Electronics, Communications and Networks
A.J. Tallón-Ballesteros et al. (Eds.)

doi:10.3233/FAIA231181

Essentials for Developing an Educational Course in Artificial Intelligence in Cybersecurity for Managers

Dimiter VELEV[a,1] and Plamena ZLATEVA[a,b]
[a] *University of National and World Economy, Sofia, Bulgaria*
[b] *Institute of Robotics, Bulgarian Academy of Sciences, Sofia, Bulgaria*

Abstract. In recent years, cybersecurity threats have become more sophisticated and they have the tendency to be hard to detect and prevent. This has led to a growing interest in the use of Artificial Intelligence (AI) in cybersecurity. However, the adoption of AI in cybersecurity also raises concerns about the risks and ethical implications associated with its use. The aim of the paper is to reveal the potential benefits and challenges of AI in cybersecurity, and also to propose an educational course in AI in Cybersecurity for managers, who should be aware of current developments in this sensitive field.

Keywords. Cybersecurity, Artificial intelligence, Machine learning, Deep learning, Educational course, Managers

1. Introduction

The current state of cybersecurity can be described in the rise of cybersecurity threats and attackers using increasingly advanced tactics and techniques to gain access to sensitive information and systems. Some of the most common cybersecurity threats today include ransomware, phishing, malware and social engineering attacks. On the other hand, cybersecurity professionals and ITC developers try constantly to stay ahead of such threats by developing new tools, techniques and best practices to protect networks systems and data. This also includes the use of Artificial Intelligence (AI) algorithms to detect and respond to threats in real-time. In other words, current state of cybersecurity can be characterized as an ongoing "arms race" between cybercriminals and cybersecurity professionals. The cybersecurity landscape will become even more complex and challenging in the years to come as technologies continue to advance and develop.

Cybersecurity has become increasingly important as more and more of people's lives are conducted online. This type of activity generates large volumes of sensitive data, which is being stored and transmitted over digital networks. Therefore, there is a growing need for robust cybersecurity measures to protect against cyber threats. Of utmost importance is to educate especially managers of organizations to not only to understand the AI basics, but also to know how to handle cybersecurity threats with this technology.

[1] Corresponding author: Dimiter Velev, University of National and World Economy, 19 December 8th Str., 1700 Sofia, Bulgaria; E-mail: dgvelev@unwe.bg.

The aim of the paper is to reveal the potential benefits and challenges of AI in cybersecurity, as well as to propose an educational course in AI in cybersecurity for managers, who should be aware of current developments in this field.

2. Challenges of Cybersecurity

Cybersecurity refers to the protection of digital devices, networks and information systems from unauthorized access, damage or disruption. It involves the use of technologies, processes and policies to safeguard digital assets from cyber threats. Cybersecurity professionals work to identify and mitigate security risks, develop security protocols and policies, and monitor networks and systems for signs of unauthorized activity. They also conduct regular security assessments and tests to identify vulnerabilities and ensure that security measures are up to date and effective.

A cyber threat refers to any malicious or unauthorized activity that is intended to disrupt, damage, steal, or gain unauthorized access to computer systems, networks, or digital devices. Cyber threats can take many forms, such as computer viruses, malware, phishing attacks, ransomware, and denial-of-service attacks. Cyber threats are a growing concern for individuals, businesses, and governments as our reliance on digital technology increases. These threats can result in the theft of sensitive data, financial loss, damage to reputation, and even physical harm. Cyber threats can come from a variety of sources, including cybercriminals, hacktivists, nation-state actors, and insider threats. These threats can be motivated by financial gain, political or ideological motives, or simply the desire to cause harm or disruption.

Cyber threats can be classified into several categories depending on their characteristics and the type of damage they can cause [1, 2]:

- Malware refers to any software that is designed to harm, steal, or spy on a computer system. Malware can take many forms, such as viruses, Trojans, worms, and spyware.
- Phishing is a type of social engineering attack where an attacker tries to trick a user into giving up sensitive information, such as login credentials or financial data, by posing as a trustworthy entity.
- Ransomware is a type of malware that encrypts a victim's files or locks their computer and demands a ransom payment in exchange for the decryption key or unlock code.
- Denial-of-service (DoS) attacks are designed to overwhelm a computer system or network with traffic, making it unavailable to legitimate users.
- Advanced persistent threats (APTs) are long-term, targeted attacks that are typically carried out by nation-state actors or other well-funded and organized groups. APTs are designed to remain undetected for extended periods and can involve a combination of techniques, such as malware, social engineering, and insider threats.
- Insider threats refer to threats that come from within an organization, such as employees or contractors who have access to sensitive data or systems. Insider threats can be intentional, such as theft or sabotage, or unintentional, such as the accidental disclosure of sensitive information.

The current state of cybersecurity is complex and rapidly evolving. While advances in technology have brought many benefits, they have also created new opportunities for cyber criminals and other malicious actors to exploit vulnerabilities in computer systems and networks. Here are some key aspects of the current state of cybersecurity [3 - 6]:

- Increasing Sophistication of Cyber Attacks are becoming increasingly sophisticated and targeted, making them harder to detect and prevent. Cyber criminals are using advanced techniques such as AI to evade traditional security measures and identify new vulnerabilities.
- Proliferation of Connected Devices - the Internet of Things (IoT) has led to numerous connected devices, which present new challenges for cybersecurity. Many of these devices lack strong security controls, making them vulnerable to cyber attacks.
- Data Breaches occur when unauthorized individuals gain access to sensitive data, such as personal information or financial data. These breaches can lead to significant harm, including identity theft, financial loss, and reputational damage.
- Compliance Issues - many industries are subject to regulatory compliance requirements related to cybersecurity. Failure to comply with these regulations can result in fines, legal action, and reputational damage.
- Cybersecurity Workforce Shortages - there is a significant shortage of cybersecurity professionals with the necessary skills and qualifications to meet the growing demand for cybersecurity expertise. This shortage creates challenges for organizations seeking to hire and retain skilled cybersecurity personnel.
- International Cybersecurity Cooperation: Cybersecurity is a global issue, and requires international cooperation to be effective. Cooperation is required to share information on emerging threats, develop common standards and protocols, and coordinate responses to cyber-attacks.
- Cybersecurity Measures - organizations implement a range of cybersecurity measures, including firewalls, intrusion detection and prevention systems, antivirus software, encryption, access controls, and user training and awareness programs.
- Heightened Regulatory Requirements related to cybersecurity are becoming increasingly stringent, with new regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. Organizations that fail to comply with these regulations may face significant fines and legal action.
- Emergence of New Threats are constantly evolving, with new threats emerging on a regular basis.
- Increasing Focus on Risk Management - organizations are increasingly focusing on risk management as a key component of cybersecurity. This involves identifying and prioritizing cybersecurity risks, and developing strategies to mitigate those risks.
- Cybersecurity Challenges - cyber threats continue to evolve and become more sophisticated. Cybersecurity professionals face the challenge of keeping up with the latest threats and developing effective strategies to protect against them.
- Importance of Cybersecurity has become an essential part of modern life. Protecting digital assets and data is critical to safeguarding privacy, maintaining

trust in online transactions, and ensuring the continued growth of the digital economy.

- Growing Cybersecurity Skills Shortage - there is a growing shortage of cybersecurity professionals with the necessary skills and qualifications to protect against cyber threats. This shortage is creating challenges for organizations seeking to hire and retain skilled cybersecurity personnel.
- Cybersecurity Careers - Cybersecurity is a growing field, with many job opportunities available for those with the necessary skills and qualifications. Careers in cybersecurity include roles such as cybersecurity analyst, information security specialist, penetration tester, and security consultant.

Defending against cyber threats requires a multi-layered approach that includes technical solutions such as firewalls, antivirus software, and intrusion detection systems, as well as employee training and awareness programs. It is also important to stay tuned with the latest threats and vulnerabilities and to regularly review and update security policies and procedures to address emerging threats. It is important to implement a comprehensive cybersecurity strategy that includes regular security assessments, employee training, and the use of security technologies such as firewalls, antivirus software, and intrusion detection systems. Organizations should also have an incident response plan in place to quickly respond to and mitigate the impact of cyber-attacks.

3. Artificial Intelligence in Cybersecurity

Artificial Intelligence refers to the simulation of human intelligence in machines that are programmed to think and act like humans. AI involves developing intelligent algorithms and models that can perform tasks that usually require human intelligence such as reasoning, learning, and decision-making [7].

Machine Learning (ML) is a subset of AI that involves developing algorithms that can automatically learn from data without being explicitly programmed. ML algorithms learn from data and improve their performance on a specific task by identifying patterns and relationships in the data [8].

Deep Learning (DL) is a subfield of ML that involves using artificial neural networks to develop complex models capable of learning from large amounts of data. DL algorithms can learn to identify patterns and features in data that are not easily detected by traditional machine learning algorithms, making them particularly useful for tasks such as image recognition, speech recognition, and natural language processing [9].

AI, ML, and DL are interconnected and form a hierarchy of complexity. AI is the broadest term that encompasses all techniques, methods, and approaches used to create intelligent machines that can perform human-like tasks. ML is a subset of AI that focuses on training algorithms to learn from data without being explicitly programmed [10].

In general, AI refers to machines that can mimic human intelligence, ML is a technique that allows machines to learn from data, and DL is a specific type of ML that uses artificial neural networks to learn complex patterns and relationships in large datasets.

AI is a powerful technology that can be used to enhance cybersecurity measures, but it can also be used to create new cybersecurity threats.

3.1. AI-powered Malware

Cybercriminals can use AI-powered malware to evade detection and improve its effectiveness. Malware is software that is designed to disrupt, damage or gain unauthorized access to a computer system or network. AI-powered malware uses ML algorithms to automatically adapt to changes in a system's defenses and to identify new vulnerabilities that can be exploited [11].

A frequent case of AI-powered malware is a Trojan horse program that uses AI to evade detection by traditional antivirus software. The malware is programmed to analyze the behavior of the antivirus software and to modify its own behavior to avoid detection. This makes the malware more difficult to detect and remove, and it can potentially remain undetected for long periods of time.

Another example is a phishing attack that uses AI to create convincing emails or messages that are tailored to the victim's interests or preferences. The AI analyzes data from social media and other sources to build a detailed profile of the victim, which then is used to prepare personalized messages that are more likely to be effective.

AI-powered malware can also be used to automate the process of identifying vulnerabilities in computer systems and networks. A botnet can be programmed to use machine learning algorithms to scan for vulnerabilities in a network and to exploit them automatically. This can significantly increase the speed and effectiveness of cyber-attacks.

AI-powered malware is a growing threat that can evade traditional security measures and adapt to changes in a system's defenses. It is important for organizations to implement strong cybersecurity measures, such as firewalls, intrusion detection systems, and regular security assessments, to mitigate the risk of AI-powered cyber-attacks.

3.2. AI Adversarial Attacks

AI Adversarial Attacks refer to techniques used to manipulate ML algorithms by exploiting their vulnerabilities. These attacks involve introducing small changes to input data that can cause the algorithm to make incorrect predictions or classifications [12].

Adversarial attacks work by exploiting the fact that ML algorithms are trained on large datasets to learn patterns and features that are used to make predictions or classifications. By making small changes to input data, attackers can create images or other types of input that appear normal to humans, but that the ML algorithm misinterprets.

Examples of AI Adversarial Attacks include:

- Image manipulation - attackers can modify images in such a way they are misclassified by a ML algorithm. Adding small imperceptible changes to an image of a stop sign, an attacker can trick an autonomous vehicle's image recognition system into interpreting it as a speed limit sign.
- Text manipulation - attackers can modify text data in ways that can trick ML algorithms into making incorrect predictions or classifications. Introducing small changes to a spam email, attackers can evade spam filters and deliver the message to the intended victim.
- Voice manipulation - attackers can modify audio data to create voice commands that are misinterpreted by ML. An attacker can create an audio recording that

is misinterpreted by a voice recognition system, causing it to execute a command that the user did not intend.

Adversarial attacks can pose a significant threat to the security of ML algorithms, particularly in areas such as autonomous vehicles, cybersecurity, and biometric authentication. It is important for researchers and practitioners to develop methods for detecting and mitigating the impact of adversarial attacks on ML algorithms.

3.3. AI Data Poisoning

Data poisoning is a type of cyber-attack in which the attacker intentionally introduces malicious data into a system's training data set with the aim of compromising the integrity of the model that is built using that data. The goal of this attack is to undermine the accuracy of the ML model so that it produces incorrect or misleading results [13].

Data poisoning attacks can be carried out in various ways, including:

- Injecting false data - the attacker can insert false or misleading data into a training dataset in order to bias the ML model towards making incorrect predictions or classifications.
- Modifying existing data - the attacker can modify the values of existing data in a training dataset, making it more difficult for the ML algorithm to learn the correct patterns.
- Selective sampling - an attacker can selectively choose which data to include in a training dataset, with the aim of influencing the ML model to make incorrect predictions or classifications.

Data poisoning can be particularly effective because it can be difficult to detect and can have a long-lasting impact. If an attacker can introduce poisoned data into a training dataset, the resulting model can be used to make incorrect predictions or classifications for a long period of time.

Defending against data poisoning attacks requires a combination of strategies, including careful data management, robust data validation techniques, and continuous monitoring of ML models for signs of tampering. ML models should also be trained on diverse datasets to reduce the risk of data poisoning attacks. Data poisoning attacks are a growing concern in the AI field, and researchers are actively working to develop new techniques to detect and mitigate the impact of these attacks.

As AI and ML continue to be integrated into a wide range of applications, the risk of data poisoning attacks is expected to grow. It is essential for researchers, practitioners, and policymakers to remain vigilant and work together to develop effective strategies for detecting and mitigating the impact of these attacks.

3.4. AI Deepfakes

AI Deepfakes refer to realistic images, videos or audio that are created using AI algorithms [14]. These creations are often used to manipulate or deceive people by making it appear as if someone said or did something that they did not. Deepfake technology works by using ML algorithms to train a computer program to identify patterns and features in data sets of images, videos, and audio. Once trained, the program can generate new content that looks, sounds or appears very similar to the original.

AI Deepfakes can be used for various purposes, including entertainment, political propaganda, and cybercrime. Malicious actors could use deepfake technology to create convincing phishing attacks, impersonate public figures or business leaders, or manipulate the stock market by spreading false information.

Deepfakes pose a significant threat to individuals and organizations, as they can be used to spread misinformation and to manipulate public opinion. It is important for individuals and organizations to be aware of the risks posed by deepfakes and to take steps to verify the authenticity of content before sharing or acting on it. Additionally, researchers and policymakers are working to develop methods for detecting and mitigating the impact of deepfakes on society.

3.5. AI-based Social Engineering

AI-based social engineering is a type of cyber-attack that involves using AI techniques to manipulate people into divulging sensitive information or performing actions that are harmful to their organization [15]. Social engineering attacks have been around for many years, but the use of AI techniques has made them more sophisticated and effective.

AI-based social engineering attacks can take many forms, but they generally involve the use of AI-powered chatbots, voice assistants, or other intelligent agents to communicate with the victim. These agents are designed to mimic human behavior and interact with the victim in a natural and convincing way.

Examples of AI-based social engineering attacks include:

- Phishing - attackers can use AI-powered chatbots to send phishing emails or messages to potential victims. The chatbots can be programmed to mimic the language and tone of the organization they are impersonating, making it more difficult for the victim to detect the attack.
- Vishing - attackers can use AI-powered voice assistants to make voice calls to potential victims. The voice assistants can be programmed to mimic the voice of a trusted person or organization, making it more likely that the victim will divulge sensitive information.
- Impersonation - attackers can use AI-powered chatbots or voice assistants to impersonate a trusted person or organization in order to gain access to sensitive information or perform unauthorized actions.

AI-based social engineering attacks can be difficult to detect and defend against, as the intelligent agents used in these attacks can adapt their behavior in real-time based on the victim's responses. However, there are some strategies that organizations can use to reduce the risk of these attacks, such as implementing strong authentication measures and educating employees about the risks of social engineering attacks. AI-powered security solutions can be used to detect and prevent these attacks by analyzing patterns of behavior and identifying anomalies that may indicate an attack is underway.

Another challenge of defending against AI-based social engineering attacks is that they often exploit human emotions and biases, such as trust, fear, and urgency. The attacker may use an AI-powered voice assistant to impersonate a trusted authority figure, such as a CEO or government official, in order to gain access to sensitive information or perform unauthorized actions.

To defend against AI-based social engineering attacks, organizations can take several steps:

- Educating employees about the risks of social engineering attacks, including the use of AI-powered agents.
- Implementing strong authentication measures, such as two-factor authentication, to reduce the risk of unauthorized access.
- Monitoring network traffic and user behavior to detect unusual patterns of activity that may indicate an attack is underway.
- Using AI-powered security solutions, such as anomaly detection and behavior analysis tools, to detect and prevent attacks.

AI-based social engineering attacks represent a growing threat to organizations, and defending against these attacks requires a multi-layered approach that incorporates both technical and human-focused defenses.

3.6. AI Autonomous Cyber Attacks

AI Autonomous Cyber Attacks, also known as fully automated cyber-attacks, refer to attacks that are carried out by AI systems without any human intervention [16]. In these attacks, the AI system is programmed to identify vulnerabilities in a target system, develop attack strategies, and execute those strategies on its own.

AI autonomous cyber-attacks are becoming increasingly sophisticated and pose a significant threat to organizations. These attacks can be carried out at a much faster pace and with greater efficiency than traditional cyber-attacks, and they can continue to evolve and adapt over time.

There are several types of AI autonomous cyber-attacks [17]:

- Automated vulnerability scanning - AI systems can be programmed to scan target systems for vulnerabilities, such as unpatched software or weak passwords, and then launch automated attacks to exploit those vulnerabilities.
- Automated malware generation - AI systems can be used to generate new malware variants that are designed to evade traditional anti-virus and anti-malware tools. These systems can also generate targeted attacks that are tailored to specific organizations or individuals.
- Automated phishing attacks - AI systems can be used to generate convincing phishing emails or messages that are designed to trick users into divulging sensitive information or downloading malware.
- Automated DDoS attacks - AI systems can be used to launch distributed denial-of-service (DDoS) attacks that can overwhelm target systems with traffic and cause them to crash.

Defending against AI autonomous cyber-attacks requires a multi-layered approach that incorporates both technical and human-focused defenses. Effective measures should be [18]:

- Regular vulnerability assessments and penetration testing to identify and remediate weaknesses in their systems.
- Implementing robust access control and authentication measures to prevent unauthorized access.
- Using AI-powered security tools to monitor network traffic and detect unusual activity.

- Educating employees about the risks of cyber-attacks and the importance of maintaining good cyber hygiene.

One of the main challenges of defending against AI autonomous cyber-attacks is that they can evade traditional security measures, such as signature-based antivirus software and rule-based intrusion detection systems. This is because AI systems are able to identify and exploit vulnerabilities that are not previously known.

AI autonomous cyber-attacks represent a significant threat to organizations, and defending against these attacks requires a comprehensive and proactive approach that incorporates both technical and human-focused defenses.

4. The need for managers to take an educational course in AI in cybersecurity

To address all AI issues in cybersecurity, organizations should ensure that they have appropriate processes and tools in place to monitor and evaluate the performance of AI algorithms. They should also prioritize transparency and interpretability in AI algorithms and ensure that they are trained on diverse and unbiased data. Organizations should also carefully consider the potential risks and limitations of AI before deploying it for cybersecurity purposes. An educational course in AI in cybersecurity for managers can provide valuable knowledge and skills for managers who are responsible for ensuring the security of their organization's systems and data [19].

There are several other reasons why managers in the cybersecurity field should consider taking an educational course in AI [20, 21]:

- Understanding the competitive landscape - AI is becoming increasingly important in the field of cybersecurity, and organizations that do not keep up with the latest developments in AI may fall behind their competitors. By taking a course in AI in cybersecurity, managers can stay up-to-date with the latest trends and technologies and develop strategies that give their organizations a competitive edge.
- Developing a future-oriented mindset - AI is likely to play an increasingly important role in cybersecurity in the coming years. By taking a course in AI in cybersecurity, managers can develop a future-oriented mindset and be better prepared to navigate the rapidly changing technological landscape.
- Enhancing communication skills - Effective communication is essential in the cybersecurity field, particularly when it comes to explaining complex technical concepts to non-technical stakeholders. By taking a course in AI in cybersecurity, managers can improve their communication skills and be better equipped to explain the potential benefits and risks of AI to decision-makers in their organizations.
- Building a network of experts - Taking a course in AI in cybersecurity can provide managers with the opportunity to connect with other professionals in the field and build a network of experts. This can be valuable for sharing knowledge, exchanging ideas, and collaborating on projects.

Professionals who may benefit from taking an educational course in AI in cybersecurity can be grouped in the following manner [22 - 25]:

- Chief Information Security Officers (CISOs) are responsible for checking their organization's information security program. Taking a course in AI in cybersecurity can help CISOs understand how AI can be used to enhance their organization's threat detection and response capabilities and how to manage the risks associated with using AI.
- Security analysts are responsible for monitoring their organization's networks and systems for potential threats. A course in AI in cybersecurity can help security analysts understand how AI can be used to automate threat detection and response, enabling them to focus on more complex and high-level security tasks.
- Incident response teams are responsible for responding to security incidents and mitigating their impact. Taking a course in AI in cybersecurity can help incident response teams understand how AI can be used to enhance their ability to detect and respond to security incidents in real-time.
- Network administrators are responsible for managing and maintaining their organization's network infrastructure. A course in AI in cybersecurity can help network administrators understand how AI can be used to identify and respond to potential network security threats.
- Compliance officers are responsible for ensuring that their organization complies with relevant laws and regulations related to information security. Taking a course in AI in cybersecurity can help compliance officers understand the legal and regulatory implications of using AI in cybersecurity.
- Researchers who are interested in studying the intersection of AI and cybersecurity can benefit from taking a course in AI in cybersecurity to gain a deeper understanding of the field and its potential implications.

For a manager it is important to have a basic understanding of AI and its potential applications in cybersecurity. This includes understanding the basic concepts and terminology of AI, as well as the potential benefits and risks of using AI in cybersecurity. Managers do not necessarily need to have a deep technical understanding of how AI algorithms work, but they should have a general understanding of how AI can be used to automate threat detection and response, as well as the potential limitations and ethical concerns associated with AI. In addition, managers should have a good understanding of their organization's specific cybersecurity needs and the potential benefits and risks of using AI to address those needs. This may require working closely with technical experts, such as data scientists and security analysts, to ensure that the organization is implementing AI in a responsible and effective manner.

A manager in AI in cybersecurity would benefit from having a broad understanding of both AI and cybersecurity. Here are some key areas of knowledge that a manager in AI in cybersecurity should possess [26 - 28]:

- Artificial intelligence - the manager should have a good understanding of the AI fundamentals, including machine learning, natural language processing, and computer vision. They should also have a good understanding of the current state of AI technology, including its limitations and potential applications in cybersecurity.
- Cybersecurity – the manager should have a strong background in cybersecurity principles and practices, including threat analysis, risk management, and

incident response. They should be familiar with the latest trends in cybersecurity, including emerging threats and new technologies.

- Data science – the manager should be comfortable working with data and have a good understanding of data science principles and techniques. This includes skills in data modeling, data warehousing, data mining, and data analysis.
- Software engineering – the manager should have a good understanding of software engineering principles and practices, including software development methodologies, software testing, and software security. They should also be familiar with programming languages and software frameworks commonly used in AI, such as Python and TensorFlow.
- Business acumen – the manager should have strong business acumen and be able to make data-driven decisions based on the needs of the organization. They should be able to communicate effectively with other stakeholders, such as executives, customers, and employees.

Overall, a manager in AI in cybersecurity should have a broad range of knowledge and skills that encompass AI, cybersecurity, data science, software engineering, and business acumen. By possessing these skills, they can effectively lead and manage AI-based cybersecurity projects and ensure that they meet the needs of the organization.

5. The Course of Artificial Intelligence in Cybersecurity for Managers

Based on all discussions and inferences above, the current research propose the following educational course in AI in Cybersecurity for managers [29 - 32]:

Course Title: Artificial Intelligence in Cybersecurity

Course Description: This course will introduce managers to the applications of AI in the field of cybersecurity. The course will cover the fundamental concepts of cybersecurity and AI and how it can be used to identify and mitigate security threats.

Course Outline:

Module 1: Introduction to Cybersecurity

- Overview of Cybersecurity
- Types of Cyber threats
- Hardware and software for Cybersecurity

Module 2: Introduction to Artificial Intelligence in Cybersecurity

- Overview of AI and its applications in cybersecurity
- Understanding cybersecurity threats and challenges
- Overview of the cybersecurity landscape

Module 3: Machine Learning in Cybersecurity

- Introduction to machine learning and its applications in cybersecurity
- Types of machine learning algorithms
- Supervised, unsupervised and reinforcement learning
- Machine learning in threat detection and response

Module 4: Deep Learning in Cybersecurity

- Introduction to deep learning and its applications in cybersecurity
- Neural networks, convolutional neural networks, and recurrent neural networks
- Deep learning for malware detection and intrusion detection

Module 5: Natural Language Processing in Cybersecurity

- Introduction to natural language processing and its applications in cybersecurity
- Techniques for natural language processing
- NLP for threat intelligence and cybersecurity analytics

Module 6: Case Studies

- Real-world case studies of AI applications in cybersecurity
- Ethical and legal considerations in the use of AI in cybersecurity
- Future of AI in cybersecurity

Course Project: Students will work on a project to propose an AI-based security solution for a real-world cybersecurity problem. They should identify a security challenge and propose a machine learning or deep learning model to detect and mitigate the threat.

Prerequisites: To succeed in this course, managers should have a basic understanding of programming concepts and cybersecurity fundamentals. Experience with a programming language such as Python is recommended, but this is not obligatory. Managers who are interested in cybersecurity and AI will find this course particularly valuable.

Course duration: The number of academic hours for a course in AI in Cybersecurity can vary depending on the depth and breadth of the course content, the level of expertise of the intended audience and the learning objectives of the course. In general, a basic introductory course in AI in Cybersecurity may range from 20-30 academic hours, while a more advanced course that covers topics such as machine/ deep learning and adversarial attacks may range from 50-100 academic hours. It is important to note that the number of the academic hours is not necessarily the same as the duration of the course, as factors such as class size, teaching style, and the pace of learning can all affect the amount of time required to cover the material.

6. Learning Outcomes of the AI for Cybersecurity Educational Course

Educating managers in AI for cybersecurity aims to achieve specific learning outcomes, which should determine what the managers will know, understand and be able to do when they finish the course. The main achievements will include:

Strong Understanding of AI and Cybersecurity, where the managers will know the basic AI concepts and terminologies, as well as to understand the fundamentals of cybersecurity, including common threats, vulnerabilities and mitigation techniques.

Acknowledgment of AI role in Cybersecurity will help managers to recognize how AI can be utilized to enhance cybersecurity measures and understand the potential benefits and limitations of AI in cybersecurity.

Knowledge of AI-driven Cybersecurity Solutions will help managers familiarize with AI tools and technologies like machine learning, deep learning, neural networks and natural language processing and their relation to cybersecurity, as well as recognize common AI cybersecurity solutions, such as anomaly detection, phishing detection, automated threat intelligence.

Risk Assessment and Management will allow managers to evaluate the risks and benefits associated with deploying AI cybersecurity tools and to understand the issues of integrating AI into cybersecurity strategies.

Strategic Deployment and Resource Allocation will help managers know how to evaluate the suitability of AI solutions for specific cybersecurity challenges and to be able to make informed decisions on budgeting and resource allocation for AI cybersecurity campaigns.

Effective Communication will help managers to translate technical AI and cybersecurity concepts of into understandable terms for non-technical stakeholders and promote AI role in enhancing cybersecurity within the organization.

Continuous Learning and Adaptation will help managers recognize the evolving nature of both AI and cybersecurity and the need for continuous learning and adaptation and stay informed latest trends, challenges and solutions in AI cybersecurity.

The successfully completed course will have strong learning outcomes due to which, managers will be better prepared to lead their organizations in applying AI for cybersecurity to ensure protection of their data and information systems.

7. Conclusions

The application of AI in cybersecurity has the potential to revolutionize the way responsible persons can manage the detection and mitigation of cyber threats. AI can provide a more effective and efficient approach to cybersecurity. However, there are also potential risks and ethical implications associated with the use of AI in cybersecurity. It is important to address such challenges actively to ensure that the benefits of AI in cybersecurity are realized without compromising the security and privacy of digital systems. The role of the manager in the application of AI in Cybersecurity will undoubtedly become increasingly important, and it is essential that they should take at least an introductory educational course in AI in Cybersecurity. The proposed educational course could be regarded as a conceptual one. In future it could be extended with the key requirements, regulations, and recommendations derived from Cybersecurity Act (and Certification Schemes), AI Act, various directives, relevant and updated standards (ISO, ETSI, CEN, NIST), ENISA and ITU recommendations.

Acknowledgement

The research was supported by the Science Fund of the University of National and World Economy under the project “Development and Use of Artificial Intelligence in Education and Economy” (Grant No. NID NI 1/2021).

References

[1] DeFranco JF, Maley B. What every engineer should know about cyber security and digital forensics, CRC Press: 2022.
[2] Årnes A. Cyber investigations-A research based introduction for Advanced Studies, NY:Wiley; 2022.
[3] Ojula Technology Innovations. Cybersecurity Essentials - The Beginner’s Guide, Ojula Technology Innovations (OTI); 2022.
[4] Lefty I. The User's Guide to the Dark Web - Encyclopedia Cyberspacia - The 42nd and Final Encyclopedia Cyberspacia. January 23, 2023, https://leanpub.com/encyclopediacyberspacia
[5] Fischerkeller MP, Goldman EO, Harknet RJ. Cyber Persistence Theory - Redefining National Security in Cyberspace, Oxford University Press, UK; 2022.

[6] Gupta BB, Sheng M (Eds.). Machine Learning for Computer and Cyber Security - Principles, Algorithms, and Practices, CRC Press; 2019.
[7] Russel S, Norwig P (Eds.). Artificial Intelligence: A Modern Approach, Global Edition Pearson; 2021.
[8] Serrano LG. Grokking Machine Learning, Manning Publ. Co; 2021.
[9] Goodfellow- I, Bengio Y, Courville A. Deep Learning, The MIT Press; 2016.
[10] Liu ACC, Kin OM, Law I. Understanding Artificial Intelligence-Fundamentals and Applications, Wiley-IEEE Press; 2022.
[11] Labaca-Castro R. Machine Learning under Malware Attack, Springer Vieweg, Wiesbaden; 2023.
[12] Chivukula AS, Yang X, Liu B, Liu W, Zhou W. Adversarial Machine Learning: Attack Surfaces, Defence Mechanisms, Learning Theories in Artificial Intelligence, Springer; 2023.
[13] Thakkar HK, Swarnkar M, Bhadoria RS (Eds.). Predictive Data Security Using AI: Insights and Issues of Blockchain, IoT, and DevOps. Springer; 2022.
[14] Abaimov S, Martellini M. Machine Learning for Cyber Agents: Attack and Defence, Springer;2022.
[15] Das R. Practical AI for Cybersecurity, CRC Press. 2021.
[16] Odayan K. Artificial Intelligence Controlling Cyber Security, KO, Independently published; 2021.
[17] Kamhoua CA, Kiekintveld CD, Fang F, Zhu Q (Eds.). Game Theory and Machine Learning for Cyber Security, Wiley- IEEE Press; 2021.
[18] Njenga K. Information Systems Security in Small and Medium-Sized Enterprises: Emerging Cybersecurity Threats in Turbulent Times, NOVA Science Publishers; 2022.
[19] Tagarev N. Role of Case Study Analyses in Education of Cybersecurity Management. Proceedings of the 13th Int. Multi-Conference on Society, Cybernetics and Informatics (IMSCI'2019), 2019; 1: p. 61-4.
[20] Allen G, Chan T. Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA; 2017.
[21] Tsado LK, Osgood R. Exploring Careers in Cybersecurity and Digital Forensics, Rowmann & Littlefield Publishers; 2022.
[22] National Security Commission on Artificial Intelligence. Final Report; 2021, https://www.nscai.gov/
[23] Horner C (Ed.). Cybersecurity in Business Valuation: Addressing the Impact of Data Breaches on Value. Business Valuation Resources, LLC, USA; 2020.
[24] Whitlock C, Strickland F (Eds.). Winning the National Security AI Competition: A Practical Guide for Government and Industry Leaders, Apress, CA, USA; 2022.
[25] Montasari R (Ed.). Artificial Intelligence and National Security, Springer; 2022.
[26] Gupta BB, Perez GM, Agrawal DP, Gupta D (Eds.). Handbook of Computer Networks and Cyber Security: Principles and Paradigms. Springer; 2020.
[27] Malik P, Nautiyal L, Ram M (Eds.) Machine Learning for Cyber Security. De Gruyter: Berlin; 2023.
[28] Ganapathi P, Shanmugapriya D. Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Advances in Information Security, Privacy and Ethics, IGI Global: USA; 2019
[29] Mueller JP. Machine Learning Security Principles. Packt Publishing; 2022.
[30] Sipola T, Kokkonen T, Karjalainen M (Eds.). Artificial Intelligence and Cybersecurity: Theory and Applications. Springer Cham, Switzerland; 2023.
[31] Wens C. ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. Independently published Deseo; 2019.
[32] Douglass R, Gremban K, Swami A, Gerali S (Eds.). IoT for Defense and National Security. Wiley-IEEE Press: NY, USA; 2023.