Exploration of AI-enabled Contents for Undergraduate Cyber Security Programs

Ramoni O. Lasisi and **Matthew Menia** and **Zachary Farr** and **Corey Jones**
Department of Computer and Information Sciences
Virginia Military Institute, Lexington, VA
LasisiRO@vmi.edu, {meniamc20, farrzr22, jonescc22}@mail.vmi.edu

Abstract

This paper investigates the AI courses and/or topics that are needed to enhance cybersecurity education towards preparation of the future AI-enabled cybersecurity leaders. We found that, although sophisticated cyber crimes are now been perpetrated using AI technologies, AI courses and topics are currently missing in virtually all the undergraduate cybersecurity programs we reviewed.

Introduction

The increasing cyber threats, security breaches, and cyber-attacks on key network infrastructure today account for one of many organizations huge amount of loss - in terms of money, denial of services, privacy control compromise, and reputation costs (Dipankar et al. 2010). The global economy suffers a loss of about $400 billion every year due to cyber crimes (LI 2018). These threats are at scale as sophisticated cyber crimes are now been perpetrated using artificial intelligence (AI) technologies. The increase in sophistication of cyber attacks by many organizations has also recently necessitates the employment of AI as key tool to counter cyber-attacks (Capgemini 2019). There is thus the need to train cyber analysts and other security professionals to learn, understand, and be able to use AI-enabled cyber security technologies to address the continuity of cyber-attacks.

This research work investigates the AI contents (courses and topics) that are needed to enhance cyber security education at the undergraduate level and provide recommendations towards preparation of the future AI-enabled cyber security leaders and experts to be workforce-ready. In our preliminary work, we surveyed 24 undergraduate cyber security programs (Cyb 2020) in the US to understand their relevance to the state of the art and ensure that students are being prepared to be AI-enabled cyber security professionals or experts. Out of all the programs we surveyed, only one of them has in its curriculum a course in AI or AI-related topics. Furthermore, at this only institution, the AI course focuses on "explor[ing] the technologies used to construct computer-based agents that perceive, represent knowledge, search spaces, and learn." No mention of cyber security or its applications in cyber security is found in the course description.

See Figure 1 for a summary of distribution of contents taught in the 24 undergraduate cyber security programs we surveyed. AI contents and/or courses account for only about 4% of courses and topics taught among all the programs under study.

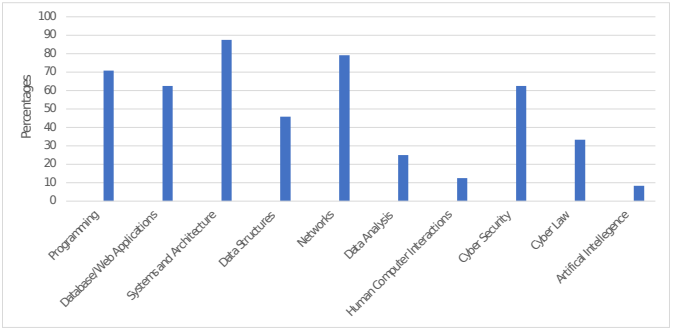

Figure 1: A summary of the distribution of contents taught in the 24 surveyed undergraduate cybersecurity programs in the US

Our working hypothesis is stated below:

The inclusion of AI courses or topics in the curricula of undergraduate cyber security programs, either by way of dedicated courses or AI modules in multiple classes will help students to learn how to use, develop, and integrate AI technologies in combating cyber attacks, and thus preparing them to be AI-enabled cyber security professionals or experts that are workforce-ready.

We reviewed several works at the intersection of AI and cybersecurity to provide background of the broad area of applications of AI in cybersecurity. We consider the dual field of beneficial and malicious AI, including how attackers use AI to carry out sophisticated cyber-attacks, that help in security improvement, testing assistance, security monitoring, social-engineering, attack undetectability, and making decision upon cyber-attacks (Szychter et al. 2018). Our aim is to provide expositions of issues that leverage AI in cybersecurity to aid in the development of AI-enabled contents, projects, experiments, and demonstrations that may lead to improvement in undergraduate cyber security curricula.

The following provides our main findings and/or contributions:

- We identify AI topics that are relevant to cybersecurity and currently missing in the curricula of the 24 programs we surveyed. We then generate an AI-Cybersecurity topics matrix that we have strong expectation will help in the preparation of AI-enabled contents for undergraduate cybersecurity program towards the level of AI sophistication in cybersecurity to meet today's cyber fields need
- We identify how attackers use AI and how to use AI to detect attackers' behavior in cyber security. Our idea is to provide some of these expositions to aid in developing AI-enabled experiments and projects in undergraduate cybersecurity curriculum
- Finally, we organized a half-day workshop tagged "Exploring AI-Enabled Cybersecurity" and invited stakeholders in the cybersecurity fields - students, professors, and practitioners, to present and receive feedback on our research findings

Artificial Intelligence in Cybersecurity

The application of AI in cyber security is spreading globally (Abbas et al. 2019). The cross fertilization of the broad field of AI including machine learning, deep leaning, multi-agent systems, game theory, and neural networks, with cybersecurity education at the undergraduate level is a needed approach to preparing students and getting them ready to solve the sophisticated problem of protecting the critical infrastructure around the world. AI is currently being applied in many fields including disaster response, medicine, automated vehicles and self-driving cars, economics, management, and business.

Keeping resources and information safe is a key concern in cybersecurity. Most traditional security uses guards, physical deterrents, and static control of devices such as firewalls and intrusion detection systems (LI 2018). Now more than ever we are seeing different vulnerabilities that advances in technology have created in personal and shared resources. Adversaries have also made advances in new technologies, and no longer are passive defense methods effective against new cyber threats. To get ahead of attacks of this sophistication, there is the need for intelligent methods, techniques, and procedures that provide adaptive security, management, and controls to overcome such attacks (LI 2018). A possible solution among others is the employment of AI to combating Cyber threats. Cyber crimes have presented a new set of problems for security experts. The proliferation of information technology has also provide platforms for the globalization of these crimes by making countries borderless. Thus making monitoring, detecting, and preventing intrusions increasingly difficult to manage. Varying definitions of cybercrime show just how adaptable today's security must be. Security systems need to change to meet the needs of their environment.

Cyber security methodologies are constantly adapted to counter known assaults. Due to their lack of flexibility, security frameworks typically cannot change to encompass new domains without a slow and insufficient human element. AI techniques can help improve deficiencies of today's cyber security tools due to their flexibility and adaptability (Anwar and Hassan 2017).

What follows give some examples of applications areas of AI in cybersecurity (Dilek, Çakır, and Aydın 2015; Anwar and Hassan 2017; LI 2018) :

- In large scale DDoS attack, botnets and worm infections can be a big problem for dynamic networks. Intelligent agents are adaptable and effective for combating these kind of cyber-attacks. For example, in a multi-agent setup, interaction among individual agents allows for adjustment of their configurations and behaviors according to the conditions of their environment and the severity of an attack. Intelligent agents are self sufficient and good at communicating with other agents, sharing knowledge, and coordinating reactions. These are utilized in resistance against DDoS attacks due to their synergistic nature, allowing a coordinated response to an attack
- Intrusions often do not present themselves as an immediate threat. Fuzzy logic/sets help in making decisions with incomplete or inconclusive data. They have capability to categorize possible threats with high probability of being a threat or not. Through genetic algorithms and fuzzy logic, threat detection systems are made to be more accurate as the system will learn what is abnormal and what is normal over time, alerting humans or software once something has been found to be abnormal, allowing it to be stopped in its tracks or allowed to pass through
- The diversity of cyber threats has rendered conventional fixed algorithms ineffective. Artificial immune systems (AIS) are adaptable and can be used to combat dynamically evolving cyber threats. AIS are capable of detecting an intruder, learning about it, and becoming immune to it and other similar threats
- Artificial neural networks are good at learning about patterns and making decisions. They can learn about patterns of attacks and threats over time and can detect and/or report an intrusion with little or no false positives. They are also good at DoS identification, malware classification, spam recognition, zombie detection, and computer worm identification due to their pattern recognition ability. This ability makes them important in detecting abnormal or malicious behaviors in cyber environments
- Unsupervised learning can be used to comb through large amounts of data, such as log files. Supervised learning while adding hash functions to training data could allow data to stay secure, and as well detect data tampering based on the hash functions

Relevant AI Topics to Cyber Security Undergraduate Curriculum

Our literature review to identify AI topics that match those of cyber security reveals interesting topics across the two fields. We summarize our findings in the following AI-cyber security matrices with relevant topics in AI matched with topics in cybersecurity.

AI/Cyber Security Topics	Authenticity, Confidentiality, and Integrity of Data	Data Breaches	Network Security	Cloud Security	Internet of Things	Ethical Hacking	Common Attacks	Intrusion Detection	Zero Day Attacks
Reinforcement Learning	x	x	x	x	x		x	x	x
Supervised Learning	x	x	x	x	x	x	x	x	x
Unsupervised Learning	x		x	x			x	x	x
Convolutional Neural Network			x			x	x	x	
K Nearest Neighbor				x	x		x	x	x
Decision Trees		x	x	x	x	x	x	x	x
SVM		x	x	x			x	x	x

Figure 2: AI-Cyber Security Topics Matrix 1

AI \Cyber Security Topis	Network Security	Forensic Investigations	Fraud Detection	Cryptography	DDoS Attacks	Spam Detection	Intrusion Detection and Prevention Systems
Neural Nets	x	x	x	x	x	x	x
Expert Systems	x	x	x	x		x	x
Machine Learning	x		x	x	x	x	x
Genetic Algorithms/Fuzzy Logic	x			x			
Unsupervised Learning	x		x				
Intelligent Agents	x		x	x	x		x
Data Mining	x	x	x	x		x	x
Pattern Recognition	x	x	x	x	x	x	x

Figure 4: AI-Cyber Security Topics Matrix 3

AI \Cyber Security Topics	Cyber Threat Intelligence	Disinformation and Computational Propaganda	Security Operations Centers	Cryptography	Fraud Detection	Intrusion Detection	Network Security	Integrated Security Approach
Artificial Immune Systems			x		x	x	x	x
Artificial Neural Networks	x	x	x	x	x	x	x	x
Genetic Algorithms			x	x	x	x	x	x
Intelligent Agents	x	x	x	x	x	x	x	x
Expert Systems	x	x	x	x	x	x	x	x
Fuzzy Sets	x	x					x	
Machine Learning	x	x	x	x	x	x	x	x

Figure 3: AI-Cyber Security Topics Matrix 2

There are several possible topics in both AI and cybersecurity to consider in completing the categorization in the three matrices above. For example, in Figure 2, i.e., AI-Cyber Security Topics Matrix 1, we considered the following cybersecurity topics: CIA (Confidentiality, Integrity, and Authenticity of Data), Data Breaches, Network Security, Cloud Security, Internet of Things, Ethical Hacking, Common Attacks, Intrusion Detection, and Zero Day Attacks. Many of these topics are central to many cybersecurity courses.

The AI topics in the matrices are some of the most often referenced topics in many of the literature we reviewed. See for example, (Depren et al. 2005; Sedjelmaci and Senouci 2016; Hendrix, Al-Sherbaz, and Bloom 2016). These topics have the potential to provide security for user's data and systems, as well as potential to launch attacks on systems. We provide applications of AI topics in Figure 2 as they apply to cybersecurity problems, thus informing the suggested matching in the AI-Cyber Security Topics Matrix 1.

- Using k-Nearest Neighbor to isolate features of a zero-day attack and in conjunction with SVM to detect where the attack was initiated
- Using artificial neural networks and self-organizing maps to determine a new type of attack and then develop rules to detect the attack when used in another system
- Using decision trees to predict logical moves that an attacker might make if the attacker has already gained access to a system. This could prove essential to stopping the attack before big damages are caused
- Decision trees are also used to determine if an event is an attack or not since they have capabilities to detect anomalies due to the rules that are created during training with sample data sets
- Supervised learning and neural networks are used to detect intrusion in personal systems and cloud infrastructure. The AI could deploy immediate defensive actions while the admin is alerted to respond to the incident
- Unsupervised learning could be used to detect DoS attacks, and as well as phishing attacks so that the defenders could determine different features of the phishing emails, tag them, and then prevent them from reaching targeted users, thus keeping them safe
- Convolutional neural networks are used to classify the direction and how attacks work with a zero-day attack

Similar applications can be completed among the AI and cybersecurity topics in matrices 2 and 3.

AI-enabled Projects for Undergraduate Cybersecurity Program

We propose a general discussion on possible projects ideas based on the different AI topics illustrated earlier. We situate our projects ideas around attackers' view, behavior, and use of AI in cybersecurity.

How attackers use AI

Attackers are able to use AI to support their attacks, and in some cases attacks could be conducted autonomously. There are different options that could be paired to create a successful attack where the user would not need to do anything other than point an AI in a direction and wait for the results of an attack to be delivered to the user. Some examples of this application could begin with training a machine learning model by adding data from penetration testing of a system so that the model could learn where to search for vulnerabilities that may be used to gain access. After this step a decision tree could be made that lists the steps to gain access to the system when certain weaknesses are found. From here you can have the AI penetrate the system, then remain dormant, and finally begin to send messages to the user to do malicious functions on the attacked system. Attackers could also use an AI to monitor a system. In this case, the AI would be expected to gain access to the system as before and apply a simple key logger to the computer so that when users attempt to log in, their credentials are collected for the attacker to use at a later time.

How to use AI to detect attackers' behavior

There are different AI options users can use to detect different attacks being launched by an attacker. The user could implement an AI that use unsupervised learning to detect patterns in some data that has been collected in the network traffic to detect a possible attack pattern. The user could also pair this idea with some supervised learning that is trained to detect known attacks and then will work to combat the attack by launching a DoS attack or other attacks that will isolate the attackers AI. Users can then be notified so that they may launch the proper steps to terminate this threat to the system. Users may also adapt AI search algorithms to view paths that may lead to sensitive data. This could then be combined with monitoring the network traffic and a decision tree could lead to important information that a suspicious user is attempting to reach.

The issue now is to then design experiments around these general projects backgrounds that fit undergraduate cybersecurity curriculum.

Evaluation

To provide initial evaluation and validation of our research proposal, idea, and preliminary findings, we organized a workshop tagged "Exploring AI-Enabled Cybersecurity," and invited stakeholders in the field, comprising of students, professors, and practitioners. We presented the gap of the missing AI topics and/or contents as noted in the 24 undergraduate cybersecurity programs we surveyed. This was followed by the presentation of our hypothesis as stated in the Introduction section. Finally, we presented our preliminary findings from the extensive literature review of articles at the intersection of AI and cybersecurity.

Feedbacks from participants at the workshop provide a general interest in the proposed problem, and also suggest the need to address the problem by developing AI-enabled contents that will support a cybersecurity course of the present time, where sophisticated cyber crimes are now been perpetrated using AI technologies. There is thus that common understanding of the need to prepare AI-enabled cybersecurity professionals or experts that are workforce-ready.

Conclusions and Future Work

Findings reported in this paper are at preliminary stage. The outcomes of this interdisciplinary research in AI and cybersecurity are expected to have a high positive impact on cybersecurity education in our society. The successful completion of the research is expected to provide a new frontier in AI-enabled cybersecurity education and resources that benefit the academic community. The expected outcomes will aid faculty in the teaching of cybersecurity in schools, and also assist students in their projects, research works, and get them prepared for cybersecurity workplace readiness.

References

Abbas, N. N.; Ahmed, T.; Shah1, S. H.; Omar, M.; and Park, H. W. 2019. Investigating the applications of artificial intelligence in cyber security. *Scientometrics* 121.

Anwar, A., and Hassan, S. I. 2017. Applying artificial intelligence techniques to prevent cyber assaults. *International Journal of Computational Intelligence Research* 13(5).

Capgemini. 2019. Reinventing cybersecurity with artificial intelligence - a new frontier in digital security. *Capgemini Research Institute Report*.

2020. 25 best bachelor's in cybersecurity degree programs for 2020. *https://www.bachelorsdegreecenter.org/best-cybersecurity-degrees*.

Depren, O.; Topallar, M.; Anarim, E.; and Ciliz, M. K. 2005. An intelligent intrusion detection system (ids) for anomaly and misuse detection in computer networks. *Expert Systems Applications* 29(4).

Dilek, S.; Çakır, H.; and Aydın, M. 2015. Applications of artificial intelligence techniques to combating cyber crimes: a review. *International Journal of Artificial Intelligence & Applications* 6(1).

Dipankar, S. S.; Vivek, D.; Roy, S. S.; Ellis, C.; and Wu, Q. 2010. A survey of game theory as applied to network security. In *Proceedings of the 43rd Hawaii International Conference on Systems Sciences*.

Hendrix, M.; Al-Sherbaz, A.; and Bloom, V. 2016. Game based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games* 3(1).

LI, J. 2018. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*.

Sedjelmaci, H., and Senouci, S. M. 2016. Smart grid security: A new approach to detect intruders in a smart grid neighborhood area

Szychter, A.; Ameur, H.; Kung, A.; and Daussin, H. 2018. The impact of artificial intelligence on security: A dual perspective.