare individuals to enter the workforce. Second, we argue that, by introducing cyber defense that stresses good design principles and careful planning, along with cyber offense that embodies attack understanding philosophy (i.e., system exploitation), individuals will conceive cybersecurity from multiple perspectives. As a result, this will empower individuals to gain a more thorough understanding in cybersecurity.

Our research question is: *how to improve the quality of cybersecurity education through an understanding of cyber offense and cyber defense?* This study provides two key contributions. First, we suggest the pedagogical strategies for cybersecurity learning, providing a theoretical framework related to cybersecurity education. Second, we share practical knowledge of implementing cyber offense and cyber defense in the classroom settings to enhance student learning and promote the quality of cybersecurity education. This paper is organized as followed. First, we presented literature review. This is accompanied by research design and methodology. Next, we discussed our findings. Finally, we shared our research implications, limitations, and conclusion**.**

Theoretical Framework

Activity Theory (AT)

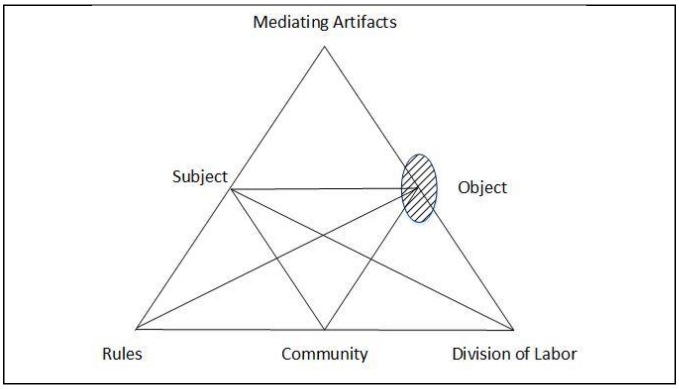

Figure 1. Triangle Framework (Engeström, 1990)

AT focuses on the interaction among subjects (i.e., actors like system administrators and ethical hackers) to identify the important concepts (i.e., behavioral model of system administrators and ethical hackers) and to suggest mechanisms of certain occurrences (i.e., explaining how and why system administrators and ethical hackers behave in certain ways) (Engerström, 1999; Kaptelinin & Nardi, 2006). Generally, activity, the unit of analysis, pertains to a subject-object interaction wherein a subject is considered an active entity (i.e., actors) whose motives is to transform an object (Kaptelinin & Nardi, 2006). Object is associated with a subject's motive in that object represents an entity that motivates a subject or that meets the needs of a subject. Overall, AT embodies a concept in which activity is "*a unit of subject-object interaction defined by the subject's motive. It is a system of process-oriented toward the motive, where the meaning of any individual component of the system is determined by its role in attaining the motive*." (Kaptelinin and Nardi, 2006, pg. 60).

The "triangle framework" of AT (see Figure 1) (Engeström, 1990) has been widely used to study technologically meditated activities (Kaptelinin & Nardi, 2006). The framework consists of subject, object, instrument, rule, community, division of labor, and outcome. In an activity system, a subject is a social actor engaging in activities and an object is the objective of the activity system. A community provides the social context for a subject, which is an integral part of the activity system (Engeström, 1999). As a subject (e.g., a system administrator or an ethical hacker) operates in and interacts with a community (e.g., organization), a subject is aware of the rules (e.g., group norms) and realizes the division of labor (e.g., tasks assigned to other subjects) in the community. Using mediating tools (e.g., software), a subject will attempt to achieve certain objectives (e.g., secure a system) decided by the community. Eventually, the outcome is that the entire activity system is transformed.

Third Generational Activity Theory (AT)

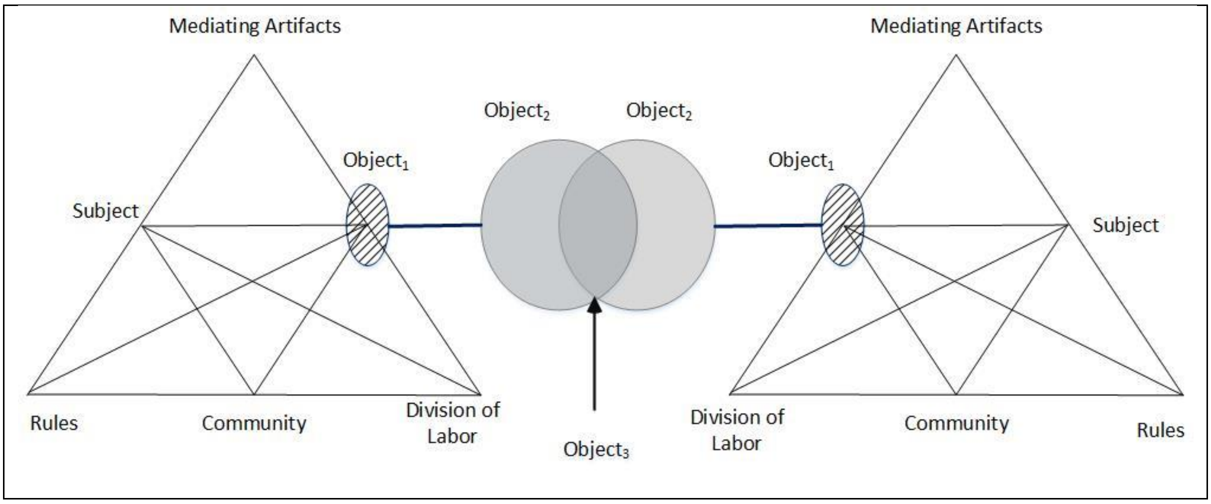

Figure 2. Third Generation Activity Theory (Engerström 2001)

Third Generation AT (see Figure 2) has two interactive systems consisting of dialogue, diverse perspectives, and interacting activities that later construct a shared object (Engerström, 2001). Engerström (2001) illustrated how third generation activity system worked in a healthcare study where patients and healthcare system were conceived as two separate, interactive systems. The objective of patients was to heal (object$_1$) and the objective of healthcare system was to provide healthcare services (object$_1$) (Engerström, 2001). When both systems interacted, patients provided information about their illness to recover (object$_2$) and healthcare system categorized patient's diseases to identify the correct diagnosis (object$_2$); and finally, both systems constructed information that produced a good diagnosis (object$_3$ - shared object) (Engerström, 2001).

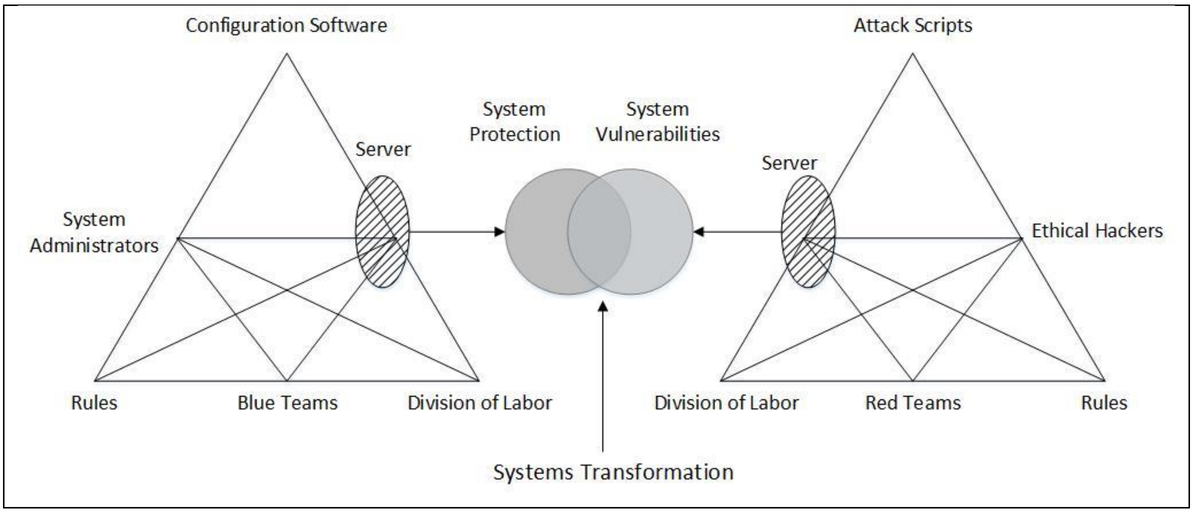

Figure 3. Theoretical Framework based on Activity Theory

In the ISS research, Chen, Sharman, Rao & Upadhyaya (2013) adopted Third Generation AT to develop a data model for fire-related emergency; and Valecha, Rao, Upadhyaya & Sharman (2019) used the same approach to build a framework for sharing critical information related to dispatch-mediated emergency response. Drawing on the Third Generation AT, we suggest that system administrators (i.e., blue teams) and ethical hackers (i.e., red teams) are two different bodies in that each body works in a separate system. The objective of the system administrators in the blue teams (i.e., cyber defense) is to secure the server but the objective of the ethical hackers in the red teams (i.e., cyber offence) is to discover system vulnerability through hacking. Then, both systems interact with each other to produce a secure server in support of systems hardening and systems transformation (shared object). See Figure 3 above.

The Third Generation AT subsumes the following five principles that guide this study (Engerström, 2001). Following these principles, we will discover the elements presented in the theory -- rules (i.e., group norms), division of labor (i.e., task assigned to individuals), and tools (i.e., software used) to unveil the differences between both groups in terms of cybersecurity learning.

1. **Unit of Analysis:** The unity of analysis is *activity* (Engerström, 2001), referring to activity system that creates actions. For example, the unit of analysis includes the actions taken by system administrators and ethical hackers within each group or the interactive between both groups.
2. **Multi-Voicedness:** Multi-voicedness involves different views, work outcomes, and system assessment expressed by system administrators and ethical hackers. Examining "multi-voicedness" between system administrators and ethical hackers will enable us to uncover the differences in motivation, performance, and operation between both groups. Additionally, this will facilitate the discovering of group norms (i.e. rules) in each group.
3. **Historicity:** History can refer to a series of past actions taken to exploit system vulnerabilities or to protect a system. Looking into the history (e.g., recurring events recorded in the log files) enables us to identify the common patterns. As a result, this will allow us to examine who is responsible for a specific task, thus revealing the division of labor in each group. Furthermore, by examining the historical events using the log files in the operating system, we can also learn the tools (i.e. software) used during system administration or ethical hacking.
4. **Contradiction:** *"Contradictions are historically accumulating structural tensions within and between activity systems."* (Engerström, 2001) Contradiction can be caused by new elements that try to integrate into the existing system. Additionally, when a new circumstance collides with group norms (i.e., values and norms of blue and red teams), contradiction emerges. In a cybersecurity context, contradictions may arise when a cyberattack disrupt the computer system.
5. **Expansive Cycles:** There will be a collaborative, deliberate change effort initiated by participants when contradiction intensifies. This will then produce transformations for objects due to expansive cycles of changes initiated by subjects. For example, during interactions (e.g., between blue and red teams), both groups may discover that the existing protection mechanisms are not effective to deter attack. This may cause a drastic change in system configuration that may result in a vastly different configuration framework.

Research Design and Methodology

Laboratory Environment and Participants

Our participants were graduate students (N=12). There were two blue (i.e., cyber defense) and red (i.e., cyber defense) teams in which each team had three members. Whereas the blue teams played the role of ethical hackers for cyber offense, the red teams acted as system administrators for cyber defense. To prepare for the penetration testing (i.e., ethical hacking) environment, we first built a vulnerable server (VS) with many security holes. We then cloned the VS and sent each server to each team. Our purpose was enabling each team to work on and run some testing in an isolated environment. Additionally, we cloned the same VS to create a community server shared by both teams (red vs. blue teams). On a designated date, each team migrated system configurations or uploaded attack scripts to the community server. All the servers could be accessed from the Skytab cloud environment. See Figure 4.

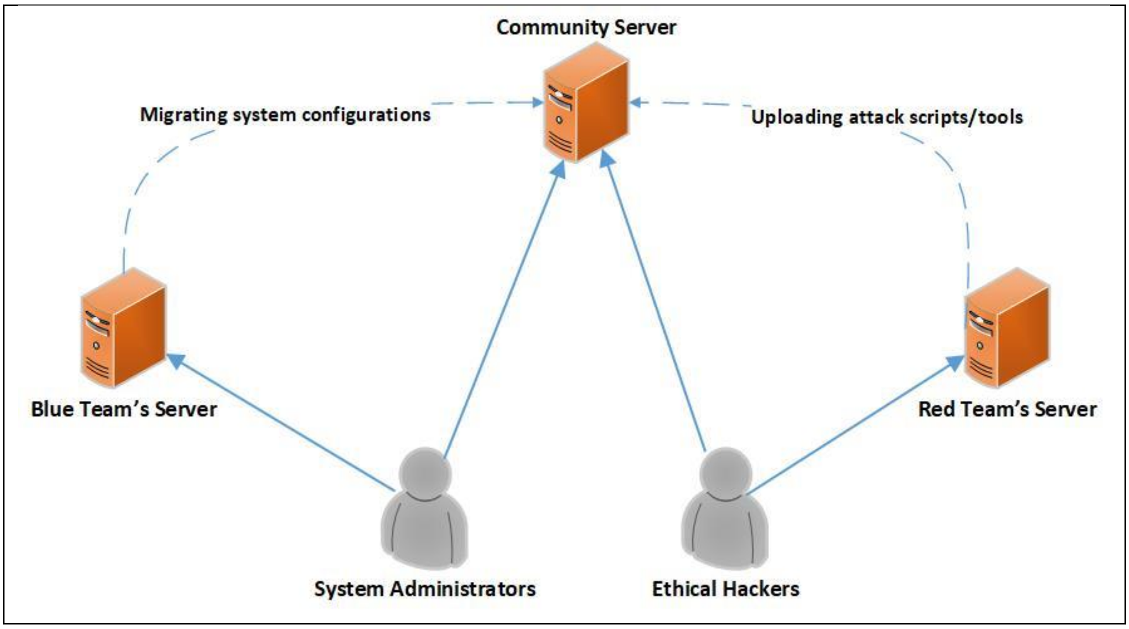

Figure 4. Laboratory Environment

Data Collection

In this study, we collected data from the graduate students in a state university in the Midwestern USA. There were two blue and red teams where each team had three group members (N=12). The average age of the participants was 25. There were 3 females and 9 males among our participants. These participants majored in cybersecurity with a concentration on either incident response or security informatics (i.e., data analytic in cybersecurity). Many of them had no prior ethical hacking or system hardening (i.e., protecting systems for cyber defense) experiences.

Overall, we planned for data collection based upon the five principles of Third Generation AT (as discussed above). Our data collection included group reports, event logs (i.e., summary of tasks), individual reports, and screenshots. The following table outlines our data collection plan.

Table 1. Data Collection

Principles	**Key Areas in Research**	**Data Collection**	**Expected Findings**
Principle 1: Activity system as unit of analysis	Study how each group achieves its goal by examining the actions and operations taken.	Each participant will record the software he or she has used along with the procedures taken.	Participant's activities consisting of actions and operations.
Principle 2: Multi-voicedness	Study factors that motivate each group and affect group dynamic.	Interviewed the participants to collect written feedback. Group reports were collected.	Motivation of each group and norms
Principle 3: Historicity	Study the pattern of actions taken by each team in the cloud environment.	Collected the event logs to uncover the patterns in the tasks.	Activities, norms (rules), and division of labor in each group
Principle 4: Contradictions	Study the conflicts and changes occurred in the blue and red teams.	Interviewed the participants to collect written feedback. Group reports were collected.	Norms (rules) and values in each group
Principle 5: Expansive cycles	Study any external (e.g., difficulties caused by the opponents) and internal (e.g. difficulties caused by other team members) struggle.	Data were collected from group reports and interviews (written feedback).	Factors that challenged the actions and efforts in an activity system.

Data Analysis

We used NVivo 12 software to conduct open coding. Specifically, we adopted content analysis to analyze the written feedback in the format of group reports and transcribed interviews. Overall, we analyzed more than 80 pages of data. Content analysis draws inferences from text to identify the psychological behavior in a group and describe behavioral responses to communication (Weber, 1985). In particular, content analysis enables researchers to classify words of the text into fewer categories (Weber, 1985). As noted, we used the five principles of third generation AT (see Table 1) as the framework of data analysis.

Moreover, we adopted semiotic method (Maasik & Solomon, 2012) under content analysis. By supporting the analysis of signs and symbols (Manning & Cullum-Swan, 1994), semiotic method embodies the meaning of signs and symbols that could then be classified into the core categories (Myers, 1997). This method supports a richer analysis of text (Manning & Cullum-Swan, 1994), and therefore, researchers could employ a content analysis to draw inferences from words and signs in the text (Myers, 1997).

In a face-to-face manner, both researchers ran open coding to identify the core categories from the participants' feedback and group reports. Any disagreements during coding were resolved by reaching a common ground. Additionally, both researchers revisited these differences after analyzing all collected written feedback. While other studies used interrater reliability to correlate the observations or scores of the raters and render an index of how consistent their ratings were (Cooper & Schindler, 2000), we did not compute the interrater reliability in this study. This is primarily because we worked together in a face-to-face manner and discussed with each other to find a common ground. Working in a face-to-face manner also allowed us to minimize any potential biases derived from preconceived notions. Finally, we conducted open coding to generate a separate set of categories for each team (blue team vs. red team). The categories generated enabled us to identify the key elements for each principles (see Table 1). The following presents the results of our data analysis.

Principle 1: Activity System as Unit of Analysis

In both the blue teams, we discovered that the key activity was constant monitoring and configuration.

> *"The work of the defensive team is never finished. Even once we had limited services and carefully selected and installed appropriate security tools on the server, applied patches and updates, we still had to monitor our server for detection of alarms….."*

> *"The challenge in Blue Team system defense is involves trying to protect everything. In both Windows OS many security processes needed to be enhanced. We had to update and patch both operating systems. We had to manually shutdown open ports and turn the firewall back on…."*

On the other hand, in the red teams, the key activities involved random attempts of attacking the target machine.

> *"We used Armitage and Metasploit to try and exploit vulnerabilities…We also tried brute force attack….Since we could not exploit their machine and get the password hashes, we tried to use the tool Ophcrack and we tried to brute force the password…"*

> *"A basic understanding of the HTML language is enough to perform XSS attack* …. *[Command line injection] became very interesting and fun. We were able to find the running process, documents, user accounts…and even perform a DDOS attack by manipulating the firewall."*

Another key difference between the blue and the red teams is the platform they picked to communicate. Although each team used a variety ways to communicate (e.g., texting, email etc.), the main communication tool differed between the blue and red teams. To facilitate team communication, the blue teams tailored a communication tool that could only be accessed by the team members.

> *"An important aspect of our communication strategy included the development of a shared GoogleDoc to document change management processes at every step of our defensive strategy…The*

> *discussion board on Blackboard was extremely valuable and used to update each group member on the progress or difficulties experienced by other members."*

> *"We used Google Chat to hold organized weekly team meetings to provide each other with updates on ...we also used Blackboard file uploads to share PowerPoint slides, recommended resources such as books or fact sheets, and report information."*

On the other hand, the red team used communication tools that has a more "open" platform and that serves other purposes aside from team communication.

> *"We communicated in a variety of ways but the method we used most was email. This allowed us to discuss how much work we have completed, challenges faced, share ideas, ask questions and share individual portions of the collaborative group project."*

> *"Facebook provides an option of sharing documents and images which helped the team to see what others were up to… The application also gives notifications of the activities performed by the team in the group and acknowledges the members who saw the activities."*

Principle 2: Multi-Voicedness

We examined team motivation and team dynamic. Virtually all the teams expressed that their motivations stemmed from a desire to learn and competitive spirit.

> *"Learning was prevalent motivation for this final project. Each of us had to do research and read books to learn how to complete the project. Without a desire to learn, the project would have failed."*

> *"Another influence that motivated our team was the drive to learn. Each member was faced with new tasks they had never encountered before and went above and beyond to try and tackle these tasks"*

As for competitive spirit, team members stated:

> *"The presence of the defense team on the other side made a huge impact on the behavior of the offense team by motivating them to dig deep and fast before the defense team fixes the vulnerabilities.…"*

> *"There was a competitive side of this project with the mission to penetrate the defensive team's server. This competitiveness gave the drive to research and test different tools on the defensive team..."*

> *"We also all seem to have a competitive streak that motivated us to secure our system as best as possible so as not to let the offensive team be successful in their attacks."*

The only difference in motivation between the red and blue teams is that the red teams were also motivated by fun.

> *"One of the tasks that we thought was interesting was exploiting a vulnerability. This would often be a distributed denial of service attack (DDoS) or a buffer overflow attack. We found this task interesting because of how common it is."*

> *"Performing an XSS attack was both fun and interesting because everyone in the team was coming up was different ideas to deface the web page."*

Additionally, the key difference in team dynamic is how the blue and red teams acted when confronting obstacles. Our data showed that the blue team coped with unexpected changes by finding a solution.

> *"One of the biggest challenges was updating Windows 7 SP1….. Windows update didn't work. Try to update Windows manual, but it didn't work. After several tries we decided to secure the windows system with other third party application. So, we increase the firewall protection and other security precaution to protect the OS."*

> *"During the system hardening and defense building period, our biggest challenge was the web application vulnerabilities…we have never worked with web application development….We had to look for had to look for alternative remediation to the known vulnerabilities. Finally, we found the use of a web application firewall (WAF)."*

On the other hand, when confronting changes and problems, the red team circumvented the problems without finding a solution.

> *"They hardened their machine really well and made sure it was not susceptible to any of these vulnerabilities…With the time we had to complete this project we could not overcome the issue. We had to accept the fact that we could not exploit their machine and we moved on to another task."*

> *"First, we tried XSS in Kali and was unsuccessful. Then we tried in the windows machine on Samurai Dojo Basic Home and found that the register page was accepting the values but not creating any users even after registering successfully. We discussed this with my team leader and he also tried it and was unsuccessful. Then we worked on SQL Injection on PHP Admin page…"*

Principle 3: Historicity

When studying the chronological lists of activities in both teams, we discovered that the blue teams had a pattern of "patching vulnerabilities" and configuring systems. On the other hand, the red teams showed a pattern of moving from one attack attempt to the next. Compared to the blue teams that started early on system configuration, the red teams focused on their attack in a relatively short period. The following table displayed the historical activities of a blue team.

Table 2. Event Logs of a Blue Team

Date	Task	Software	Description
11/18	Set User Account Control (UAC)	Windows Graphical User Interface	Set UAC to "Always Notify".
11/18	Disabled IPv6	Regedit GUI	Changed the Registry to disable IPv6. Disabled IPv6 Protocol in Local Area Connection (LAN).
11/21	Installed Internet Explorer (IE) 11	Microsoft Internet Explorer 11	Installed IE11 to try to update Windows 7 Professional
11/22	Installed McAfee	McAfee LiveSafe	Installed and configured the pack.
11/23	Installed Malwarebytes	Malwarebytes (Anti-Exploit Premium)	Installed and configured the application
11/28	Monitored traffic	Wireshark, McAfee, & LiveSafe	Filtered traffic to see Attacker's IP then changed McAfee rules.

Next, the table below shows the event log of a red team.

Table 3. Event Logs of a Red Team

Date	Task	Attack	Description
11/26	Scan for all open ports	Nmap software in Kali Linux	The open ports on the target were scanned using Nmap advanced scan.
11/27	Identify users with administrator privileges	Command Line Injection	To find out the users with administrators privileges, command line injection was used in the VulnsSripts (i.e., vulnerable website).
11/27	Launch session hijacking attack	Hamster	Successful attempts of hijacking session tokens and capturing cookies.
11/27	Detect any vulnerabilities in SQL Injection	Used "SQL Inject Me"	This tool tested many different combinations of inputs to identify the vulnerabilities for SQL Injection attack.

Additionally, by studying a history of interactive patterns within each team, we discovered that the red teams divided the tasks by expertise.

> *"We can divide our work into parts based on the strengths of the group members"*

> *"Two of our team members did not have any experience using Kali Linux or pen-testing so, I decided to assign them tasks like XSS and SQL injection which did not require any prior experiences"*

On the other hand, the blue teams delegated their works based on the given tasks and system components.

> *"And as a defend team, we knew that we need to protect all possible area that attacking team will attack. So, we assigned tasks for each team member…. Start with basic updates to security setting, then security programs, vulnerability scanners and fix any existing issues."*

> *"The initial project plan that we developed divided the tasks into four components that included the O/S, Apache Web Server, MySQL Database and Web Application Security…each of us worked on the assigned components."*

Principle 4: Contradictions

What contradicted the activity systems is a lack of knowledge for completing the tasks on hand. That is, insufficient knowledge contradicted the actions required (i.e., defending and attacking the systems) in the activity systems for the blue and red teams.

> *"One of our biggest challenges as a team in system protection is lack of knowledge. If we don't have the knowledge of how to find vulnerabilities or understand how to correct them, we cannot properly protect our server."*

> *"While some of the team members were familiar with a majority of the concepts, none of our team was familiar with PHP which made working with the PHP web server very difficult for us."*

> *"We had limited programming knowledge with web apps and therefore had to depend on firewalls and malware protection software."*

> *"Our group members had no knowledge about PHP and HTML and that hindered our progress on the project…"*

Principle 5: Expansive Cycles

We discovered that interactions between blue and red teams along with insufficient knowledge for completing tasks on hand propelled individuals to engage in learning. Specifically, they learned from the team that they competed with. The blue teams stated:

> *"Working against the offense team, we understand the tools attackers use by using Kali Linux, understand the types of attacks of which they are capable, and how those attacks are carried out…"*

> *"I have learned from an attacker's perspective, few of them include; how Trojans, worms, trap doors and viruses work."*

> *"Working in the apache files I learned how to change settings to help stop against system hijacking and cross site scripting (XSS). By turning these setting on it helped project the website from the offensive team."*

On the other hand, the red teams mentioned the following:

> *"As part of offense team, I had to learn what exactly the defense team does. Because you can attack on them only if you know what they have done and it would be impossible for me if I do not know the tasks of the defense team…."*

> *"As I am in the offensive team I learnt how to attack the defensive team with the various of tasks in the network. Identify the ways to exploit the vulnerabilities to defeat the security measure of the defensive system components."*

Summary of Data Analysis

Based on the data analysis, we draw a summary in the following table:

Table 3. Summary of Data Analysis

Principles	Findings	Suggestions/Implications
Principle 1: Activity system as unit of analysis	• Whereas that the key activities for the blue teams constant monitoring and configuration, the key activities for the red teams involved random attempts of attacking the target machine. • The blue teams used a communication tool that streamlined the search and access of data (e.g. messages). However, the red teams adopted a communication tool that handled tasks aside from exchanges between the team members.	• The blue teams solved problems by overseeing the entire system components, but the red teams randomly attacked a problem. • The blue teams tried to have a faster and easier access to messages exchanged between team members, so that the teams could be aware of the activities taken place
Principle 2: Multi-voicedness	• While both blue and red teams claimed that they were motivated by desire to learn and competitive spirit, the red teams were also motivated by fun.	• This suggests that there is a "hedonistic" element in cyber offense.
Principle 3: Historicity	• The blue teams started early on planning and system configuration, but the red teams tried multiple attempts and launched each attack in a short time. • The blue teams divided labor by system components, but the red teams divided labor by tasks.	• Cyber defense requires some careful planning but cyber offense moves from one tactic to the next. • Cyber defense conceives a system made of interconnected components, but cyber offense views a system made of independent entities.
Principle 4: Contradictions	• For both the blue and red teams, there was a lack of knowledge to complete the tasks on hand.	• A lack of knowledge urged the participants to acquire knowledge.
Principle 5: Expansive cycles	• Interactions between the blue and red teams along with insufficient knowledge for completing tasks on hand propelled individuals to engage in expansive learning, which involved their opponent's next move.	• Cyber offense and cyber defense learning fosters introspection in that individuals foresee the patterns of their opponent's activities.

Discussion

Based on Table 3 above, we elaborate our findings and provide the following rationales for our discoveries.

As noted, whereas that the key activities for the blue teams constant monitoring and configuration, the key activities for the red teams involved random attempts of attacking the target machine. Accordingly, our data revealed that one of the key differences between cyber offense and cyber defense is that cyber defense learning involves systems thinking but cyber offense learning incorporates effective thinking. Systems thinking (Senge, 1991; Checkland, 2005) requires individuals to identify the key system components and interrelations between the components (Assaraf & Orion, 2005). On the other hand, effective thinking "*is the result of conditionalized knowledge - knowledge that becomes associated with the conditions and constraints of its use*" (Glaser, 1984, pg. 99). Skills developed from effective learning are applied in a novel (i.e., non-entrenched or non-familiarized) situation (Sternberg, 1981). Because the blue teams defended the systems by constant monitoring (as shown in our data), they had to inspect multiple components, such as, services, processes, and network operating within the system. As a result, they had to understand the key components (e.g., running processes) in the systems and how these components relate to each other (e.g., interrelationship between services and processes). In contrast, the red teams could just launch any attacks that they saw fit. When running an attack, they formed an understanding of the target (e.g., system configuration etc.) and gradually customized their attacks to exploit their target. This suggests that, during cyber offense, individuals developed knowledge associated with their target machines (i.e., conditionalized knowledge) after harvesting information (i.e., reconnaissance) about their targets. Next, they used the information to launch an attack in a new environment (e.g., new system configuration resulted from system hardening) that they were not familiar with (i.e., novel situation).

Such a different learning mode explains why individuals in the blue teams searched for a solution when encountering a problem, but those in the red teams circumvented a problem by moving to a different attack tactic. Because the blue teams conceived that a system was made of interconnected components, they might think that a problem occurred in a component would propagate to the rest of the system. Therefore, finding a solution was crucial to maintain system integrity. On the other hand, the red teams conceived a system filled with rich information that they could use to their advantages. Hence, they were not so concerned to find a solution to a problem, because they could move to a different system component if the attempt on hand failed.

Moreover, different learning mode between the blue and red teams explains the differences in division of labor. As noted, the blue teams divided their tasks based system components, but the red teams divided their tasks based on expertise. Since the blue teams conceived that a system was comprised of multiple, interrelated system components, they delegated tasks based on components. Conversely, the red teams compartmentalized system components in which some components represented an entry point for cyberattack. Team members who had advanced knowledge in some of the system components (e.g., web application) were assigned specific tasks for exploiting those components.

We also discovered that the nature of cyber offense vs. cyber defense created a difference in learning motivation between the blue and red teams. Because cyber defense is tedious and complicated (Gartzke & Lindsay, 2015), individuals in the blue teams were not motivated by "fun" in comparison to their counterparts in the red teams. That is, some individuals in the red teams immersed into the fun of learning, motivating them to learn more (Csikszentmihalyi, 1990).

Additionally, based on the communication tools selected by the blue and red teams, we contend that there is a "subtle" difference between both teams in terms of team communication. Overall, we discover that the blue teams had a preference for a communication medium that streamlined the process of reporting team progress. For example, all the blue teams used Blackboard, but the red teams mainly used social media and email for tracking and updating team progress. Blackboard provided a platform where a team's shared documents could only be viewed by the team members. Therefore, it became easier to search through the Blackboard to realize the team activities that had taken place, and to effectively inform the team members of the team progress. This suggests that the blue teams were more concerned about action awareness – information about what has happened to the commonly shared objects (e.g., firewall) and who has modified the objects (Carroll, Neale, Isenhour, Rosson, & McCrickard, 2003), along with activity awareness – information about the task completions that shed light on group performance (Gross, Stary, & Totter, 2005; Kimmerle & Cress, 2008). Eventually, this further infers that cyber defense learning requires a higher action awareness and activity awareness to achieve its learning goals. One of the plausible explanations is that cyber defense is complex (Gartzke & Lindsay, 2015), thus requiring a more thorough coordinated efforts (Denning, 2014) supported by action and activity awareness.

Finally, insufficient knowledge in each team propelled team members to initiate changes (e.g. engaging in research and knowledge searching) that resulted in expansive learning. Expansive learning refers to:

> *"The object of expansive learning activity is the entire activity system in which the learners are engaged. Expansive learning activity produces culturally new patterns of activity. Expansive learning at work produces new forms of work activity."* (Engerström, 2001, pg. 139)

Referring to our analysis results, we assert that the learning of cyber offense and cyber defense cultivated introspection in that individuals foresaw new patterns of cyber offense/defense activities. Our data demonstrated that individuals involved in cyber offense tried to understand cyber defense. The opposite is true as well – those involved in cyber defense tried to gain a perspective of cyber offense. This suggests that the cyber offense/defense learning inadvertently put individuals in their opponents' shoes in order to predict their opponents' next move. Eventually, this promoted expansive learning wherein individuals developed new patterns of thought and activities (Engeström & Sannino, 2010) (e.g., defending a system from the cyber offense's perspective or attacking a system by understanding how cyber defense would thwart cyberattack).

Next, to summarize our findings, we present the following diagram based on the Third Generation AT (Engerström, 1999) (See Figure 4). As discussed earlier, the interactions between the blue and red teams generated expansive learning.

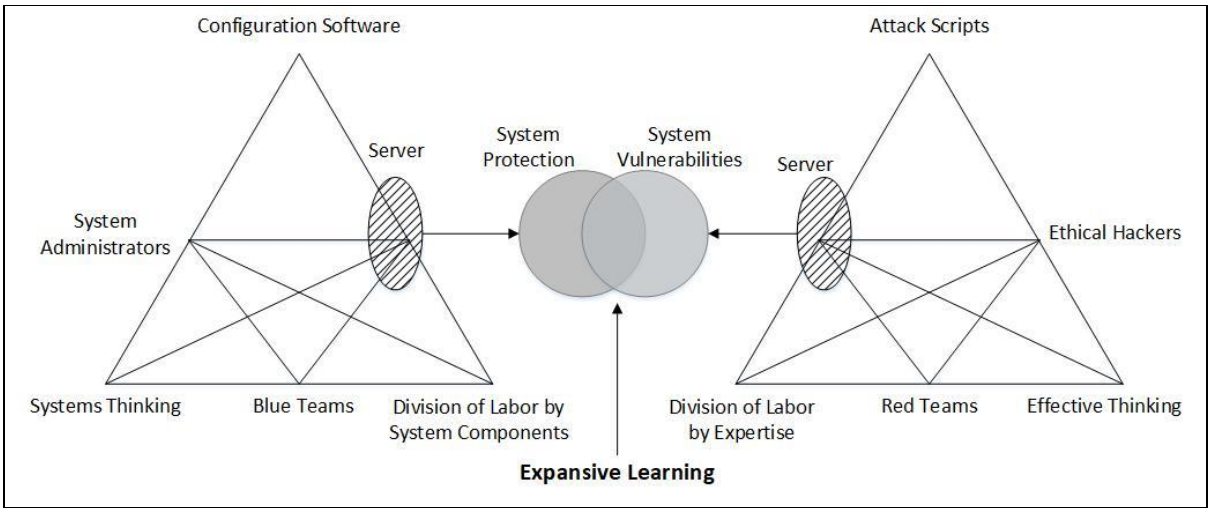

Figure 4. Research Findings

Research Implications, Limitations, and Future Research

This study contributes to the ISS research in the following ways. First, this study proposes the key differences between cyber defense learning and cyber offense learning to lay the foundation for the framework of cybersecurity education. Specifically, we posit that cyber defense learning engages individuals in systems thinking but cyber offense learning cultivates effective thinking. Furthermore, we suggest that cyber offense learning embodies hedonistic effect in which individuals may experience fun in ethical hacking. The hedonistic factor motivates individuals in cyber offense learning, drawing a contrast to cyber defense learning. This further suggests that there are two different streams of cybersecurity learning: seriousness in cyber defense vs. fun in cyber offense. We posit such differences can complement each other to improve the quality of cybersecurity education. This brings about the second contribution. That is, based upon our research findings, we suggest that universities and colleges can improve the quality of cybersecurity education by designing lessons that incorporate both cyber defense and cyber offense. For example, to teach cyber defense, instructors can first introduce the complexities involved, including system configuration, system auditing via event logs, and validating scripts and software implemented in a system. Meanwhile, instructors can introduce the hackers' perspectives in terms of system exploitation, so that individuals will realize how to patch system vulnerabilities. To engage students in cyber defense, instructors can give hands-on exercises of ethical hacking and then present how to harden a system, so that students can experience some "fun" in ethical hacking. In a learning process that involves convoluted studies of cyber defense, the hedonistic factor (i.e., fun) is meant to reward students for encouraging them to engage in learning.

Finally, this study is not without limitations. We used graduate students rather than information security professionals. Hence, our results may be limited to student learning. However, we argue that using students serves the purpose of this study that examines cybersecurity learning and suggests how to improve the quality of cybersecurity education. Additionally, due to the budget constraints, we cannot deploy a cyber-range that facilitates centralized logging for better data analysis. In the near future, we will look for more research fund and continue to analyze data to derive meaningful findings.

References

Assaraf, O. B.-Z., & Orion, N. (2005). Development of System Thinking Skills in the Context of Earth System Education. *Journal of Research in Science Teaching*, 42(5), 518–560. https://doi.org/10.1002/tea.20061

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Carroll, J. M., Neale, D. C., Isenhour, P. L., Rosson, M. B., & McCrickard, D. S. (2003). Notification and Awareness: Synchronizing Task-Oriented Collaborative Activity. *International Journal of Human-Computer Studies*, 58(5), 605–632. https://doi.org/10.1016/S1071-5819(03)00024-7

Checkland, P. (1999). Systems Thinking. In W. Currie & B. Galliers (Eds.), *Rethinking Management Information Systems: An Interdisciplinary Perspective*. New York: Oxford University Press, Inc.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. J. (2013). Data Model Development for Fire Related Extreme Events: An Activity Theory Approach. *MIS Quarterly*, 37(1), 125–147. https://doi.org/10.25300/MISQ/2013/37.1.06

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-Engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *System Sciences (HICSS), 2014 47th Hawaii International Conference* on (pp. 2006–2014). IEEE.

Cooper, D., & Schindler, P. (2000). *Business Research Methods* (7th ed.). New York, NY: McGraw-Hill.

Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS). Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience*. New York: Harper & Row.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dark, M., & Mirkovic, J. (2015). Evaluation Theory and Practice Applied to Cybersecurity Education. *IEEE Security Privacy*, 13(2), 75–80. https://doi.org/10.1109/MSP.2015.27

Denning, D. E. (2014). Framework and Principles for Active Cyber Defense. *Computers & Security*, 40, 108–113. https://doi.org/10.1016/j.cose.2013.11.004

Engeström, Y. (1999). Innovative learning in Work Teams: Analyzing Cycles of Knowledge Creation in Practice. In Y. Engeström, R. Miettinen, & R.-L. Punamäki (Eds.), *Perspectives on Activity Theory* (pp. 377–406). Cambridge. MA: Cambridge University Press.

Engeström, Y. (1990). Learning, Working and Imagining: Twelve Studies in Activity Theory. Helsinki: Orienta-Konsultit Oy.

Engeström, Y. (2001). Expansive Learning at Work: Toward an Activity Theoretical Reconceptualization. *Journal of Education and Work*, 14(1), 133–156. https://doi.org/10.1080/13639080020028747

Engeström, Y., & Sannino, A. (2010). Studies of Expansive Learning: Foundations, Findings and Future Challenges. *Educational Research Review*, 5(1), 1–24. https://doi.org/10.1016/j.edurev.2009.12.002

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 24(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188

Glaser, R. (1984). Education and Thinking: The Role of Knowledge. *American Psychologist*, 39(2), 93-104. https://doi.org/10.1037/0003-066X.39.2.93

Gross, T., Stary, C., & Totter, A. (2005). User-Centered Awareness in Computer-Supported Cooperative Work-Systems: Structured Embedding of Findings from Social Sciences. International *Journal of Human–Computer Interaction*, 18(3), 323–360. https://doi.org/10.1207/s15327590ijhc1803_5

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Kaptelinin, V., & Nardi, B. A. (2006). *Acting with Technology: Activity Theory and Interaction Design*. Cambridge. MA: The MIT Press.

Kimmerle, J., & Cress, U. (2008). Group Awareness and Self-Presentation in Computer-Supported Information Exchange. *International Journal of Computer-Supported Collaborative Learning*, 3(1), 85-97. https://doi.org/10.1007/s11412-007-9027-z

Maasik, S., & Solomon, J. (2012). *Sign of Life in the USA: Readings on Popular Culture for Writers* (7th Ed.). Boston, MA: Bedford/St. Martin's.

Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 42(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, 21(2), 241–242. https://doi.org/10.2307/249422

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring Game Design for Cybersecurity Training. In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2012 IEEE International Conference on (pp. 256–262). IEEE.

NIST (2017). *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. The Secretary of Commerce and the Secretary of Homeland Security. Retrieved from https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

NIST Special Publication 800-181. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology (NIST). Retrieved from https://doi.org/10.6028/NIST.SP.800-181

Pastor, V., Díaz, G., & Castro, M. (2010). State-of-the-Art Simulation Systems for Information Security Education, Training and Awareness. In *2010 IEEE Education Engineering (EDUCON) Conference* (pp. 1907–1916). IEEE.

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security Privacy*, 11(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Senge, P. M. (1991). The Fifth Discipline, the Art and Practice of the Learning Organization. *Performance + Instruction*, 30(5), 37–37. https://doi.org/10.1002/pfi.4170300510

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487–502. https://doi.org/10.2307/25750688

Sternberg, R. J. (1981). Intelligence and Nonentrenchment. Journal *of Educational Psychology*, 73(1), 1-16. https://doi.org/10.1037/0022-0663.73.1.1

Valecha, R., Rao, R., Upadhyaya, S., & Sharman, R. (2019). An Activity Theory Approach to Modeling Dispatch-Mediated Emergency Response. *Journal of the Association for Information Systems*, 20(1). https://doi.org/10.17705/1jais.00528

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems*, 92, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Weber, R. P. (1990). *Basic Content Analysis*. Beverly Hills, CA: SAGE.