PREPRINT

Publisher IEEE: https://doi.org/10.1109/RWEEK.2017.8088665

Using a critical infrastructure game to provide realistic observation of the human in the loop by criminal justice students

Resilience Week

A. Rege and E. Parker
Temple University
T.R. McJunkin
Idaho National Laboratory

2017

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Using a Critical Infrastructure Game to Provide Realistic Observation of the Human in the Loop by Criminal Justice Students

Aunshul Rege, Edward Parker
Dept of Criminal Justice
Temple University
Philadelphia, PA
rege@temple.edu

Timothy McJunkin
Power and Energy Systems Department
Idaho National Laboratory
Idaho Falls, Idaho 83415
Timothy.McJunkin@inl.gov

***Abstract*—Understanding human behavior is crucial in anticipating adversarial actions during cyberattacks. The Criminal Justice (CJ) discipline offers the necessary frameworks to unpack the complex facets of adversarial behavior and movement, and should therefore be leveraged for their possible contributions to the area of proactive cybersecurity. Yet the discipline remains weak at training current and future CJ workforce on these matters in a hands-on manner. This paper presents a cybersecurity training exercise where a power grid simulator is used to educate CJ students via *experiential learning* about concepts of cyberattacks and cybersecurity as well as exposing them to doing hands-on cybersecurity field research. The paper reports on Game use as an important opportunity to observe humans put under additional stress in operating conditions. The paper discusses what CJ students learn from multidisciplinary simulation-based exercises, the challenges and limitations they face, and how training this workforce could help contribute towards proactive cyberdefense of critical infrastructure.**

Keywords—experiential learning; multidisciplinary education; hands-on simulation training; cybersecurity-field research; critical infrastructure; human in the loop observations

I. Introduction

The current state of cybersecurity is reactive, which has limited efficacy as it does not capture adapting adversaries and attack vectors. Furthermore, this response-drive approach is costly as the damage has already occurred and cleanup efforts are taxing with regards to time and manpower. Many security experts are calling for proactive defense measures, which require an understanding of the human behavior and movement. Social science disciplines, such as sociology, criminology/criminal justice, and psychology are particularly adept at unpacking the complex facets of human behavior and should therefore be leveraged for their possible contributions to the area of proactive cybersecurity [1-4]. While the social science arena has done considerable cybercrime research, it remains weak in cybersecurity training and education of the future social science workforce [5]. A qualitative, social science learning focus is crucial to understand both adversarial and defender behaviors. Thus, a trained social science workforce would understand how adversaries think, move laterally inside targeted systems, and adapt to any disruptions, which would offer a complementary approach to existing technical proactive cybersecurity measures. This paper presents one such *exploratory* effort to address this workforce training gap by using a power grid simulator to educate Criminal Justice (CJ) students via *experiential learning* about concepts of cyberattacks and cybersecurity as well as exposing them to doing hands-on cybersecurity research.

This paper is structured as follows. The next section details experiential learning theory as well as the five stages of the experiential learning process. The third section details the logistics and structure of the joint multidisciplinary cybersecurity course exercise between the CJ and Electrical and Computer Engineering (ECE) students. The fourth section discusses each of the five experiential learning stages through the qualitative reflections of CJ students in three areas: research, cyberattacks, and cybersecurity. The next section shares some findings from a post-exercise evaluation survey of CJ students who took part in the joint exercise. The sixth section discusses some challenges and limitations, and how these can be effectively managed. The paper concludes by offering directions for future research and the relevance for training a social science workforce to benefit critical infrastructure protection against cyberattacks.

II. Experiential Learning

Experiential Learning Theory (ELT) describes a process by which knowledge is acquired through praxis, by doing, reflecting and trying again with improved methods [6]. Thus, the learner's *subjective* experience is at the heart of the experiential learning process. ELT can be described using the following 6 principles [7-8]:

1. ELT is a process, which moves away from memorization. Students must take the initiative in guided experiences and receive feedback based on the event.

2. ELT draws out students' beliefs, ideas, and prejudices, after which students engage in critical reflection and synthesis. The student is thus involved in a cyclic and dynamic learning process in which they are a source of creativity and conflict.

3. This process is driven by conflict and disagreement, and it is critical to move between these opposing modes of reflection

and action. This allows students to learn from each other and grow from each conflict.

4. The process involves perceiving, thinking, feeling and behaving. It adds the emotional and social learning aspects often missing from most intellectual exercises, and offers a more authentic experience.

5. ELT elicits learning from dynamic transactions between students and their environments. The students' experience cannot be predicted, it is unknown whether they will achieve success or failure.

6. ELT's goal is to create knowledge that originates within the learner, as opposed to simply transmitting a fixed idea from one generation to the next. Thus, results are personal and form the foundation for further iterations of experiential learning.

Experiential learning, as displayed in Fig. 1, can be broken down into 5 steps [6]:

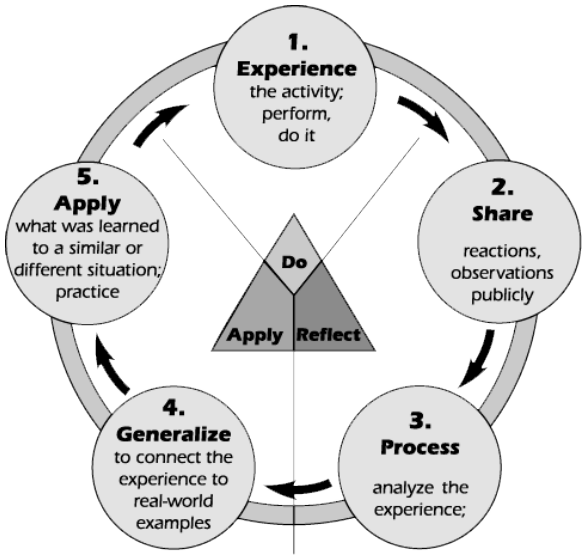

Fig. 1: Experiential Learning Model [4]

1. Experience: In this first step, students are engaged in hands on exercises, or activities.

2. Sharing: During this step, the students share their observations, reactions, and results with one another.

3. Critical Analysis/ Processing: This is where problems are discussed and worked through with others, which contributes to the synthesis of new ideas.

4. Generalization: Student take what they have learned and connect/compare it to real world examples.

5. Application: The students conceptualize what they have learned thus far and use it to make changes in the next iteration of the process or future events.

III. Cyber-Security Exercise Case Study

This paper uses a case study of a joint cybersecurity course project between the Electrical and Computer Engineering (ECE) and Criminal Justice (CJ) departments. Specifically, this paper focuses on the experiences of Criminal Justice students enrolled in an upper-level, Computer Crime course in Spring 2016. The class had 18 students, 15 of which were criminal justice majors, and the other three were Information Science and Technology; Media Studies major; and Environmental Engineering. With regards to student status, 50% of the class were Juniors, 16.7% were Seniors, 22.2% were Sophomores, and 11.1% were Freshman.

The GridGame is a simulation of a microgrid control system base on the swing equation [10], which is the differential equation describing the dynamics of the frequency due to power imbalance and the rotating inertia of the prime movers generating electricity [11-12]. The game is driven with a year of load and generation data from Idaho Falls Power played back at a rapid rate to make the game more exciting for short periods of game play. Players are provided an energy storage asset that they control manually or with a proportional-integral-differential feedback controller for which they adjust the gains. The overall goal is to sell as much energy to your customers as possible thus accumulating more points than the player's competitors. The players interact with the game through a user interface designed to show current state of the grid system and provide input mechanism to execute their decisions. The game provides a rich set of possible decisions in both tactical and strategic time frames, including demand response and energy contracts with fellow competitors. Players are also given the opportunity to proactively and reactively purchase security measures. As with any digital control system, there is a possibility of cybersecurity attack. The game is designed to allow game masters to attack the players with a list of attacks with increasing severity from small financial harm to a "zero day" catastrophic impairment of the automatic control system. To view the more details of the game or to download and play the game, the reader is referred to the website: http://gridgame.ironforidaho.net.

Typical "official" game sessions are held over a thirty-minute time period divided into two fifteen-minute halves. In the first half the players are make decisions about investments in microgrid assets, customer recruitment and cybersecurity measures. In the second half, the Red Team launches a sequence of attacks, which may include messages (e.g. "resistance is futile", "Sorry!—Not Sorry!", etc.). In past events, players have reported emotional responses as they attempt to keep the system up and running and wondering if their cybersecurity protection is going to hold. The game environment with provides sufficient realism for control of a microgrid by driving it with historical data from Idaho Falls Power and simulating the electromechanical nature of the grid with the swing equation. Players are able to experience many of the conditions that an operation team might experience with respect to human performance in a critical infrastructure control system environment. As such, the game provided an interesting platform for both ECE and CJ students to interact with each other.

The ECE students downloaded the GridGame software on their laptops from the game website, and played the role of electric utility administrators responsible for managing consumer loads, generating revenue, and deflecting malicious cyberattacks that tried to bring their grids down. There were 6 ECE teams with 2-3 members each.

CJ students were provided with details about the various attacks, their costs (loss of revenue/ points), and what parts of the grid they targeted, as summarized in Table I. CJ students then worked in groups to create (and justify) attack sequences that could be launched against ECE students. The group sequences were then vetted in class and two attack sequences were chosen for two rounds during the joint exercise. CJ students also had the flexibility of launching certain attacks against certain ECE teams. The final attack sequences are shown in Table II.

TABLE I: Attack Type Summary

Name	*Type*	*Remedy Available*
Little Guy	Small persistent financial	Proactive low cost
Big Guy Virus	Large persistent financial	Proactive medium cost
Denial of Service	Communication disruption	Proactive low cost
Gluxnet	Control system gain setting disruption	Proactive high cost
Blue Frog	Automatic control system disruption, Zero Day	Reactive Only – requires manual control skillset to survive

TABLE II: Attack Sequences Designed by CJ students

Round 1		
Time	*Attack Type*	*ECE Teams*
2:25pm	Denial of Service	All Teams
2:28pm	Gluxnet	Teams 1,2,3
2:28pm	Little Guy	Teams 4,5, 6
2:33pm	Blue Frog	All Teams
2:38pm	Big Guy Virus	All Teams
Round 2		
Time	*Attack*	*ECE Teams*
3:00pm	Gluxnet	All Teams
3:03pm	Denial of Service	Teams 2,4,6
3:05pm	Big Guy Virus	Teams 1,3,5
3:09pm	Denial of Service	Teams 1,3,5
3:10pm	Gluxnet	Teams 2,4, 6
3:12pm	Blue Frog	Team 3
3:15pm	Blue Frog	Teams 1,2,4,5,6
3:19pm	Blue Frog	Team 3

ECE students were not told about the attack sequences. The exercise was held over the course of 1.5 hours playing two rounds with fifteen minutes without cybersecurity attacks followed by fifteen minutes using the attack schedule in Table II. Thus, CJ students got a chance to 'play red' and, more importantly, *think offense*. CJ students (red team) had to think carefully about how to sequence each attack, why that sequence was effective, and which ECE (blue) teams they wanted to target.

CJ students then designed data collection instruments for the joint exercise. They reviewed existing cybercrime and cybersecurity literature, the grid game user manual, and publications on conducting field research, to generate observation guides and interview guides. CJ students then discussed the guides in the context of the attack sequences they had created, which allowed them to be more effective with regards to interviewing and observing ECE students as they would know exactly when attacks were expected to see how their teams performed. The CJ students engaged in this data collection process before, during, and after the joint exercise. Audio recordings of the interview were collected. Temple University's Internal Review Board approved this class project. All students were informed of the study's purpose and signed the informed consent forms.

After the exercise, CJ students were surveyed about their experiences with the grid game's structure and form. In addition to surveyed experiences, two CJ students' (referred to as CJ1 and CJ2) personal learning experiences are shared in this paper with regards to both developing their research skills as well as understanding cyberattacks and cybersecurity.

IV. Experiential Learning for Criminal Justice Students

CJ students were asked to write qualitative reports detailing their reflections and perspectives on each of the experiential learning stages in three areas: research, cyberattacks, and cybersecurity. Summaries of their experiences are discussed next along with specific comments from CJ1 and CJ2.

A. Stage 1: Experience, Exploration, Doing

Research: CJ students were actively involved in designing and implementing stages of research. They designed interview and observation guides and engaged in 'field research' by observing and speaking with the ECE students, which allowed the CJ students to "learn essential skills of how to interview individuals with a variety of backgrounds, how to use prompts and probes during the actual interview, and how to manage interview contexts" [8].

CJ students had to 'think on their feet' as the exercise progressed. CJ students found that the interview and observation guides complemented and supplemented each other. Based on their observations, CJ students would ask new questions (not listed in the interview guides that they had generated) to the ECE students. Thus, CJ students had to change and adapt their observation and interview techniques at various points during the exercise.

Allowing students to collect primary data made it much more interesting for them, in contrast to "students who … are relegated to the rather mundane task of interview transcriptions" [13]. CJ1 explains that he had never done any

hands-on research prior to this exercise, and this allowed him to understand and appreciate the research process more. CJ2 was also a first-time field observer and had never conducted hands-on research previously. CJ2 noted that keeping up with the recording in real-time as the exercise was progressing was "complicated, and nerve-racking".

Cyberattacks: CJ students had to work in groups to generate their own attack schedules. They had to justify the attack sequence stating why they picked certain types of attacks at certain times. Each group had a different objective. For instance, CJ2's group justified its attack sequence as follows: "This attack is designed to punish teams who do not have total familiarity and expertise in controlling their grid. As the options are to wipe the system or manually control the [grid], groups that have not sufficiently practiced will likely be dealt a lethal or near lethal blow". Thus, they had to think offense and as CJ1 noted: "playing the attackers was fun because we knew what was coming".

Cybersecurity: CJ students had the chance to understand how cybersecurity functioned as a group event when they studied ECE students. They learned about possible group dynamics, divisions of labor, decision-making, conflict resolution [13]. CJ2's ECE team had two members with one serving as the grid operator (physically controlled the grid game) while the other had an advisory role (guidance on buying, storing, and cybersecurity purchases). CJ1's ECE group had three members, with one serving in operator capacity and all members contributed equally to the decision-making process and what actions to complete. Each ECE group exhibited strong cohesion between its members and generally agreed on the how to progress during the joint exercise. Thus the CJ students had the opportunity to experience grid operations and cybersecurity planning as executed by a group of ECE students.

B. Stage 2: Sharing, Reflecting

Research: In this stage, students "share and analyze what is important…students can discuss what they thought of the research experience itself: how did they feel doing the research? Students can share their respective experiences and learn from each other." [13]. During the post-exercise debriefing CJ students commented about the shared challenges they experienced, such as (i) realizing that they all had to generate questions on the fly for the teams they observed, (ii) speaking with students from different (ECE) disciplines, and (iii) collecting data under spatio-temporal constraints (the exercise was conducted over 1.5 hours in a small room). Students also shared positive experiences. For instance, the predetermined attack schedule allowed the CJ students to be effective observers as they knew exactly when to observe reactions from their respective ECE teams. As CJ2 noted, "We consistently asked awareness gauging questions in accordance to the attack schedule to gain insight on how they were measuring up to our anticipated results". CJ1 echoed this point: "knowing what was going to happen … allowed us to focus more on certain aspects of the game."

CJ students could also ask specific questions tailored to the timed attack sequence to get the most informative data for analysis. CJ2's experiences serve as a case in point. He explains that the "interview questions were prompted by what we observed the participants doing. For example, once the participants started talking to each other about what antivirus software they would use, we would proceed to ask them about their choice and their plan for the rest of the game."

Cyberattacks: After each CJ group created their attack schedules, it had to defend its schedule against those prepared by other groups. This sharing and reflecting activity took place in class prior to the joint exercise as CJ students had to agree on two finalized attack schedules. Here, students reflected about the pros and cons of attack vectors and the relevance of timing these vectors effectively. By engaging in a debate and voting for the best attack sequence, students were able to also tie this in to the CJ class learning material on attack vectors, attacker motivations, and case studies.

Cybersecurity: During the post-exercise debriefing, CJ students shared their thoughts on how their respective ECE students fared in the area of cybersecurity. As CJ2 noted: "We witnessed ECE students get attacked and how they reacted". When CJ1 asked his ECE team whether it had any preemptive steps to defend against attacks, one member stated: "Good question, I did not think about that. We will probably buy it later, but I am not really sure about this." CJ2 shared a similar experience, when his ECE team "at this moment we don't need any [security measures]… These are investments … so we want to make sure we are buying what we can afford". CJ students realized that their teams were nonchalant and reactive about cybersecurity, and even engaged in a cost-benefit analysis with regards to security purchases.

C. Stage 3: Critical Analysis

Research: This stage included CJ students discussing what challenges they faced while "interviewing and observing, and how they managed these." [13]. Regarding the first research challenge of generating questions as the exercise unfolded, CJ students used their observations to guide when and how to best ask ECE students questions. For the second research challenge of multidisciplinary communication, CJ student chose informal, conversational communication mechanisms over the formal interview style developed in class prior to the exercise. This helped increase the comfort levels of both CJ and ECE students and made data collection easier. With the last challenge of space and time constraints, CJ students spread themselves (and their recording devices) out across the ECE students to better collect audio interview data and get stronger observations.

Cyberattacks: CJ students realized that even though they had voted on the best two attack schedules (Table II) for the exercise, these were still *static* (predetermined) in nature. CJ students could not change the sequence during the live exercise. Furthermore, even though the CJ students had timed the attack schedules for specific intervals, these were launched with a 1-2 minute delay due to logistics and setup issues and

time constraints. CJ students realized that both these issues could be encountered by cyberattackers in reality: they may not always be able to change their attack vectors and timings, and executing attacks may not always run smoothly.

Cybersecurity: CJ students realized that even though the ECE students had an opportunity to learn in the first round, players only minimally focused on cybersecurity in the second round. CJ2 commented on the reactionary nature of cybersecurity: "I gathered that the defense aspect really is just like playing whack-a-mole with the attacks". Similarly, CJ1 noted that the "thought process that goes into defending against an attack, [involves] a lot of second guessing". At several points during both attack sequences, the CJ students noted that their ECE groups did not even realize that it was under attack.

D. Stage 4: Generalization

Research: CJ students were directed to connect their research experience with real world research. They were able to understand the various components of the research process: designing and refining data collection instruments, doing field research; understanding and appreciating the research environment; respecting research subjects; managing unanticipated events and hurdles; data coding; data analysis; and formal report writings to disseminate findings.

Cyberattacks: The joint exercise gave CJ students a hands-on, tangible example of a cyberattack processes and implications. As CJ2 commented: "we got [a glimpse of] everyday [cyberattack] encounters our power grids face". CJ students also learned about the complexities of cyberattacks, the many possible permutations and combinations of attack vectors, and how "thinking offense" was critical to be effective at "thinking defense"; how could attack schedules be used to understand *proactive* cybersecurity.

Cybersecurity: CJ students compared the ECE students' reactive approach to cybersecurity to the class topics on the current response-driven state of cybersecurity in reality. They drew parallels in the lack of cybersecurity knowledge, the trade-off between generating revenue and spending on cybersecurity, and confusion over which cybersecurity measures were effective.

E. Stage 5: Application

Research: Finally, CJ students were challenged to apply the knowledge they obtained from designing data collection instruments, primary data collection, and analysis to other cybersecurity exercises, and even other field research in the CJ discipline. CJ students thus became more seasoned researchers as they could "apply what they … learned in both the research and cybersecurity contexts to future … situations." [13].

Cyberattacks: CJ students could apply what they learnt about 'playing red' in this joint exercise to future iterations of similar exercises. While they may not possess the technical know-how of how to engage in ethical hacking, they did develop the ability to conceptualize, plan/schedule, and justify attack trajectories. As CJ1 and CJ2 noted, they developed an "appreciation of the complex nature of cyberattacks and the challenges of real time defense", which they would not have received through traditional Criminal Justice assignments. For those CJ students who pursue the area of cyberdefense as a career, this exercise gave non-technical students a chance to experience real-time attacker-defense interaction.

Cybersecurity: This joint exercise provided the CJ students with several benefits, such as understanding real-time cyberdefense; assessing group behavior, dynamics, and decision-making with regards to grid operations and security; and the ability to work with multiple disciplines, which is crucial at gaining a holistic understanding of cyberattacks and cybersecurity.

V. EVALUATION

To evaluate the effectiveness of this exercise for CJ students, two main components were used. First, students had to write a reflection report at the end of the exercise where they reflected heavily on each of the experiential learning stages. These responses served as qualitative evaluations and were listed in section IV.

Second, a post-exercise survey was implemented as this evaluation technique has been used for other simulated educational games [14-16]. Each of the relevant survey components are discussed next.

A. Project Effort

CJ students were asked to rate the amount of effort they put into the project on a Likert scale from 1 (least effort) to 100 (most effort). On average, CJ students reported the overall effort at 60%. This is relevant because in order to foster the desire to continue the process, a specific amount of difficulty must be maintained. If the process is too easy, they will become bored and lost interest. If the process is too difficult they may give up mid cycle or choose to disengage after the current iteration.

B. Working as a Research Group

CJ students worked in groups to observe ECE students. They were asked how they felt about the group size that they were a part of. 83.3% of students said that the teams were of an appropriate size. CJ1 states "I was in a group of four, including myself, and it seemed to work out pretty well. We all did a good amount of work but did not seem to be overworked, and having four people observing allowed us to observe more [and validate our observations]." Some students found that the groups allowed for an unequal division of labor; it is unknown, however, whether this was tied more to group dynamics or group size.

C. Recommendations for Subsequent Iterations

CJ students were asked what they would change in future iterations of the joint exercise. One of the leading answers was "nothing." The most interesting answer was suggesting that the ECE students become more familiar with the grid game before the CJ students engaged in data collection. Furthermore, one or two students commented on better logistics issues, stating that

they would make efforts to limit noise pollution in future data collections.

D. Understanding Cyberattacks, Cybersecurity, and Cybercriminals

CJ students were asked to rate how well the exercise helped them to understand cyberattacks, cybersecurity, and cybercriminals. A majority of the CJ students rated the knowledge gained in the area of cyberattacks at 66.7%. Roughly half of the CJ students ranked their understanding of cybersecurity at 75%. Knowledge about cybercriminals was ranked at 66%. While it is difficult to assess 'how much and how well' CJ students learned about these topic areas, the survey results provided some insight.

VI. CHALLENGES AND LIMITATIONS

While the joint exercise offered CJ students several benefits, they also experienced some challenges, which are common for any qualitative, field research irrespective of the domain being studied:

A. Multidisciplinary Communication

CJ students had to communicate effectively with ECE students. During the post-exercise debriefing, several CJ students were dissatisfied with their inability to "break the ice" with ECE students and found themselves limited by their understanding of engineering principles.

One means of minimizing these issues is to have a 'meet and greet' the week before the joint exercise to explain what CJ students would be doing. This would make both CJ and ECE students familiar and comfortable with each other. To address the issue of limited knowledge of ECE principles, CJ students could be exposed to the Grid Game software before and even engage in a hands-on practice session prior to the joint exercise to better understand ECE students' actions.

B. Communication During Cyberattacks

CJ2 commented on the difficulties he encountered communicating with his ECE team when it experienced cyberattacks: "… in both round[s], ECE students [were frustrated]. If they became frustrated at any moment they would stop talking about what was happening as well as almost become apathetic on the game itself and give up."

While experiencing cyberattacks, it is not surprising that ECE students would be reclusive and unwilling to talk. Some CJ students managed this lack of communication by focusing heavily on observations rather than interviews to get a read on what ECE students might be experiencing. By focusing on body language, facial expressions, and how they moved around in the grid game interface, CJ students were still able to get some insight on how ECE students performed when their grids were subjected to cyberattacks.

C. Game Logistics

CJ students also experienced difficulty with the spatial logistics. As CJ1 noted, "something that would help with observations [and interviews] would be separating the tables more; the tables are very close and it makes it difficult to talk with one another."

One obvious fix would be to hold future joint exercises in larger rooms to space out ECE players and the CJ research teams. Nevertheless, CJ students found creative means to observe and interview ECE students. CJ students positioned themselves next to ECE students so as to get as close to 1:1 ratio. This allowed each student in the CJ team could observe 1-2 ECE students, which allowed for effective data collection. Furthermore, each CJ student could then compare his/her notes with the team for validation and fill in any missing observation and interview data.

D. Methodological Hurdles

Another limitation noted by CJ1 dealt with equipment used for recording: "it would be nice if we had great recording equipment, not just our phones. That way we would be able to pick up on everything." Among the other students, there was also a repeated response about the difficulties recording data without picking up the noise of other ECE and CJ groups.

One means to manage this limitation would be to have each CJ-ECE team in a separate 'breakout' room. Not only would this limit any 'outside' noise picked up by recording devices, but this would also ensure that each CJ-ECE team is not impacted by other CJ-ECE teams' actions and conversations. This team separation would improve any issues of bias and/or influence during data collection.

E. Group Work

Other struggles noted by some CJ students were inherent to group work; they faced disorganization within their groups and some reported a dislike of the "group work distribution." This discontent towards group activity is not new.

CJ students could manage this hurdle by agreeing roles and divisions of labor of data collection and analysis prior to the joint exercise. Furthermore, the biggest benefit to group activity is the data validation; CJ students can increase the confidence in their collection and analysis when they cross-check their datasets with their teammates for accuracy and coherent analysis. An additional benefit is the ability to minimize 'missing data'. In a fast-paced exercise, it is likely that CJ students (who are also novice researchers) may miss out on certain observations or not ask certain questions. Having a team improves the chances that any data missed by one teammate may have been captured by other team members.

VII. CONCLUSSIONS AND FUTURE DIRECTIONS

The joint exercise case study detailed in this paper is highly significant in expanding the cybersecurity education of *non-technical* students in the area of critical infrastructure protection. To summarize the main benefits for CJ students, they: (i) get a small-scale introduction to real-time cyberattack and cyberdefense through a controlled simulated classroom exercise, (ii) move beyond traditional class assignments based on secondary data collection and analysis to doing hands-on research and engage in primary data collection, (iii) partake in multidisciplinary research where they must dialog with ECE

students, (iv) no longer limited by their non-technical backgrounds to be able to "think offense" effectively, and (v) understand and appreciate the complexities and back-and-forth aspects of cyberattacks and cyberdefense.

As with any educational exercise, there are lessons learned and recommendations made for future iterations:

1. Introduce variations in the exercise by changing the duration of the overall exercise and attack sequences, altering the attack schedules, switching ECE group members to see effects of group dynamics, decision-making, strategy and planning, and approach to cybersecurity.

2. Engage in multidisciplinary dialog *after* the joint exercise. Once CJ students are done with their analysis and reports, they can meet with their respective ECE teams to share their findings. This serves as a means to not only 'close the loop', but also validates the CJ students' findings.

3. Analyzing the technical logs from the exercise to get metrics on ECE student performance and reactions to the cyberattacks. This data could then be married to the CJ students' qualitative interview and observation data to get a more holistic understanding of ECE students' performance.

While this paper makes the case that this joint cybersecurity exercise served the CJ community, it should be noted that training a future CJ workforce in the area of cybersecurity would ultimately benefit the area of critical infrastructure protection. First, this group could be involved in the design of an assortment of table-top exercises geared to the training of ECEs or grid operators; the CJ personnel could gauge ECEs ability to manage grid operations in general and during cyberattacks. Second, CJ personnel could engage in qualitative research methods of observations, interviews, and focus groups during these exercises as well as post-exercise debriefings to understand ECE and grid operators' concerns about cyberattacks and cybersecurity. Finally, CJ personnel could combine their analysis of ECE performance and knowledge to develop, implement, and evaluate effective education programs for the ECE workforce. Having a multidisciplinary workforce would thus offer a more holistic approach to the area of critical infrastructure cybersecurity.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 1453040 and Grant No. 1446574.

Timothy McJunkin thanks Idaho National Laboratory and the Center of Advanced Energy Study for supporting educational outreach efforts with the GridGame and to Idaho Regional Optical Networks for providing the server for the game

REFERENCES

[1] M. Branlat, A.M.Morison, G.J. Finco, D.I. Gertman, K. Le Blanc, and D.D. Woods, "A study of adversarial interplay in a cybersecurity event," in *10th International Conference on Naturalistic Decision Making*, 2011

[2] M. Branlat, A. Morison, and D.D. Woods, "Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cybersecurity exercise," in *Human Systems Integration Symposium*, 2011, 10-25.

[3] R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours, and S. Chon, "An Analysis of the Nature of Groups Engaged in Cyber Crime. An Analysis of the Nature of Groups engaged in Cyber Crime," *International Journal of Cyber Criminology*, 8(1), 2014, 1-20.

[4] B. Leclerc, "Crime Scripts," in *Environmental criminology and crime analysis,* Routledge, 2016

[5] B. Payne, "Cybersecurity in the Criminal Justice Curriculum", paper presented at the 2016 American Society of Criminology Conference, New Orleans, LA, 2016.

[6] NIU.edu (N.D.)."Experiential Learning." Retrieved April 10, 2015 Online at http://www.miu.edu/facdev/resources/guide/strategies/experential_learning.pdf

[7] Association for Experiential Education http://www.aee.org/

[8] A. Y. Kolb and D. A. Kolb, "Learning styles and learning spaces: Enhancing experiential learning in higher education," *Academy of management learning and education*, 4(2), 2005, 193-212.

[9] D. A. Kolb,. "Experiential learning: Experience as the source of learning and development," New Jersey: Prentice-Hall, 1984

[10] J. Grainger and W. D. Stevenson, *Power System Analysis*. McGra-Hill, 1994.

[11] T. R. McJunkin, C. G. Rieger, B. K. Johnson, D. S. N. P.E, L. H. Beaty, J. F. Gardner, I. Ray, K. L. L. Blanc, and M. Guryan, "Interdisciplinary Education through Edu-tainment: Electric Grid Resilient Control Systems Course," in *2015 ASEE Annual Conference & Exposition*. Seattle, Washington: ASEE Conferences, Jun. 2015, https://peer.asee.org/24349.

[12] T. R. McJunkin, C. G. Rieger, A. Rege, S. K. Biswas, M. Haney, M. J. Santora, B. K. Johnson, R. L. Boring, D. S. N. P.E, and J. F. Gardner, "Multidisciplinary Game- based Approach for Generating Student Enthusiasm for Ad- dressing Critical Infrastructure Challenges," in *2016 ASEE Annual Conference & Exposition*. New Orleans, Louisiana: ASEE Conferences, Jun. 2016, https://peer.asee.org/25763.

[13] A. Rege, "Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation," in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2015.

[14] M. Olano, A. T. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik,, and D. Thomas, "SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education," in *3GSE*, Aug. 2014

[15] P. Chapman, J. Burket, and D. Brumley, "PicoCTF: A Game-Based Computer Security Competition for High School Students," in *3GSE,* Aug. 2014.

[16] T. Denning, A. Shostack, and T. Kohno, (2014). "Practical Lessons from Creating the Control-Alt-Hack Card Game and Research Challenges for Games In Education and Research," in *3GSE*, 2014