Artificial Intelligence and its Impact on Cybercrime

Carla LOZONSCHI, Irina BAKHAYA, PhD
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
carlalozonschi@gmail.com, i.bakhaya@gmail.com

Abstract

It is well known that technology is becoming increasingly prevalent among us, and that it is evolving at a quick pace. We're hearing more and more about artificial intelligence and how it affects our lives. Opinions on AI split the globe into two camps. Therefore, we choose to discuss what Artificial Intelligence is and how it marks our lives. Is it good to employ artificial intelligence? If so, how far should this be taken? Can it be used in a bad way? Sure, but this may also play a significant role in preventing and combatting cybercrime. All of these topics will be addressed in the next article.

Index terms: Artificial Intelligence, cybercrime, cybersecurity, deepfakes, bots

1. Introduction

Artificial intelligence is referred to as intelligent machines. This is in contrast to humans' and animals' innate intelligence. Machines use Artificial Intelligence to execute operations including learning, planning, reasoning, and problem solving. The most notable aspect of Artificial intellect is the replication of human intellect by machines. It is most likely the most rapidly developing advancement in the world of technology and innovation. Furthermore, many experts believe AI has the potential to tackle huge problems and crisis circumstances.

2. What is AI and how it marks our lives?

We have all heard about artificial intelligence in recent years, but few are aware that it has been developed since the twentieth century, i.e. after World War II and the name itself was coined in 1956. AI currently encompasses a huge variety of subfields, ranging from the general (learning and perception) to the specific, such as playing chess, proving mathematical theorems, writing poetry, driving a car on a crowded street, and diagnosing diseases. AI is relevant to any intellectual task; it is truly a universal field.

Artificial Intelligence can be seen from several perspectives [1]. The definitions on top are concerned with thought processes and reasoning, whereas the ones on the bottom address behavior. The definitions on the left measure success in terms of fidelity to human performance, whereas the ones on the right measure against an ideal performance measure, called rationality.

Thinking Humanly	**Thinking Rationally**
"The exciting new effort to make computers think ... machines with minds, in the full and literal sense." (Haugeland, 1985) "[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning ..." (Bellman, 1978)	"The study of mental faculties through the use of computational models." (Charniak and McDermott, 1985) "The study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)
Acting Humanly	**Acting Rationally**
"The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990) "The study of how to make computers do things at which, at the moment, people are better." (Rich and Knight, 1991)	"Computational Intelligence is the study of the design of intelligent agents." (Poole et al., 1998) "AI . . . is concerned with intelligent behavior in artifacts." (Nilsson, 1998)

ACTING HUMANLY

The Turing Test, proposed by Alan Turing (1950), was designed to provide a satisfactory operational definition of intelligence. A computer passes the test if a human interrogator, after posing some written questions, cannot tell whether the written responses come from a person or from a computer. Chapter 26 discusses the details of the test and whether a computer would really be intelligent if it passed. For now, we note that programming a computer to pass a rigorously applied test provides plenty to work on. The computer would need to possess the following capabilities:

- natural language processing to enable it to communicate successfully in English;
- knowledge representation to store what it knows or hears;
- automated reasoning to use the stored information to answer questions and to draw new conclusions;
- machine learning to adapt to new circumstances and to detect and extrapolate patterns.

Turing's test deliberately avoided direct physical interaction between the interrogator and the computer, because physical simulation of a person is unnecessary for intelligence. However, the so-called total Turing Test includes a video signal so that the interrogator can test the subject's perceptual abilities, as well as the opportunity for the interrogator to pass physical objects "through the hatch." To pass the total Turing Test, the computer will need:

- computer vision to perceive objects, and
- robotics to manipulate objects and move about.

These six disciplines compose most of AI, and Turing deserves credit for designing a test that remains relevant 60 years later. Yet AI researchers have devoted little effort to passing the Turing Test, believing that it is more important to study the underlying principles of intelligence than to duplicate an exemplar.

THINKING HUMANLY

The interdisciplinary field of cognitive science brings together computer models from AI and experimental techniques from psychology to construct precise and testable theories of the human mind. Cognitive science is a fascinating field in itself, worthy of several textbooks and at least one encyclopedia. In the early days of AI, there was often confusion between the approaches: an author would argue that an algorithm performs well on a task and that it is therefore a good model of human performance, or vice versa. Modern authors separate the two kinds of claims, allowing both AI and cognitive science to develop more rapidly. Computer vision, which incorporates neurophysiological evidence into computational models, is an example of this.

THINKING RATIONALLY

The Greek philosopher Aristotle was one of the first to attempt to codify "right thinking," that is, irrefutable reasoning processes. His syllogisms provided patterns for argument structures that

always yielded correct conclusions when given correct premises. This study initiated the field of logic, which developed a precise notation for statements about all kinds of objects in the world and the relations among them. By 1965, programs existed that could, in principle, solve any solvable problem described in logical notation. However, there are two main obstacles to this approach: it is not easy to take informal knowledge and state it in the formal terms required by logical notation, particularly when the knowledge is less than 100% certain, and there is a big difference between solving a problem "in principle" and solving it in practice. These obstacles appear first in the logicist tradition.

ACTING RATIONALLY

The "laws of thought" approach to AI emphasizes correct inferences, but there are also ways of acting rationally that do not involve inference. The rational-agent approach is more general than the "laws of thought" approach, as correct inference is just one of several possible mechanisms for achieving rationality. It has two advantages over the other approaches: it is more general and is more general than the "laws of thought" approach, and it is more general than the "laws of thought" approach because correct inference is just one of several possible mechanisms for achieving rationality. The rational-agent approach has two advantages over the other approaches: it is more.

The standard of rationality is more amenable to scientific development than approaches based on human behavior or human thought. It is mathematically well defined and completely general, and can be "unpacked" to generate agent designs that provably achieve it. Human behavior, on the other hand, is well adapted for one specific environment and is defined by the sum total of all the things that humans do. Despite the apparent simplicity of the problem, an enormous variety of issues come up when we try to solve it. To simplify the problem, perfect rationality is a good starting point for analysis, as it simplifies the problem and provides the appropriate setting for most of the foundational material in the field.

What is the significance of discussing artificial intelligence? We can all see how much technology affects our life, from the most basic to the most complicated activities a person may engage in. For this reason, we must understand how and when to apply Artificial Intelligence. If we don't know how to utilize it, it has a lot of power. Regarding cyber crime, it can be used in both directions, either to increase the rate of criminal crime, or by preventing and combating it.

How can artificial intelligence be used for negative purposes?

Cybercriminals are already using AI to make their attacks more effective and far-reaching. It will only grow more widespread.

In 2020, a study by European police agency Europol and security provider Trend Micro, identified how cybercriminals are already using AI to make their attacks more effective, and the many ways AI will power cybercrime in future [2].

While AI and ML can support businesses, critical infrastructures, and industries as well as help solve some of society's biggest challenges (including the Covid-19 pandemic), these technologies can also enable a wide range of digital, physical, and political threats to surface. For enterprises and individual users alike to remain protected from malicious actors who are out to misuse and abuse AI, the risks and potential malicious exploitations of AI systems need to be identified and understood.

DEEPFAKES

Deepfakes are a common kind of AI abuse in which audio and visual information is created or altered to seem authentic using AI algorithms. An purported deepfake video that purports to show a Malaysian political assistant engaging in sexual relations with a cabinet minister is one illustration of this, and it demands for the cabinet member to be looked into for potential wrongdoing. Another instance is a UK-based energy company that was tricked into sending over 200,000 British pounds (about $260,000 as of this writing) to a Hungarian bank account after a malevolent person impersonated the voice of the company's CEO using deepfake audio technology. Since Buzzfeed

collaborated with actor and filmmaker Jordan Peele on Deepfakes, it can serve as a beneficial tool for teaching people about their potential abuses.

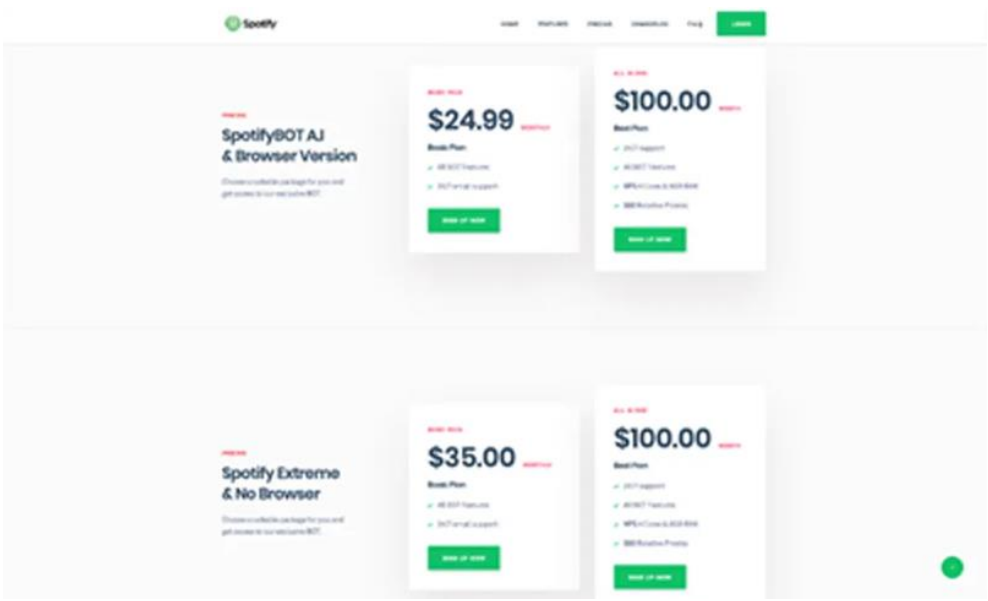
AI-SUPPORTED PASSWORD GUESSING

Cybercriminals are using ML to enhance password guessing algorithms. It is already possible to effectively determine the password that matches to the password hash using more conventional methods like HashCat and John the Ripper, which compare several permutations to the password hash. However, thieves would be able to examine big password datasets and develop password variants that suit the statistical distribution using neural networks and generative adversarial networks (GANs). This will eventually result in more precise and profitable password guesses as well as more opportunities for profit.

HUMAN IMPERSONATION ON SOCIAL NETWORKING PLATFORMS

AI is being used by cybercriminals to mimic human behavior. By imitating human-like usage patterns, they may, for instance, easily fool bot detection algorithms on social media networks like Spotify. Cybercriminals may then monetise the infected system to produce phony streams and traffic for a particular artist using this AI-supported impersonation.

An AI-supported Spotify [2] bot on a forum called nulled[.]to claims to have the capability to mimic several Spotify users simultaneously. It employs a number of proxies in order to evade discovery. This bot raises the number of streams (and therefore, revenue) for particular songs. It also produces playlists with other songs that reflect human-like musical preferences rather than playlists with random tracks, since the latter might suggest bot-like activity, to further elude discovery.



In the future, I envision criminals using AI in a variety of ways. It is quite possible that cybercriminals will use AI to increase the breadth and size of their assaults, avoid detection, and abuse AI as both an attack route and an attack surface.

Criminals will employ AI to carry out nefarious operations such as social engineering to victimize companies. Cybercriminals may utilize AI to automate the earliest phases of an attack by creating content, increase business information collecting, and accelerate the detection rate of potential victims and business operations. This can lead to faster and more accurate business fraud via different tactics such as phishing and business email compromise (BEC) schemes.

Artificial intelligence (AI) is playing a massive role in cyber attacks and is proving both a “double-edged sword” and a “huge challenge,” according to NATO.

"Artificial intelligence allows defenders to scan networks more automatically, and fend off attacks rather than doing it manually. But the other way around, of course, it's the same game," David van Weel, NATO's Assistant Secretary-General for Emerging Security Challenges, told reporters earlier this month [3].

Since the Ukraine war, cyber assaults on national infrastructures and commercial organizations have increased tremendously and become a focus point. This year, NATO stated that a cyber assault on any of its member nations might trigger Article 5, which specifies that an attack on one member is considered an attack on all of them and may result in a collective reaction.

AI-based technologies may be used to better detect and fight against threats, but hackers can also utilize the technology for more sporadic attacks that are more difficult to defend against since there are so many of them at the same time.

AI cyber attacks can be used not just to shut down infrastructure but also to exploit information, said Alberto Domingo, technical director of cyberspace at NATO Allied Command Transformation [3].

"I think AI is a critical threat. The number of attacks is increasing exponentially all the time," he told Euronews Next, adding that at the moment the world is simply "living with these attacks" and needs more cybersecurity rules.

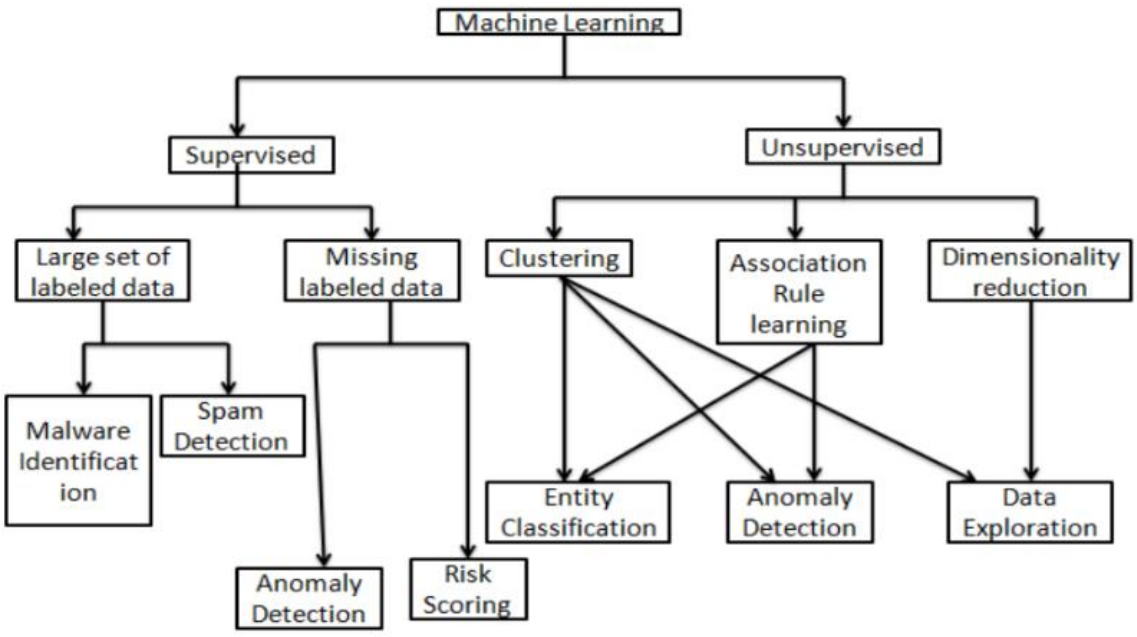
"We are not yet at a stage where we identify that this is simply not acceptable. These behaviours cannot be allowed in cyberspace," he said.

"It shows you that we still don't have a collective common approach to react to those things, but those things are simply not acceptable".

As a result, while Artificial Intelligence may mark crimes negatively by easing the labor of numerous hackers, it can also be utilized to prevent and combat cybercrime.

Advantages of AI in Cybersecurity

Because cyber security risks are always changing and evolving, a rapid and automated reaction is essential. As a result, machine learning techniques, particularly deep learning, that do not often require prior expertise or reliance on past expert classifications may be very useful in the application of cyber security AI systems. The research [4] Security examined the efficiency of machine learning methods for cyber security reasons. This study involves the use of machine learning technologies to detect intrusions, spam, and malware.



AI has several benefits and uses in a range of fields, one of which is cybersecurity. With today's rapidly developing cyberattacks and rapid device proliferation, AI and machine learning can assist in keeping up with cybercriminals, automating threat detection, and responding more efficiently than traditional software-driven or manual procedures.

Using complicated algorithms, AI systems are being trained to recognize malware, perform pattern recognition, and detect even the smallest features of malware or ransomware assaults before they reach the system. AI may deliver more predictive intelligence using natural language processing by scanning through articles, news, and studies on cyber dangers and selecting material on its own. According to Tech Republic, a mid-sized corporation receives alerts for over 200,000 cyber events per day. This volume of assaults would overwhelm a typical company's security personnel. As a result, some of these attacks may go undetected, causing considerable network damage. Security personnel require considerable assistance from intelligent machines and current technologies such as AI to function efficiently and safeguard their companies from cyber attacks.

DETECTING NEW THREATS

AI may be used to detect cyber dangers and potentially harmful behavior. Traditional software systems simply cannot keep up with the huge volume of new viruses developed each week, thus this is an area where AI may be really useful.

AI systems are being trained to identify malware, run pattern recognition, and detect even the smallest behaviors of malware or ransomware assaults before they reach the system using advanced algorithms. AI enables higher predictive intelligence through natural language processing, which curates material on its own by scraping articles, news, and cyber threat research. This can provide novel abnormalities, cyberattacks, and protection techniques. After all, hackers, like everyone else, follow trends, so what's popular with them changes all the time.

AI-based cybersecurity solutions may give the most up-to-date knowledge about global and industry-specific threats, allowing you to make more informed prioritizing decisions based not just on what could be used to attack your systems, but also on what is most likely to be used to attack your systems.

BATTLING BOTS

Bots account for a significant portion of internet traffic nowadays, and they may be deadly. Bots may be a serious threat, from account takeovers using stolen passwords to fraudulent account creation and data theft.

Manual answers alone will not suffice to combat automated threats. AI and machine learning assist in developing a comprehensive knowledge of website traffic and distinguishing between good bots (such as search engine crawlers), malicious bots, and humans.

AI helps us to evaluate massive amounts of data and allows cybersecurity teams to modify their approach to an ever-changing scenario.

“By looking at behavioral patterns, businesses will get answers to the questions ‘what does an average user journey look like’ and ‘what does a risky unusual journey look like’. From here, we can unpick the intent of their website traffic, getting and staying ahead of the bad bots,” explains Mark Greenwood, Chief Technical Architect & Head of Data Science at Netacea [5].

BREACH RISK PREDICTION

AI systems assist in determining the IT asset inventory, which is a precise and thorough record of all devices, users, and apps with varying levels of access to various systems.

Taking into account the asset inventory and threat exposure (described above), AI-based systems can forecast how and where you are most likely to be hacked, allowing you to plan and allocate resources to the most vulnerable regions.

AI-based analysis provides predictive insights that allow you to set and optimize policies and procedures to strengthen your cyber resilience.

What Cybersecurity Executives Think About AI?

Capgemini Research Institute analyzed the role of AI in cybersecurity and their report titled Reinventing Cybersecurity with Artificial Intelligence [6].

Respondents to a poll (850 executives from cybersecurity, IT information security, and IT operations from ten countries) agree that AI-enabled response is needed due to cybercriminals using AI technology to execute assaults.

The following are some of the report's primary takeaways:

- According to three out of four CEOs polled, AI enables their firm to respond to breaches more quickly.
- 69% of businesses believe AI is required to respond to threats.
- According to three out of every five companies, utilizing AI enhances the accuracy and efficiency of cyber analysts.
- AI gives better answers to an organization's cybersecurity demands as networks get larger and data grows more complicated. Simply said, humans are incapable of dealing with the increasing complexities on their own, and the employment of AI will become unavoidable sooner or later.

To summarize, artificial intelligence is well on its way to dominating the planet. While this may appear to be a frightening and worrisome future, there is no major or reliable evidence to suggest that the usage, application, implementation, and assimilation of artificial intelligence would harm the planet in any manner. So far, technology has only worked to better existing problems and living conditions. Artificial intelligence has helped both those who developed it and those who utilize it. Unlike in Hollywood sci-fi movies, the planet is not vulnerable to an invasion by renegade robots. For those who are still skeptical, experts believe that introducing one case where a hypothesis does not hold true can invalidate it.

Artificial Intelligence has thus far shown to be nothing but positive. Artificial intelligence is on its approach to being a game changer in ethics, social welfare, healthcare, and workforce. Because these are the most important components of life on a daily basis, technological developments in these domains will matter far more than in any other. Improving ethical standards, benefiting societal welfare through regulated surroundings, greatly increasing healthcare, and transforming the workforce; artificial intelligence is the unanticipated but much needed miracle. Artificial Intelligence supremacy will substantially enhance the quality of living and reshape the globe.

References

[1]. P. Norvig, S. Russell, Artificial Intelligence: A Modern Approach, Global Edition, pg. 2.

[2]. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml.

[3]. https://www.euronews.com/next/2022/12/26/ai-cyber-attacks-are-a-critical-threat-this-is-how-nato-is-countering-them#:~:text=Artificial%20intelligence%20(AI)%20is%20playing,rather%20than%20doing%20it%20manually.

[4]. https://www.researchgate.net/publication/364126309_Artificial_Intelligence_in_Cyber_Security.

[5]. https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity.

[6]. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.