Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 8

October 2023

Like Treating the Symptom Rather than the Cause - the Omission of Courses over Terrorism in NSA Designated Institutions

Ida L. Oesteraas
Old Dominion University, ioestera@odu.edu

Like Treating the Symptom Rather than the Cause - the Omission of Courses over Terrorism in NSA Designated Institutions

Abstract

The National Security Agency (NSA) awards Center of Academic Excellence (CAE) designations to institutions that commit to producing cybersecurity professionals who will work in careers that reduce vulnerabilities in our national infrastructure. A review of the curricula in the 327 institutions and their degree programs reveal that only two programs offer a required course about terrorism. Given the fluid nature of terrorism and its threat to national infrastructure, the omission is concerning. It is recommended that NSA-certified cybersecurity programs begin implementing educational content that aim to teach about this emerging crime and justice issue. One suggestion is to embrace the interdisciplinary nature of cybersecurity, as exemplified in the success of the Cybersecurity Living and Learning Community (CLLC). Designing courses that educate about the social processes that leads to the growing problem of violence and terror directed towards marginalized communities and our nation's technological infrastructure, is another.

Keywords

terrorism, cyber terrorism, cybersecurity, national security, curriculum development, interdisciplinary education.

Like Treating the Symptom Rather than the Cause - the Omission of Courses over Terrorism in NSA Designated Institutions

Ida Oesteraas
Old Dominion University
Norfolk, VA, USA
ioestera@odu.edu
https://orcid.org/0000-0001-6524-061X

***Abstract*—The National Security Agency (NSA) awards Center of Academic Excellence (CAE) designations to institutions that commit to producing cybersecurity professionals who will work in careers that reduce vulnerabilities in our national infrastructure. A review of the curricula in the 327 institutions and their degree programs reveal that only two programs offer a required course about terrorism. Given the fluid nature of terrorism and its threat to national infrastructure, the omission is concerning. It is recommended that NSA-certified cybersecurity programs begin implementing educational content that aim to teach about this emerging crime and justice issue. One suggestion is to embrace the interdisciplinary nature of cybersecurity, as exemplified in the success of the Cybersecurity Living and Learning Community (CLLC). Designing courses that educate about the social processes that leads to the growing problem of violence and terror directed towards marginalized communities and our nation's technological infrastructure, is another.**

Keywords — terrorism, cyber terrorism, cybersecurity, national security, curriculum development, interdisciplinary education.

I. Introduction

The National Security Agency (NSA) awards Center of Academic Excellence designations (CAE) to institutions that commit to producing cybersecurity professionals who will be trained to reduce vulnerabilities in U.S. infrastructure. The main goal of this program is to promote and support quality academic institutions of higher learning to produce the nation's cyber workforce. After an extensive review of the different degree programs offered by the 327 NSA designated institutions, an alarming total of two of these programs require students to take a course concerned with terrorism. An additional six institutions offer courses on terrorism as an elective. Given that this NSA program is intended to educate future cybersecurity professionals on ways to combat threats to U.S. national security, the absence regarding terrorism content leaves room for concern.

Research shows that cyber terrorism has been characterized as a grave threat to western society [1]. Cyber acts are particularly difficult to attribute to specific actors, making cyber terrorism a likely outcome for those inclined to perpetrate terrorist actions [2]. It has been well established that cyber-attacks can lead to grave financial losses [3], civil torment [4], and loss of human life [5]. Given the global reliance on technological infrastructures, large-scale cyber-attacks are ranked among the top five greatest global risks affecting civilization in the next 10 years [2]. Securing the nation's technological infrastructure is therefore crucial to national functioning and security [6]. Such research clarifies the urgency in addressing the issue of cyber terrorism and its threat to national security and infrastructure.

In 2021, FBI Director Christopher A. Wray noted the following amidst the increase in domestic terrorist attacks in the U.S., "confronting domestic terrorism is a top national security priority of the agency" [7]. Given the prevalence of, and grave consequences following terrorism in the U.S. today, NSA's purpose to reduce vulnerabilities to national infrastructure is weakened by the lack of courses that aim to teach about terrorism in the agency's certified cybersecurity programs. This paper presents current developments of terrorism that are threatening the nation's technological infrastructure. Against this backdrop, the study is concerned with two research questions:

(1) To what extent do curriculums in NSA certified cybersecurity programs offer courses concerned with terrorism? and

(2) Given the omission of courses on terrorism, how can the field of cybersecurity embrace its interdisciplinary nature and consider classes or topics concerned with terrorism?

II. Literature Review

A. Cyber Terrorism

In 2005, Denning described "terrorism" as,

> ...physical acts of violence intended to inculcate fear... behind the physical assaults, is another dimension... the information dimension, and terrorists exploit it every bit as much as the physical. Their ultimate goal ... is power and influence. Terrorists seek a change, and their objective is to influence populations in ways that support that change. To do that, they engage in both physical and information operations... [1: 8].

Adding "cyber" to the equation and defining "cyber terrorism" has proven challenging. While it may be simple to

roughly define the concept, a large amount of subjectivity plays a role in understanding what the concept comprises [9]. Over the years, we have seen a change from rather simple descriptions of cyber terrorism to now more all-embracing ones. An example of the prior is "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)" [4: 10]. Newer definitions expand on this perspective and include additional components. Some bring in considerations of political leaning and define cyber terrorism as "almost any politically or socially motivated use of information technology by terrorists to perform attacks against computers, networks and information systems resulting in violence against noncombatant targets, and causing injuries, bloodshed, or serious damage or fear" [3: 2].

Given the fluid nature of the act, a cyberterrorist can not only target individual computer networks but also entire universities, communities, local, state, and federal governments. Given such detrimental consequences, acts of cyber terrorism have the potential to harm large sections of society in a multitude of ways. As researchers find, terrorism aggravates anxiety and personal insecurity while exacerbating perceptions of threat and personal insecurity [11]. Following individuals' high levels of threat perception is willingness to support strong foreign and domestic government policies (e.g., military responses to cyberattacks and support of surveillance strategies) [11]. Individual and collective perceptions of threats may lead to the unwanted societal developments discussed in a later section on the cybersecurity and terrorism symbiosis.

B. The National Center of Academic Excellence in Cybersecurity (NCAE-C) program

The National Security Agency (NSA) administers the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program [12]. There are three sub-components: the Centers of Academic Excellence in Cyber Defense (CAE-CD), Cyber Operations (CAE- CO) and Cyber Research (CAE-R). Federal partners include the Federal Bureau of Investigation (FBI) and the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), among others. In assisting quality academic institutions and programs, the program is central in supporting and producing future cyber security employees [12]. Eligibility to apply for any of the designations depends on the characteristics of the academic institution. For instance, the CAE-CD designation is available to all accredited two-year, four-year, and graduate level institutions in the United States that offer degrees related to cybersecurity [12]. In contrast, the CAE-R sub-category is accessible only for regionally accredited R1, R2, or R3 institutions [12]. Being awarded a CAE designation is an indication of approval from the NSA as it signifies that a cybersecurity curriculum is addressing topics of value to the federal government and its cybersecurity workforce.

C. The Current State of Cybersecurity Curriculum

Researchers continue to encourage the interdisciplinary nature of cybersecurity [13], [14]. This is ultimately a call for the field to move away from the dominating technological focus to consider the inclusion of content associated with the various human dimensions connected to cybersecurity efforts [14]. According to one cybercrime expert, "a holistic approach to cybersecurity is one that considers the many disciplines that produce cybersecurity professionals – technical and nontechnical alike, in a coherent fashion" [62: 14]. Efforts to embrace the interdisciplinary nature of cybersecurity has occurred in cybersecurity education. For instance, Living and Learning Communities (LLCs) has aided the promotion of interdisciplinary connections between students and instructors across disciplines, including cybersecurity [15], [16]. Others have developed interdisciplinary cybersecurity courses. One example of such classes, *Cybersecurity, Technology, and Society*, enjoy influence from several disciplines including information technology, business, and criminal justice [16].

In terms of cybersecurity curriculum development, two separate projects serve as examples that have helped guide the development: the 2017 Cybersecurity Curricula (CSEC2017) and the NSA's Center of Academic Excellence (CAE). While the former serves as an example to provide guidelines for cybersecurity curricula development [17], the latter focuses on providing a basis for cybersecurity programs to meet the needs of educating cybersecurity workers [18], [12]. CSEC2017 propose eight knowledge areas should be met when designing cybersecurity curriculum: (1) data security, (2) software security, (3) component security, (4) connection security, (5) system security, (6) human security, (7) organizational security, and (8) societal security [17]. The latter knowledge area, *societal security*, treats "cybersecurity aspects that affect society at large, such as cyberlaw and cybercrime, ethics, professional and social responsibility, and intellectual property" [2437: 18]. One of the essential knowledge units hereunder, *Cybercrime*, highlight the need to educate on the topic of *Cyber terrorism* while stating the essential learning outcome is to summarize "activities in cyberspace geared toward generating societal fear and uncertainty" [71: 17]. Such curriculum guidelines serve not only as an example of how interdisciplinary the field of cybersecurity ought to be, but also suggest that cybersecurity programs should include teaching related to terrorism in their curriculum.

Requirements set forth by the CAE project is not meant to serve as a curriculum guide but rather to provide a basis for cybersecurity programs to meet the needs of educating cybersecurity workers [18]. For institutions to be awarded any of the prestigious NSA designations described above, curriculums need to be mapped according to a set of Knowledge Units (KUs) in line with the framework set forth by the National Institute of Cybersecurity Education (NICE), a cybersecurity language that educators use nationwide [19]. One of the KUs is the *IT Systems Components* (ISC) in which topics such as endpoint protection and network security components need be addressed [20]. Multiple benefits follow being awarded the NSA designation. For instance, students and faculty become eligible to apply for scholarships and grants through collaborating agencies like the National Science Foundation (NSF). Due to such benefits, it seems fair to suggest that the CAE requirements, at least partly, help drive curriculum development. It should be noted that a complete investigation into cybersecurity curriculum is beyond the scope of this work as the focus here is to assess

the omission of courses on terrorism in CAE-C curriculums and offer solutions to this challenge.

Information security degree programs, including cybersecurity, are technical in nature and generally offered through STEM (Science, Technology, Engineering, and Math) departments [21]. Despite some of the efforts described above, current cybersecurity curriculums tend to educate on cyber threats with particularly technologically focused strategies that lack a human-centered focus [22], [23]. In line with extant cybersecurity research [24], [25], the author argues this focus is problematic as it ignores the actual threat of human action and is comparable to treating the symptom rather than the cause. It is necessary to consider an improved approach to educate about the constantly evolving cyberthreats including terrorism that are facing the nation. The recent developments in extremist violence and terror discussed below clarifies the urgent need for teachings on the human aspect regarding the link between cybersecurity and terrorism.

D. Current Challenges Following the Cybersecurity and Terrorism Symbiosis

Linking cybersecurity and terrorism, we are faced with a plethora of recent developments that threatens both civilians and national security. These include, but are not limited to, online hate speech advancing to violence and terror directed towards marginalized communities, and extremists' use of technology to enhance sociopolitical and financial goals. In mitigating these challenges, cybersecurity professionals could be helpful in many ways including designing programs to mitigate the spread of hateful and extremist content online.

Growing evidence speaks to a surge of populist-driven far-right extremism in western countries [26], [27], [28]. Terrorism (see example of definition above) can be executed by perpetrator(s) with any political or ideological leaning. However, acts perpetrated by those associated with far-right motivations (e.g., white nationalists), are found to be significantly more likely to be violent than their far-left counterparts (e.g., environmentalists) [29], [30]. Surely, in the U.S. the recent flow of xenophobic rhetoric has led the way for the mainstreaming of hate directed towards historically marginalized communities [28], [31]. Studies indicate that derogatory and discriminatory speech directed against social groups such as religious and immigrant minorities increase the risk of violence against them [28].

One consequence following the adaptation of hate towards certain groups is online radicalization. This can lead to the active intent or approval of violence to attain a stated goal perpetrated against a marginalized community [32]. The U.S. has already experienced several deadly incidents of online radicalization. As has been clarified by the words in disturbing manifestos published online prior to domestic terror attacks such as the 2015 Charleston church shooting [33], and the 2019 El Paso Walmart shooting [34], online radicalization played a pivotal part in the attacks themselves.

Terrorists and violent extremist actors also use several technologies to enhance their sociopolitical goals. For example, domestic and international terrorist groups use cryptocurrency as an enabler to finance their operations [35], [36]. The cryptocurrency arrangement is decentralized, exist outside of governmental control, and help facilitate an alternative method of payment using encrypted algorithms. As a recent report shows, international terrorist groups including Hamas's military branch, an al-Qaeda affiliate, and ISIS are currently using cryptocurrency to aid in funding operational costs such as training, bribes, and weapons [36]. Far-right extremist groups and actors also embrace the use of cryptocurrency to finance activities [37], [38]. For instance, the Swedish Neo-Nazi political party, the Nordic Resistance Movement (NRM), hold digital wallets with well-known cryptocurrency platforms, and has recently published an action plan to prepare for an economic emergency [38]. In 2020, the Department of Justice published a report stating that, "this technology [cryptocurrency exchange] already plays a role in many of the most significant criminal and national security threats our nation faces" [viii: 39]. Such statements coupled with the widespread use of cryptocurrency by extremist actors and terrorists demonstrates the capacity for these groups to evolve beyond traditional ways of financing operations as it allows for the anonymous generation of income while effectively escaping scrutiny by police.

By embracing the interdisciplinary nature of cybersecurity, the field can help mitigate some of the threats discussed above. One example is continuing the work to build strong content moderation programs that engage efforts to mitigate the spread of online hate. As mentioned earlier, terror and violence directed towards marginalized communities can be the end-result of wide-spread hate speech directed towards these groups [28]. As a response to these developments, a growing body of research turn to the development of algorithmic moderation systems [40], [41], [28]. Algorithmic moderation is defined as "systems that classify user generated content based on either matching or prediction, leading to a decision and governance outcome (e.g., removal, geo-blocking, account takedown)" [3: 42]. Two prominent technologies used by large social media companies such as YouTube and Twitter are predictive machine learning tools and matching [42]. Matching involves identifying a newly uploaded piece of content against an existing database while classification (prediction) evaluates new content that has no corresponding previous version with the goal of placing the new content into one of several categories [42].

Some argue that fully automated decision-making systems that do not include a human "checkpoint" are treacherous as it risks issues related to bias [43]. For example, if a classifier is only given examples of hateful discourse directed towards one ethnic group, it may fail to learn that hate speech can be directed against other communities. Therefore, knowledge about the social processes and the context which result in adaptations of hate towards marginalized groups is pivotal when we consider the role humans play in such moderation efforts. This demonstrates the value of integrating teachings about the social processes related to terrorism in cybersecurity curriculums.

III. Methods

This study was concerned with assessing the extent to which NSA certified cybersecurity programs offer courses concerned with terrorism, and to propose suggestions following the omission of such courses. To study this, the author reviewed curriculums in degree programs at every NSA-certified institution located at the official CAE website.

From the details regarding designation type available on this website, the designation at 60 of the 387 institutions had expired in the last two years. Given this observation, a total of 327 institutions and their cybersecurity programs were found eligible for inclusion in the study.

Given the purposes of the study in assessing the extent to which cybersecurity programs offered courses on terrorism, the author looked for any courses within these curriculums that had "terrorism" or "cyber terrorism" in the name or course description. Concentrating on one institution at a time, the author visited the official website of 327 institutions and located every cybersecurity program that had received one or more of the NSA designations described above. The author utilized several Excel sheets to track information about (1) the institution's name, (2) whether the institution was private or public, (3) what degree(s) each institution offered, (4) what type of establishment the institution was (e.g., graduate school, college, university), (5) the name(s) of the NSA certified cybersecurity degree programs offered at the institution, (6) the name of the department offering the degree, (7) the U.S. state of the institution, (8) name of the terrorism course, and (9) the department offering the terrorism course. After locating each of the NSA certified cybersecurity degree programs, the author viewed the curriculums for each of these programs and noted the information described above. This process was repeated with all 327 NSA certified institutions and yielded the results discussed below.

IV. Findings

After an extensive review of the different degree programs offered by the 327 NSA designated institutions, an alarming total of two of these programs require students to take a course concerned with terrorism. An additional six institutions offer courses on terrorism as an unrequired elective. The two tables below provide a summary of these findings.

TABLE I. Required Terrorism courses

Course	Required Terrorism Courses		
	Institution, State, Type	***Degree Program***	***Department Offering Course***
ISS 379 Cyber-warfare and Cyber-terrorism	University of Maine at Augusta, Maine, Public College	BS Cybersecurity with concentration in Cybersecurity Analyst	Cybersecurity and Computer Information Systems Department
HSPS 415 Introduction to Terrorism	Vincennes University, Indiana, Public College	BS Homeland Security and Public Safety – concentration in Cybercrime Investigation and Incident Responder	Information Technology Department

Fig. 1. Institutions offering required courses on terrorism.

TABLE II. Unrequired, Elective Terrorism courses

Course	Unrequired, Elective Terrorism Courses		
	Institution, State, Type	***Degree Program***	***Department Offering Course***
CJUS 5554 Terrorism	California State University, San Bernadino, California, Public University	BS in Intelligence and Crime Analysis	Criminal Justice Department
PSCI 5900 Seminar in International Relations (Terrorism in Africa)	California State University, San Bernadino, California, Public University	MS National Cybersecurity Studies	Political Science Department
PSCI 6060 Analysis of International Terrorism	California State University, San Bernadino, California, Public University	MS National Cybersecurity Studies	Political Science Department
CRJ 416 Terrorism and National Security	Hampton University, Virginia, Private University	BS Computer Science with concentration in Cybersecurity	Sociology and Criminal Justice Department
LAW 778 Counter-terrorism	Texas A&M University, Texas, Public University	Graduate Certificate in Risk Management and Compliance	School of Law
HSM 104 Terrorism and Homeland Security	Trident Technological College, South Carolina, Public Community College	AAS Cybersecurity	Business Technology
CSEC 723 Cybercrime and Cyber-terrorism	University of Nevada Las Vegas, Nevada, Public University	MS Cybersecurity	Computer Science Department
HLS 505 Political Violence and Terrorism	University of New Hampshire, New Hampshire, Public University	BS Homeland Security	Security Studies Department

Fig. 2. Institutions offering unrequired, elective courses on terrorism.

Regarding the institutions offering required courses on terrorism/cyber terrorism, one of these, Vincennes University, a public college in Indiana, offers a Bachelor of Science in Homeland Security and Public Safety - Cybercrime Investigations and Incident Responder Concentration. For this degree, HSPS 415: 'Introduction to Terrorism,' is listed as a required course. Offered by the Information Technology Department, the course seeks to '…examine the historical basis for terrorist acts, the psychological, cultural, and sociological underpinnings of the goals and apparent motivations of the modern terrorist, the usability and validity of "profiles" of the typical terrorist, and the differences between the modern "active" terrorist organizations.' Another public college, the University of Maine at Augusta, offers a Bachelor of Science in Cybersecurity with four different focus areas: 1) General, 2) Cyber Forensics, 3) Information Assurance, 4) Cybersecurity Analyst. In the latter specialization, students are required to take ISS 370: 'Cyberwarfare and Cyberterrorism,' which is offered in the

Department of Cybersecurity and Computer Information Systems. From the course description, the course '…explores the cyberwarfare landscape, offensive and defensive cyberwarfare techniques, and the future of cyberwarfare.'

Six other NSA certified institutions offer programs with a total of eight elective courses concerned with terrorism. California State University, San Bernardino, is a public university offering undergraduate and graduate degrees. For the degree programs in Cybersecurity at this institution, the author finds three elective course options concerned with terrorism: CJUS 5554: 'Terrorism' (elective option for the Bachelor of Science in Intelligence and Crime Analysis program), PSCI 5900: 'Seminar in International Relations' [Terrorism in Africa], and PSCI 6060: 'Analysis of International Terrorism' (the two latter courses are both elective options for the Master of Science in National Cybersecurity Studies degree).

Another elective concerned with terrorism is available at the private institution Hampton University in Virginia. In a collaborative effort between the Computer Science and Criminal Justice department, students can earn a Bachelor of Science in Cyber Security. Here, students can choose either CRJ 416: 'Terrorism and National Security' or CRJ 305: 'The Criminal Justice System' to fulfill degree requirements. In the course description, CRJ 416 addresses topics including, '…worldwide terrorism, terrorist violence, governmental reaction to specific demands and threats with the objective of weakening established governments.' Furthermore, at the public institution, Texas A&M University, a Graduate-level Certificate in Risk Management and Compliance is offered. Here, one of the 14 electives listed is LAW 778: 'Counterterrorism.' According to the course description, the class 'takes an in-depth look at counterterrorism in China, Colombia, India, Israel, Russia, Spain and the United States by examination of compelling conceptions and definitions of terrorism at the national international level and the institutions and processes relevant to operational counterterrorism.' Trident Technical College in South Carolina is a public community college offering associate degrees and undergraduate certificates in cybersecurity. One elective for the associate in applied science degree is HSM 104: 'Terrorism and Homeland Security,' a class that 'provides an overview of the issues of terrorism and homeland security efforts by drawing on several disciplines.'

Given the large number of elective options offered in the two programs discussed above, it is worth noting that students' choice to select courses represent the elective options that students have at each institution. Some students may also base their decision according to individual preferences and scheduling. Courses may also be listed as an elective but not offered every semester. HSM 104 offered at Trident illustrates this point since it is one of 22 elective options and is only offered in the fall semester. On the other hand, courses concerning terrorism at larger institutions such as California State University in San Bernadino contradict this point. In fact, from the information on their website, CJUS 5554: 'Terrorism,' has been offered every semester for years and was last accessible for students in spring 2023 while also being scheduled for fall the same year. The options of educational exposure to the issues related to terrorism for students pursuing a Master of Science in Cybersecurity at the University of Nevada in Las Vegas is one in 11. At this institution, one of the options listed is a course titled CSEC 723: 'Cybercrime and Cyberterrorism.' In a relatively vague course description signaling the predominant focus in the course is on cybercrime, the class seeks to '…expose critical issues related to privacy, terrorism, hacktivism, the dark web, and much more.' One last elective course option, HLS 505: 'Political Violence and Terrorism' is offered for students pursuing the Bachelor of Science in Homeland Security offered by the Department of Security Studies at the University of New Hampshire. From the course description, the class 'provides an interdisciplinary approach to the study of political violence and terrorism, the organization pattern of cells, groups, and networks, and the role of ideology and identity in shaping goals, targets, and tactics.'

Overall, this study finds a glaring lack of courses focused on terrorism among NSA-certified cybersecurity programs. The lack of courses regarding terrorism in the NSA certified CAE-C designated programs leaves room for concern, especially given NSA's purpose of securing national infrastructure coupled with the problematic nature of terrorism. Given this finding, a discussion on practical implications seems fitting. Overall, the recommendation is for educators to embrace the interdisciplinary nature of cybersecurity. The work now turns to a discussion of these.

V. Implications

Two major implications follow the omission of courses on terrorism in NSA designated cybersecurity curriculum. For one, and in line with extant research, the goal for future cybersecurity programs should be to keep embracing interdisciplinary efforts [13], [14]. Given that current cybersecurity curriculums embrace particularly technologically focused strategies that lack a human-centered focus, cybersecurity programs should consider collaborations with disciplines such as criminal justice, political science, and sociology when designing learning initiatives that introduce students to topics related to the social processes concerned with terrorism. Ongoing interdisciplinary efforts between the cybersecurity and criminal justice discipline illustrates how such collaborations can work in practice. Starting in 2014, criminologist Thomas Holt has led the development of the International Interdisciplinary Research Consortium on Cybercrime [44]. In the announcement of this effort, the researcher wrote,

> ...we have to develop a holistic research agenda to combat cybercrime and improve cyber security postures. This is only achieved by linking the social sciences with computer science and engineering disciplines to better understand all facets of this problem. Understanding both the human and the system is the only way to improve the state of the field of cyber security [para. 2: 44].

Holt's statement highlights the need to embrace interdisciplinary efforts among cybersecurity programs and the social sciences. It seems fair to suggest that with such collaborations, we are better equipped to handle the timely developments in terrorism that is threatening U.S. national infrastructure and security today.

The success of one prominent initiative, *Living and Learning Communities* (LLCs), clarifies how multiple disciplines can come together to engage in collaborative efforts to bridge learning outcomes and course assignments. LLCs have a long history in academic institutions. Research has established the success of such learning communities

[15], [45]. Learning communities promote student learning [46], [47], and boost graduation rates [48]. Despite the established success of these communities, it should be noted that the growth of such communities has not occurred uniformly across disciplines. For instance, researchers note that learning communities are not common in computer science [49]. Such observations suggest there is an opportunity to expand this successful practice more broadly into majors such as those dominated by the STEM discipline, including cybersecurity.

The Cybersecurity Living and Learning Community (CLLC) at Old Dominion University (ODU) is designed to promote co-curricular connections between students and instructors. The goal is to link up to three courses to explore a certain theme through different perspectives. Students connect what they are learning from each of the linked courses through integrated assignments and enrichment activities. In the CLLC at ODU, classes include *Cyber Explorers and University Orientation*, *Cybersecurity, Technology, and Society*, and *Introduction to Criminology*. Taking these three courses in their first semester, students are asked to keep in mind an overarching question; "What are the interdisciplinary intersections and emerging trends and issues in the field of cybersecurity?" This serves as the grounding concept to remind students of the general purpose of, and reasons for taking, these inter-related courses.

In a collaboration between three instructors, several linked assignments are developed with the goal to understand how the sub-fields that make up Cybersecurity are related. One of these assignments is to create a personal "ePortfolio," or a website, to showcase integrated assignments throughout student's academic career at ODU. Functioning as an extension of the traditional printed portfolios, ePortfolios are used to either maintain or monitor progress in courses or academic degrees. Due to its digital nature, ePortfolios help showcase student's work [50], and foster opportunities for integrated learning [51]. Several assignments in each class were posted onto student's ePortfolio. In answering the overall "big question" indicated above, the accumulation of assignments from the different courses helps students to engage in self-reflection of the material they are learning about [52]. Showcasing examples of integrated learning at the university level becomes realistic through ePortfolios and can help students find careers in the cybersecurity or related fields.

One of the classes in the CLLC is *Introduction to Criminology*. At ODU, this class enjoy influence from various disciplines but takes a sociological approach to crime. Objectives for this class include developing an understanding of the relationship between various criminological theories and methods used to test them, defining different types of crime, and applying theories to "real world" issues and policies. The way in which the class is taught allows for integrated assignments in bridging the connection between cybersecurity and crimes such as terrorism. A scaffolding assignment developed by a professor teaching *Introduction to Criminology*, clarifies this point. In this assignment, students were asked to select a criminological theory that can be used to explain any type of crime, including cyber terrorist activities. During the project, students were asked to focus on the following: (1) The definition of the crime in question (i.e., incidence and impact on society), (2) Application of a criminological theory (i.e., what criminological theory can be applied to the crime to explain why/how it occurs), and (3) criminal justice response(s) to the crime of choice. Such assignments serve as an example on how two departments can work together in creating projects where students are exposed to educational content on terrorism.

A new class offered at Old Dominion University in fall 2023 serves as another example of how the field of cybersecurity can embrace its interdisciplinary nature. Although not necessarily a definite solution to the problem of the omission of courses on terrorism found in this study, a class, *Cyber Terrorism* is being offered as an upper-level undergraduate class. Cross-listed and offered to both Cybersecurity and Criminal Justice students and taught by a criminologist, the class takes an interdisciplinary approach when seeking to educate students about the many connections between cybersecurity and terrorism including online hate speech advancing to violence and terror, and extremists' use of technology to enhance sociopolitical and financial goals. It should be noted that not every cybersecurity program can cover every specialty area, nor every program would need a class on cyber terrorism. Nevertheless, designing and offering similar courses may be a realistic endeavor for some institutions.

Overall, these examples illustrate the main implication of the study that is for cybersecurity curriculum developers to embrace the interdisciplinary nature of cybersecurity. With Learning Communities that include introductory Criminology or Criminal Justice courses, cybersecurity students can be introduced to the importance of topics covered in these courses for their major.

With collaborations across disciplines in creating integrated assignments and activities, or in some cases, the creation of courses on Cyber Terrorism, we can aid in clarifying this interdisciplinary connection and help students understand the links between cybersecurity and terrorism. Arguably, student's time in college will be much richer if they pull in various disciplines and synthesize their learning experiences. Learning from the social sciences about the human aspect of terrorism is clearly a pivotal part in understanding current societal developments happening online such as radicalization leading to violence.

VI. Limitations

The main purpose of this study was to address the extent to which CAE-C institutions offer courses on terrorism and offer solutions to this challenge. The findings show a glaring omission of such courses. The study started the conversation about how the cybersecurity discipline can embrace interdisciplinary efforts to provide a solution to this problem. However, the study is not without limitations.

For one, the work did not engage an additional review to assess the extent to which various university core curriculums in political science and/or criminal justice offer courses on terrorism. Many educational institutions offer courses that educate about terrorism in core programs and electives. It may be true that at some institutions (perhaps particularly at larger universities), students may take courses that educate on terrorism as part of their core electives. If students can take classes with other departments that offer courses concerned with terrorism, this would be somewhat of a solution to the evident omission of teachings on cyber terrorism/terrorism in

cybersecurity curriculums found in this study. Future studies may investigate just how often cybersecurity students at different institutions can chose courses concerned with terrorism as part of their overall degree program requirements.

Second, many of the CAE-C programs leave room for students to take a fundamental class classified as a social science (e.g., Introduction to Sociology). It is uncertain just how often cybersecurity students are exposed to educational content related to terrorism by taking these classes. Since the study did not engage a thorough investigation into the most common required and elective courses in all the CAE-C programs, it could be helpful to engage an all-embracing investigation of these. Combining the current study with this future investigation can help better identify a model curriculum that can be used to recognize ways in which terrorism should be taught in NSA designated cybersecurity programs.

VII. Concluding Thoughts

This study calls for the consideration that current cybersecurity curriculums, predominately influenced by STEM disciplines, include more emphasis on courses that educate on the human aspect of terrorism. Suggestions include the introduction of interdisciplinary initiatives to educate students about the sociopolitical forces aided by the Internet that leads to developments such as widespread radicalization and violence, as well as terrorists' misuse of technological infrastructures. As recent rise in hate crimes and terror directed at marginalized groups shows, hate speech and extremist radicalization have the potential to graduate to violence. Given the extent to which these societal processes occur in the cyber space, it is crucial that both criminal justice, and cybersecurity educators engage in interdisciplinary conversations and consider courses and other initiatives that can help educate about these evolving crime and justice issues.

References

[1] M. Abruzzo, and R. Kennedy, "Radicalization in the Cyber-Proselytism Era and the Fight Against Terrorism while Respecting Human Rights," *Gonzaga Journal of International Law*, pp. 1-10, 2018.

[2] J. J. Plotnek and J. Slay, "Cyber terrorism: A homogenized taxonomy and definition," *Computers & Security*, vol. 102, pp.1–13, 2021. Available: https://doi.org/10.1016/j.cose.2020.102145

[3] P. Linnartz, A. Winkens, and A. Ulbig, "Assessing the impact of cyber attacks manipulating distributed energy resources on power system operation." Astrophysics Data System. Accessed Oct. 4, 2022. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2022arXiv220707968L/abstract

[4] P. Wang, "Death by hacking: The Emerging Threat of Kinetic Cyber," in *Combating Violent Extremism and Radicalization in the Digital Era*, vol. 1, P. Wang, Eds. IGI Global, 2016, pp. 452- 468.

[5] M. Albahar, "Cyber-attacks and terrorism: a twenty-first century conundrum," *Science and engineering ethics*, vol. 25, no. 4, pp.993-1006, 2019. Available: https://doi.org/10.1007/s11948-016-9864-0.

[6] A. Rege-Patwardhan, "Cybercrimes against critical infrastructures: A study of online criminal organization and techniques," *Criminal Justice Studies*, vol. 22, no. 3, pp.261-271, 2009.
Available: https://doi.org/10.1080/14786010903166965

[7] D. Barrett, and M. Zapotosky, "FBI report warned of 'war 'at Capitol, contradicting claims there was no indication of looming violence." The Washington Post. Accessed: Nov. 10, 2022. [Online]. Available: https://www.washingtonpost.com/national-security/capitol-riot-fbi-intelligence/2021/01/12/30d12748-546b-11eb-a817-e5e7f8a406d6_story.html

[8] D. E. Denning, "Information Operations and Terrorism." Defense Technical Information Center. Accessed: Oct. 5, 2022. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA484999

[9] M. Plachkinova, and A. Vo, "A Taxonomy of Cyberattacks against Critical Infrastructure," *Journal of Cybersecurity Education, Research and Practice*, vol. 2021, no. 2, pp.1-17, 2022. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/3

[10] G. Weimann, "*Cyberterrorism: How real is the threat?"* Vol. 31. United States Institute of Peace, 2004.

[11] M. L. Gross, D. Canetti, and D.R. Vashdi, "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes," *Journal of Cybersecurity*, vol. 3, no.1, pp.49-58, 2017. Available: http://dx.doi.org/10.2139/ssrn.2836199

[12] NSA, "National Centers of Academic Excellence in Cybersecurity." National Security Agency. Accessed Nov. 18, 2022. [Online]. Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[13] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014. Available: https://www.timreview.ca/article/835

[14] J. Jacob, M. Peters, and T.A. Yang, "Interdisciplinary Cybersecurity: Rethinking the Approach and the Process," in *National Cyber Summit (NCS) Research Track*, pp. 61-74, 2020. Available: https://doi.org/10.1007/978-3-030-31239-8_6

[15] V. Tinto, "Learning communities: Building gateways to student success," In *The National Teaching and Learning Forum*, vol. 7, no. 4, pp. 1-11, 1998.

[16] B. K. Payne, L. Mayes, T. Paredes, E. Smith, H. Wu, and C. Xin, "Applying High Impact Practices in an Interdisciplinary Cybersecurity Program," *Journal of Cybersecurity Education, Research and Practice*, vol. *2020*, no. 2, 2021. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss2/4

[17] D. Burley, M. Bishop, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, and A. Parrish, A. "Curriculum guidelines for post-secondary degree programs in cybersecurity. Cybersecurity Curricula 2017." Association for Computing Machinery. Accessed May 17, 2023. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[18] W. Conklin, and M. Bishop, "Contrasting the CSEC 2017 and the CAE Designation Requirements." Core. Accessed May, 17, 2023. [Online]. Available: https://core.ac.uk/download/pdf/143481144.pdf

[19] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework." National Institute of Standards and Technology. Accessed: May 20, 2023. [Online]. Available: https://www.nist.gov/system/files/documents/2019/11/08/nist.sp_.800-181.pdf

[20] U. Clark, G. Stoker, and R. Vetter, "Looking Ahead to CAE-CD Program Changes," *Information Systems Education Journal*, vol. 18, no. 1, pp.29-39, 2020. Available: http://proc.iscap.info/2019/pdf/4920.pdf

[21] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity curriculum design: A survey," in *Transactions on Edutainment XV*, vol. 11345. Z. Pan, A. Cheok, W. Müller, M. Zhang, A. El Rhalibi, K. Kifayat, Eds. Berlin: Springer, 2019, pp. 93-107. Available: http://doi.acm.org/10.1145/1409908.1409918

[22] T. Aoyama, H. Naruoka, I, Koshijima, and K. Watanabe, "How management goes wrong? – The human factor lessons learned from a cyber incident handling exercise," *Procedia Manufacturing*, vol 3, pp.1082-1087, 2015. Available: https://doi.org/10.1016/j.promfg.2015.07.178

[23] R. Ait Maalem Lahcen, R. Mohapatra, and M. Kumar. (9-11 Jan. 2018). "Cybersecurity: A survey of vulnerability analysis and attack graphs," presented at the International Conference on Mathematics and Computing (ICMC), Varanasi, India. [Online]. Available:

https://doi.org/10.1007/978-981-13-2095-8_9

[24] A. I. Al-Darwish, and P. Choe, "A framework of information security integrated with human factors," in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Eds. Switzerland: Springer, 2019, pp. 217-229.

[25] G. C. Kessler, "Information security: New threats or familiar problems?" *Computer*, vol 45, no. 2, pp.59-65, 2012. Available: 10.1109/MC.2011.262

[26] A. Mammone, E. Godin, and B. Jenkins, *Mapping the extreme right in contemporary Europe*. London, UK: Taylor & Francis, 2012.

[27] S. von Mering, and T. W. McCarty, *Right-Wing Radicalism Today: Perspectives from Europe and the US*. London, UK: Routledge, 2013.

[28] R. A. Wilson, and M. K. Land, "*Hate speech on social media: Content moderation in context."* Open Commons. Accessed Dec. 10, 2022. [Online]. Available: https://opencommons.uconn.edu/law_review/449/

[29] K. Jasko, G. LaFree, J. Piazza, and M. H. Becker, "A comparison of political violence by left-wing, right-wing, and Islamist extremists in the United States and the world," *Proceedings of the National Academy of Sciences*, vol. 119, no. 30, 2022. Available: 10.1073/pnas.2122593119

[30] S. E. Reid, and M. Valasik, *Alt-right gangs: A hazy shade of white*. First ed. Berkeley, CA: University of California Press, 2020.

[31] H. Schulze, J. Hohner, S. Greipl, M. Girgnhuber, I. Desta, and D. Rieger, "Far-right conspiracy groups on fringe platforms: a longitudinal analysis of radicalization dynamics on Telegra," *Convergence: The International Journal of Research into New Media Technologies*, vol. 28, no. 4, pp.1103-1126, 2022. Available: 10.1177/13548565221104977

[32] S. Chermak, J. D. Freilich, W. S. Parkin, J. Gruenewald, C. Mills, B., Klein, L. Dillon, and C. Duran, "Far-Right Extremist Violence in the United States" in *Right-Wing Extremism in Canada and the United States*, B. Perry, J. Gruenewald, R. Scrivens, Eds. Switzerland: Palgrave Macmillan, 2022, pp. 301-326.

[33] T. J. Holt, J. D. Freilich, S. M, Chermak, C. Mills, and J. Silva, "Loners, colleagues, or peers? Assessing the social organization of radicalization," *American Journal of Criminal Justice*, vol. 44, no.1, pp.83-105, 2019. Available: https://doi.org/10.1007/s12103-018-9439-5

[34] M. Conway, R. Scrivens, and L. McNair "Right-wing extremists' persistent online presence: History and contemporary trends." Doras. Accessed Nov. 10, 2022. [Online]. Available: https://doras.dcu.ie/23960/

[35] C. Alfieri, "Cryptocurrency and National Security," *International Journal on Criminology*, vol. 9, no. 1, pp. 21-48, 2022.

[36] K. Grauer, W. Kueshner, and H. Updegrave. "The 2022 crypto crime report." Chainanalysis. Accessed May 20, 2023. [Online]. Available: https://go.chainalysis.com/2022-crypto-crime-report.html

[37] Committee on Financial Services. "Dollars against democracy: Domestic terrorist financing in the aftermath of insurrection." Congress. Accessed May 21, 2023. [Online]. https://www.congress.gov/event/117th-congress/house-event/LC66044/text

[38] M. A. Argentino, J. Davis, and T. R. Hamming, "Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies," National Counterterrorism Innovation, Technology, and Education Center. Accessed: June 8, 2023. [Online]. Available: https://digitalcommons.unomaha.edu/nctereportsresearch/22?utm_source=digitalcommons.unomaha.edu%2Fnctereportsresearch%2F22&utm_medium=PDF&utm_campaign=PDFCoverPages

[39] Department of Justice, "Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Network." U.S. Department of Justice. Accessed May 21, 2023. [Online]. Available: https://www.justice.gov/cryptoreport

[40] A. Tsesis, "Social media accountability for terrorist propaganda." Fordham Law Review. Accessed: May 25, 2023. [Online]. Available: http://fordhamlawreview.org/wp-content/uploads/2017/10/Tsesis_November_v86.pdf

[41] K. Langvardt, "Regulating Online Content Moderation," *Georgetown Law Journal*, vol. 106, no. 5, pp.1353-1389, 2018. Available: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2018/07/Regulating-Online-Content-Moderation.pdf

[42] R. Gorwa, R. Binns, and C. Katzenbach, C. "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, vol. 7, no. 1, 2020. Available: https://doi.org/10.1177/2053951719897945

[43] N. Duarte, E. Llanso, and A. Loup, "Mixed messages? The limits of automated social media content analysis." Analysis & Policy Observatory. Accessed June 1, 2023. [Online]. Available: https://apo.org.au/node/240471

[44] T. Holt, "Introducing the International Interdisciplinary Research Consortium on Cyber crime (IIRCC)." Linkedin. Accessed Nov. 30, 2023. [Online]. Available: https://www.linkedin.com/pulse/introducing-international-interdisciplinary-research-consortium-holt/

[45] R. Gebauer, M. E. Wade, T. Muller, S. Kramer, M. Leary, and J. Sopper, "Unique Strategies to Foster Integrative Learning in Residential Learning Communities," *Learning Communities: Research & Practice*, vol. 8, no. 1, 2020.

[46] O. T. Lenning, and L. H. Ebbers, "The Powerful Potential of Learning Communities: Improving Education for the Future." *ASHE-ERIC Higher Education Report*, vol. 26, no. 6, 1999.

[47] V. Tinto, "Learning better together," in *Transitioning Students into Higher Education*, A. Jones, A. Olds, and J. G. Lisciandro, Eds. London, UK: Routledge, 2019, pp. 13-24.

[48] M. Dagley, M. Georgiopoulos, A. Reece, and C. Young, "Increasing retention and graduation rates through a STEM learning community," *Journal of College Student Retention: Research, Theory & Practice*, vol. 18, no. 2, pp.167-182, 2016. Available: https://doi.org/10.1177/1521025115584746

[49] A. Settle, and T. Steinbach. (3-6 Oct. 2018). Retention rates for the first three years of a linked-courses learning community. Presented at the 19th Annual Conference on Information Technology Education (SIGITE), Fort Lauderdale FL, USA. [Online]. Available: https://doi.org/10.1145/3241815.3241854

[50] G. Matthews-DeNatale, S. J. Blevins-Bohanan, C. G. Rothwell, and C. M. Wehlburg. "Redesigning learning: ePortfolios in support of reflective growth within individuals and organizations." Appalachian State University. Accessed December 5, 2022. [Online]. Available: https://aportfolio.appstate.edu/sites/aportfolio.appstate.edu/files/field_guide_to_eportfolio.pdf

[51] B. Melles, A. B. Leger, and L. Covell, "Tell Me about Yourself-Using ePortfolio as a Tool to Integrate Learning and Position Students for Employment, a Case from the Queen's University Master of Public Health Program," *Canadian Journal for the Scholarship of Teaching and Learning*, vol. 9, no. 3, pp.1-12, 2018. Available: https://doi.org/10.5206/cjsotl-rcacea.2018.3.9

[52] A. Alexiou, and F. Paraskeva, "Enhancing self-regulated learning skills through the implementation of an e-portfolio tool," *Procedia-Social and Behavioral Sciences*, vol. 2, no. 2, pp. 3048-3054, 2010. Available: https://doi.org/10.1016/j.sbspro.2010.03.463