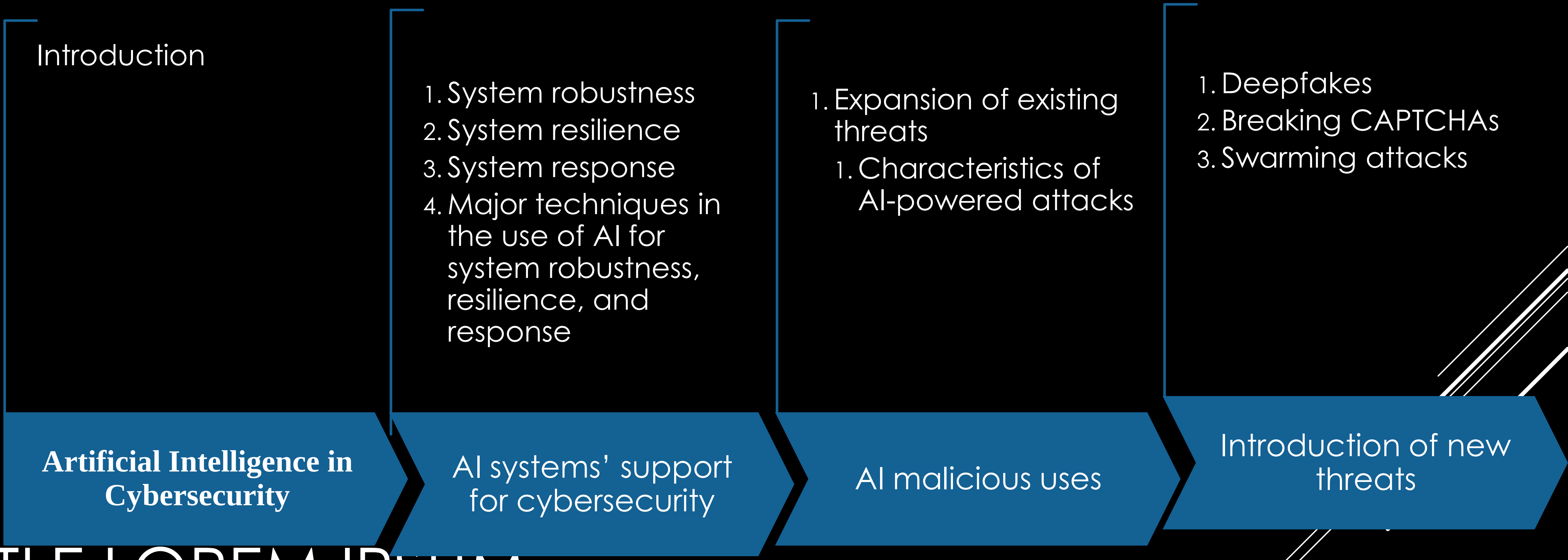
MODULE 2:

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY



Artificial Intelligence in Cybersecurity

Introduction

AI systems’ support for cybersecurity

1. System robustness
2. System resilience
3. System response
4. Major techniques in the use of AI for system robustness, resilience, and response

AI malicious uses

1. Expansion of existing threats
   1. Characteristics of AI-powered attacks

Introduction of new threats

1. Deepfakes
2. Breaking CAPTCHAs
3. Swarming attacks

TITLE LOREM IPSUM

- According to many security analysts, security incidents reached the highest number ever recorded in 2019 From phishing to ransomware, from the dark web as a service economy to attacks on civil infrastructure, the cybersecurity landscape involved attacks that grew increasingly sophisticated during the year.

- According to Interpol, 907,000 spam messages related to Covid-19 were detected between June and April 2020. Similarly, the 2020 Remote Workforce Cybersecurity Report showed that nearly two-thirds of respondents saw an increase in breach attempts, with 34% of those surveyed having experienced a breach during the shift to telework.

- In 2021 the drive for ubiquitous connectivity and digitalization continues to support economic progress but also, simultaneously and ‘unavoidably’, creates a fertile ground for the rise in scale and volume of cyberattacks. Increasing ransomware and diversified tactics, increasingly mobile cyber threats, ever more sophisticated phishing, cybercriminals and nation-state attackers targeting the systems that run our day-to-day lives, and malicious actors attacking the cloud for every new low-hanging fruit.

AI SYSTEMS’ SUPPORT TO CYBERSECURITY

- Against this backdrop, organizations have started using AI to help manage a growing range of cybersecurity risks, technical challenges, and resource constraints by enhancing their systems’ robustness, resilience, and response.
- AI systems work with security analysts to change the speed at which operations can be performed.
- The relationship between AI systems and security operators should be understood as a synergetic integration, in which the unique added value of both humans and AI systems are preserved and enhanced, rather than as a competition between the two.
- The most common applications are network security, followed by data security, and endpoint security. Three main categories can be identified in AI use in cybersecurity: detection (51%), prediction (34%), and response (18%).

THE DRIVING FORCES THAT ARE BOOSTING THE USE OF AI IN CYBERSECURITY COMPRISE:

- 1. **Speed of impact**: In some of the major attacks, the average time of impact on organizations is four minutes. Furthermore, today's attacks are not just ransomware, or just targeting certain systems or certain vulnerabilities; they can move and adjust based on what the targets are doing. These kinds of attacks impact incredibly quickly and there are not many human interactions that can happen in the meantime.

- 2. **Operational complexity**: Today, the proliferation of cloud computing platforms and the fact that those platforms can be operationalized and deliver services very quickly – in the millisecond range – means that you cannot have a lot of humans in that loop, and you have to think about a more analytics-driven capability.

- 3. **Skills gaps in cybersecurity remain an ongoing challenge**: According to Frost & Sullivan, 35, there is a global shortage of about a million and a half cybersecurity experts. This level of scarcity pushes the industry to automate processes at a faster rate.

AI CAN HELP SECURITY TEAMS IN THREE WAYS

- by **improving systems' robustness, response, and resilience -3R model**.
- AI can improve systems' robustness, that is, the ability of a system to maintain its initial assumed stable configuration even when it processes erroneous inputs, eg: self-testing and self-healing software.
- AI systems can be used to improve testing for robustness, delegating to the machines the process of verification and validation.
  - Robustness refers to the ability of a system or network to maintain its functionality and stability even in the presence of adverse conditions, stress, or unexpected events, such as cyberattacks, hardware failures, or high levels of traffic.
  - Example: A robust cybersecurity system can withstand attempts at intrusion and continue to operate effectively without compromising data integrity or availability.

AI CAN HELP SECURITY TEAMS IN THREE WAYS

- AI can strengthen systems' resilience, i.e. the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.
  - Resilience refers to the capacity of a system to absorb shocks, adapt to changing circumstances, and recover quickly from disruptions or failures. It involves the ability to bounce back and continue operations with minimal downtime.
  - Example: A resilient network can recover from a distributed denial of service (DDoS) attack by rerouting traffic and maintaining service availability.
- AI can be used to enhance system response, i.e. the capacity of a system to respond autonomously to attacks, to identify vulnerabilities in other machines, operate strategically by deciding which vulnerability to attack and at which point, and launch more aggressive counterattacks.
- Identifying when to delegate decision-making and response actions to AI and the need for an individual organization to perform a risk-impact assessment are related.

AI CAN HELP SECURITY TEAMS IN THREE WAYS

- In many cases AI will augment, without replacing, the decision-making of human security analysts and will be integrated into processes that accelerate response actions.

- Response in cybersecurity refers to the actions taken by an organization or system in the event of a security incident or breach. It encompasses the strategies, processes, and measures put in place to contain, mitigate, and recover from the incident.

- Example: An incident response plan outlines how an organization will respond to a data breach, including steps for identifying the breach, notifying affected parties, and implementing security measures to prevent further damage.

SYSTEM ROBUSTNESS

- The need to respond to cyberattacks spurs companies to build systems that are self-learning, i.e., able to establish local context and distinguish rogue from normal behavior.
- A system is robust when it can continue functioning in the presence of internal or external challenges without changing its original configuration.
- System robustness implies that AI is able to perform anomaly detection and profiling of anything that is generically different.
- These systems are able to check and optimize their state continuously and respond quickly to changing conditions. AI-powered behavioral analytics help compares how a system should run with how it is currently running and what the trigger corrections are.
- More robust and accurate approaches focus on detecting attacker's specific and immutable behaviors.
- Artificial Intelligence for software testing (AIST) is a new area of AI research aiming to design software that can self-test and self-heal.
- Self-testing refers to "the ability of a system or component to monitor its dynamically adaptive behavior and perform runtime testing prior to, or as part of the adaptation process.

- System robustness can also be enhanced by incorporating AI in the system's development to increase security controls, for example via vulnerability assessment and scanning.

- Vulnerability assessment can be either manual, assistive, or fully automated.

- Fully automated vulnerability assessment leverages AI techniques and allows for considerable financial gains and time reductions.

- ML has been used to build predictive models for vulnerability classification, clustering, and ranking. Support-vector machines (SVMs), Naive Bayes, and Random Forests are among the most common algorithms.

- Various evaluation metrics are used to determine the performance, such as precision, recall and f-score.
- Among other techniques, ML can be used to create risk-analysis models that proactively determine and prioritize security loopholes.

- **Automated planning has also been successfully applied for vulnerability assessment, mainly in the area of generating attack plans that can assess the security of underlying systems.**

- **The real-time steps of an attacker are modeled through automated planning, for example by simulating realistic adversary courses of action or focusing on malicious threats represented in the form of attack graphs.**

- **If attack plans are generated by an AI system, there is greater potential to discover more plans than if they are generated by human experts.**

- Precision is a metric that quantifies the number of correct positive predictions made.

- Recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made.

- Accuracy is defined as the proportion of correct predictions in all predictions made.
- Accuracy of a machine learning model is a metric for determining which model is the best at recognizing correlations and patterns between variables in a dataset based on the input, or training, data.

- F-Measure provides a way to combine both precisions and recall into a single measure that captures both properties.

- Code review is another area of application for enhancing system robustness. Peer code review is a common best practice in software engineering where source code is reviewed manually by one or more peers (reviewers) of the code author.

- Automating the process by using AI systems can both reduce time and allow a greater number of bugs to be discovered than ones discovered manually. Several AI systems are being developed for code review support.

- In June 2020, for example, the Amazon Web Services AI-powered code reviewer from CodeGuru was made publicly available.
- The use of AI to improve system robustness not only improves the security of systems and reduces their vulnerability but is also a strategic one.

- It decreases the impact of zero-day attacks. Zero-day attacks leverage vulnerabilities that are exploitable by attackers as long as they remain unknown to the system providers or as long as there is no patch to resolve them.

- By decreasing the impact of zero-day attacks, AI reduces its value on the black market.

SYSTEM RESILIENCE

- It is the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.
- A system is resilient when it can adapt to internal and external challenges by changing its methods of operations while continuing to function.

- System resilience implies, unlike system robustness, some fundamental shift in the core activities of the system that has to adapt to the new environment. Threat and anomaly detection (TAD) is today the most common application of AI systems.

- There are now approximately 592,145 new unique malware files every day, and possibly even more.
- Classification of new threats by humans alone is impossible, and besides, threats are becoming more complicated and better dissimulated.

- In the past, it was common to use signatures to classify malicious attacks, leveraging databases of known threats. Such measures, however, are becoming considerably less effective against the latest strains of advanced malware, which evolve by the second.

SYSTEM RESPONSE

- System resilience and response are deeply intertwined and logically interdependent, as, to respond to a cyberattack, you need to detect what it is occurring and develop and deploy an appropriate response by deciding which vulnerability to attack and at which point, or by launching counterattacks.

- Prevention of cyberattacks is increasingly going in the direction of systems able to deploy real-time solutions to security flaws. AI can help to reduce cybersecurity experts' workloads by prioritizing the areas that require greater attention and by automating some of the experts' tasks.

- AI can facilitate attack responses by deploying, for example, semi-autonomous lures that create a copy of the environment that the attackers intend to infiltrate.

- AI solutions can also segregate networks dynamically to isolate assets in controlled areas of the network or redirect an attack away from valuable data

- AI systems are able to generate adaptive honeypots (computer systems intended to mimic likely targets of cyberattacks) and honeytokens (chunks of data that look attractive to potential attackers).

- Based on the attacker's reaction to the defenses, it is possible to understand its skills and tools. The AI solution gets to learn the attacker's behavior via this tool so that it will be recognized and tackled during future attacks.

WHAT AI CAN DO?

- AI solutions for cybersecurity enable a fundamental shift from signature-based detection to more flexible and continuous monitoring of the network as it shifts from its normal behaviors.
- "AI algorithms can detect any changes that appear abnormal – without needing an advance definition of abnormal."
- AI can also provide insights into potential attacks by performing deep packet traces through internal or external sensors or pieces of monitoring software.
- Companies use AI to automate cyber defenses against spam and phishing and to detect malware, fraudulent payments, and compromised computers and network systems. Furthermore, AI is used for critical forensics and investigative techniques.
- AI is used to create real-time, customer-specific analysis, improving the total percentage of malware identified and reducing false positives. Hence, AI data processing helps cybersecurity threat intelligence become more effective.
- Organizations are using AI-based predictive analytics to determine the probability of attacks, enhancing an organization's network defense through near real-time data provisions.
- Predictive analytics can help in processing real-time data from various sources and identifying attack vectors by helping manage big data; filtering and parsing the data before they are analyzed; in automatically filtering out duplicates; categorizing information, and by suggesting which incident to prioritize. In this way, predictive analytics reduces human errors and the workload for security analysts.

THANK YOU