Diversifying Cybersecurity Education: A Non-Technical Approach to Technical Studies

Hwee-Joo Kam  
Department of Information Security and Intelligence  
Ferris State University  
Michigan, USA

Pairin Katerattanakul  
Department of Computer Information Systems  
Ferris State University  
Michigan, USA

Abstract— Cybersecurity education does not only confine to the technical studies embodying network security, malware analysis and reverse reengining, application security, and operating systems security. The increasing numbers of Cyberterrorisn and incidents of hacktivism suggest that Cybersecurity pertains to politics, religion, and culture. Drawing on globalization shaped by the economic, legal, political, religion, and social dimensions, extant literature discloses that infusing social science, cultural and political studies into Cybersecurity education could better prepare students for the job market by making students realize the complexity in the real world. This study presents the efforts of integrating cultural, social, and political dimensions into the Cybersecurity curriculum in a public, regional university in the Midwest of the United States. In particular, this study presents the approaches of introducing intelligence analysis coursework that requires students to understand the analysis of competing hypotheses for drawing conclusion related to the possible Cyberattack from a foreign nation, identify the cultural differences across nations for comprehending the hacking motivation of a different nation, and recognize individual’s cognitive and cultural biases during the process of evaluating a cultural event.

Keywords—Multiple-discipline learning; Cybersecurity education; Intelligence analysis

I. INTRODUCTION

Cybersecurity education is multidisciplinary, relying on computing infrastructure, policies, and people [4]. In reality, Cyber-attacks in the present days do not only limit to website defacements but also involve targeting specific organizations or industries to destroy infrastructure, steal intellectual property, or disrupt the economy motivated by political agenda [3][11]. Therefore, it is important to understand the non-technical aspect of Cybersecurity to protect public and private infrastructures.

Cybersecurity discipline encompasses psychology, sociology, politics, law, computer science, computer engineering, and management [5]. The multidisciplinary perspective fits the emerging theme of globalization and the notion of Cyber-attacks motivated by political agenda. Drawing on globalization driven by economic, legal, political, religion, and social dimensions, infusing social science and political studies into Cybersecurity education [16] could better prepare students for the job market by making students realize the complexity in the professional world.

There are a few studies discussing the interdisciplinary approach in curriculum development. For example, one study suggested a holistic, modular approach to curriculum design in the interdisciplinary studies of Cybersecurity [12]. That is, curriculum model must incorporate software security (e.g. mobile application security, secure coding etc.), hardware security (e.g. physical storage), E-Commerce (e.g. cloud storage, social media, online privacy), legal/ethical (digital copyright), policy/personal (e.g. social network) [12].

However, there are not many studies that demonstrate the integration of intelligence studies encompassing social, political, and cultural perspectives into curriculum and that suggest the synergy between intelligence analysis and technical studies. Therefore, this study fills in the gap by (1) presenting the approaches of introducing intelligence analysis coursework that requires students to understand the analysis of competing hypotheses for drawing conclusion related to the possible Cyberattack, identify the cultural differences across nations for comprehending the hacking motivation of a different nation, and recognize individual’s cognitive and cultural biases during the process of evaluating Cyberthreat in a global context; and (2) suggesting effective mechanism to achieve synergy by integrating technical and non-technical studies in Cybersecurity education. In this context, we examine student learning by discovering (1) how students connect their technical knowledge (e.g. network security and ethical hacking/penetration testing) to the real-life occurrence involving political or religion agenda (e.g. the hacking of a server that stored confidential data about a political group); and (2) how the cognitive and cultural biases affect student’s thought process in analyzing a real-life incident (e.g. Cyberattack against the United States).

This study took place at a university in the Midwest of the United States. The authors collected data from student’s assignments, online posts on the discussion forums, and written feedback about the coursework for intelligence analysis. The discourse analysis approach was employed for data analysis. The preliminary data analysis unfolds the findings that will help this study to improve its qualitative research design in the next stage of research and shares early findings related to the integration of non-technical (Data...
Intelligence and Competitive Theories) and technical subjects into Cybersecurity curriculum.

II. THEORETICAL FRAMEWORK

A. Intrerdisplinary Approach

Ghernaouti-Hélie [8] proposed that Cybersecurity education is “at the crossroads of technological, legal, sociological, economic, and political fields, information security is interdisciplinary by nature.” Therefore, Cybersecurity education must mirror the vision, culture, and civilization of a nation, and meanwhile, fulfill the needs of local community for information security safeguard [8].

Presently, the scope of Cybersecurity education does not confine to the needs of local community and technical studies incorporating network security, malware analysis and reverse reengineering, application security, and operating systems security. The recent threats of Cyberterrorism propel higher education to design effective curriculum models in support of counterterrorism strategy [13]. In general, cyberterrorism refers to a premeditated act of using cyberspace to destroy computer devices and national critical infrastructure (e.g. power grid).

Since Cyberterrorism transcends national boundaries, it is important to build effective curriculum model by introducing global perspective through multidisciplinary studies [8]. Accordingly, multidisciplinary studies must integrate computer science, information systems, politics and social dimension into the curriculum model. In other words, integrating social-science and political contexts into cybersecurity curriculum would close the gap between an engineering approach to cyber security education and that of a social scientist’s approach which would serve to address the expressed needs and changing face of national security [2].

B. Teaching Challenges

Technical studies relates to scientific knowledge in that “producing scientific knowledge requires the kind of sophisticated cognition that only rich social, cultural, and material environments can enable.” [14] Therefore, it is important to link technical subjects with non-technical subjects regarding social science and culture. However, linking both technical and non-technical subjects can be challenging. According to Nersessian [14], processing elements of technical studies, such as algorithm for cryptographic security systems, is independent of media or physical symbol. That is, cognition takes place in the same thinking pattern whether the algorithm will be implemented in the mobile computing or cloud computing. On the other hand, for non-technical studies involving social science and culture, cognition occurs in the physical symbols manifested as the social and culture contexts [14]. In this respect, socio-cultural dimension is examined as knowledge embedded in individual’s mind in some specific contexts [14], thus making it difficult to link context-free technical studies to socio-cultural studies that relies on specific context.

III. RESEARCH METHODOLOGY

A. Discourse Analysis

This study employed discourse analysis approach for data analysis. Building on the notion that knowledge and meanings are formed through multiple discourses, discourse analysis pertains to language-in-use or how individuals complete personal, social, and political projects through language [15]. Discourse analysis proposes that language and words are basically meaningless without the shared and mutual agreement on language usage in which meaning is produced [15]. Careful analysis of language can uncover the social norms, the formation of personal and group identities, the dynamic of social and political interaction, and the cultural practices [7].

Discourse analysis was used in health care studies, organizational studies, and social science studies [1][7][9]. Gee and Green [9] posited that discourse analysis approach could be used in education research wherein researchers discover how learners shape their social and cultural understandings across time. Accordingly, this study adopted discourse analysis to unveil how students build their understanding on the national culture of a foreign nation and the Cyber threats posed by a foreign nation. This was done by “finding meanings behind the words” or interpreting student’s words on their assignments.

B. Data Collection

This study involved a 300-level course named “Data Intelligence and Competitive Theory”. This course served to develop critical thinking skills by exposing students to the emerging themes in the Cybersecurity world.

A total of 25 students participated in this study. Students were required to conduct intelligence analysis in all the assignments. By the end of the semester, the author collected data from homework assignments, online discussions, and student’s feedback. Particularly, the assignments required students to (1) identify their cognitive and cultural biases when evaluating an event occurred in a cultural context; and (2) evaluate different hypotheses for Cyber-attack started by a foreign nation.

C. Data Analysis

In one assignment, students were required to assess an event (social phenomenon) by watching a Reality TV show taken place in and produced by a foreign nation. Basically, the Reality TV show was about a female job contestant who was rejected by the recruiters on the show and was admonished by the host for her behavior. Students were required to identify their cognitive and cultural biases after watching this show. Next, students had to conduct intelligent analysis about the culture of the foreign nation so that in the next class session they could attain better understandings on the Cyberhacking culture of the foreign nation.

At the preliminary stage, this study discovered that some students were confused by the cultural context of the show:
“Towards the beginning of the show, I felt confused as to whether the host and contestant were being serious or just joking around.”

“I did not understand why the host seemed to be very defensive towards the way [the female contestant] talked about [her own country]. I also did not understand why the host was basically condescending towards her...”

“I couldn’t understand why he was so hostile towards the contestant, and why everyone kept asking about her family.”

In spite of identifying their biases, students still evaluated the Reality TV show based on their pre-conceived notions. Many students sided with the job contestant whose values were closer to theirs.

“Since I am from the U.S., I am also on [the female contestant] side. I didn’t see anything wrong with her answers, and I didn’t feel that they host was being fair.”

“The host wasn’t fair to [the female contestant] to really give her a chance and show her strengths; instead he picked and attacked her.”

“This show would get banned from America while the first episode was airing... I have been interviewed by many employers and they don’t ask personal questions in regards to what the recruiters asked [the female contestant]”. 

Finally, students could induce culture and social norms of the foreign nation despite their biases.

“I notice the social hierarchy structure in [the foreign nation]. This was evident with the host showing dismay towards the contestant after being challenged intellectually.”

“It appears that the show is very westernized and emphasizes the individualism of both the contestant and the successful executives. It appears to have many of typical attributes of any western reality television show; however the incident with the host confirms that it is still struggling with maintaining old cultural norms.”

“The shifting roles of women in the [nation] make it difficult for many people, especially those “returnees” who spend time out of country in Westernized societies and situations.”

In another assignment, students were required to outline and assess different hypotheses about Cyber-attack initiated by another foreign nation against the US banking systems. The foreign nation in this assignment was different from that of the last assignment. Students had to come out with their own hypotheses, use the software to evaluate their hypotheses, and finally provide rationales to explain the outcomes of their evaluations.

The analysis result revealed that most students stated that the foreign nation had attacked the banks in the United States. Many suggested that the United States should strengthen its cyber offense and defense to protect the banking infrastructure.

“The weighted inconsistency score indicates that the hypothesis with the highest probability is [the foreign nation] launched a cyber-attack on major U.S. banks. My suggestion would be to analyze the attacks in order to be better prepared for similar attacks and to launch our own overwhelming offensive in order to make them expend their resources on defense.”

“Based on the weighted inconsistency scores, it is very likely that the government of [the foreign nation] is behind this attack. However, a religious movement or terrorist group could be performing these attacks as well. The evidence provided does not support the theory that it was any organization outside of [the foreign nation].”

“[The foreign nation] is making retaliatory strikes against the United States and our allies and he is trying to test his cyber-capabilities as well as the U.S.’s defensive capabilities. He is looking for ways into our critical infrastructure as he knows that is where we are weakest.”

“The hypotheses that are most likely is that it could possibly be the government [of the foreign nation] is the one who attacked the United States. My suggestions are that the U.S. should probably see if there is a bread crumb trail to see if that it leads to the [foreign nation].”

“The two hypotheses with the highest probability are the ones that suggest either the [foreign nation] is behind the cyber-attacks, or an independent group within [the foreign nation] is behind the attack. Judging by the information and evidence I researched and read about, it seems likely that one of these two hypotheses are accurate, but it is hard to say which one is actually true. I would suggest that the banks continue to upgrade and change their security to keep those who might be trying to hack them guessing.”

IV. DISCUSSION, CONCLUSION, AND FUTURE RESEARCH

The preliminary phase of analysis results revealed that students went into a stage of confusion when attempting to assess a different culture of a different nation. Although, students evaluated a cultural phenomenon with their cultural and cognitive biases, they managed to accurately derive the cultural and social norms of the foreign nation. This infers that introducing a foreign culture to students enable students to build some cultural understanding that will later help them to realize the Cyber hacking culture of the foreign nation.

In the assignment of assessing hypotheses regarding the Cyber threats, the preliminary analysis results disclose that many students assumed that the foreign nation orchestrated a Cyber-attack against the US banking systems. There might be some biases in drawing the conclusion. Students might have unknowingly influenced by the tragic incident of 9/11 in the process of evaluation.

Another interesting finding is that students did not link their technical knowledge (e.g. denial of service attack, SQL injection, XSS etc.) in their reasoning when conducting hypotheses testing related to Cyber threats. This finding is consistent with the notion that processing scientific knowledge occurs in a context-free condition but processing cultural and social elements occurs in a specific social and cultural context [14]; and therefore, it is difficult to form a bridge between the two. Another plausible explanation is that the research design did not remind students to link culture/social elements with
Cybersecurity technology. Therefore, the future research will address this issue.

Based on the preliminary findings, the future research will also adopt cognitive learning theories to examine student learning in both the socio-cultural and technological dimensions. In other words, investigate human cognition in terms of making connection between technical and socio-cultural learning.

REFERENCES


