



Amar Basnet

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

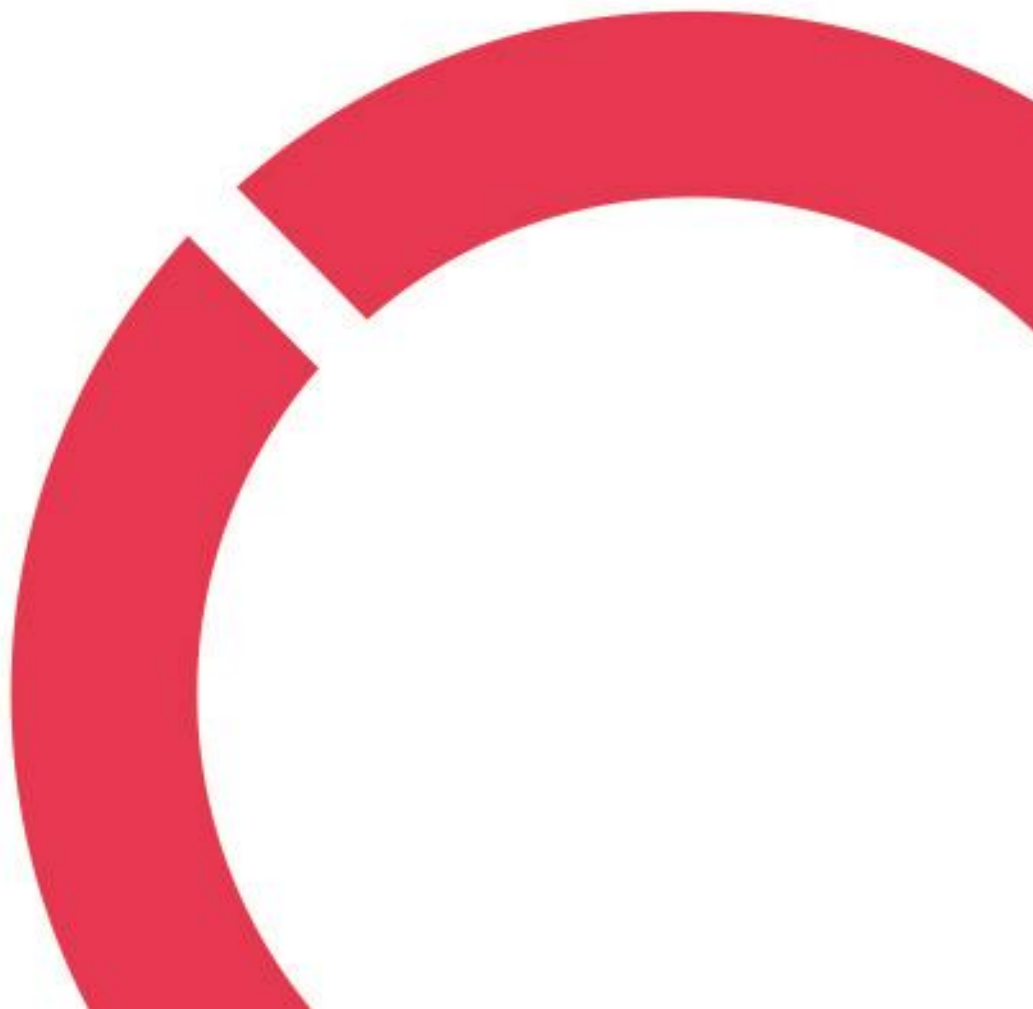
THESIS

CENTRIA UNIVERSITY OF APPLIED SCIENCES

Degree Programme

Bachelor of Engineering, Information Technology

May 2022



Abstract

Central University of Applied Sciences	Date May 2022	Author Amar Bahadur Basnet
Degree programme Bachelor of Engineering, Information Technology		
Name of Thesis ARTIFICIAL INTELLIGENCE IN CYBER SECURITY		
Centria Supervisor Jari Isohanni	Pages 26+3	
Instructor representing commissioning institution Jari Isohanni		
<p>Abstract</p> <p>The emergence of cyber threats has outstripped the cyber defense firm's budgetary capital and human analysis and confronted every new type of cyber danger. With the growing digital footprint, a substantial number of personal info should be safeguarded against cyberattacks. Data breaches can damage a brand's productivity or cause it to fail. This study investigates the use of artificial intelligence (AI) to improve information security. Recent advances in machine learning have been transformative, surpassing physical movement in activities such as data insights. The conceptual review of the literature procedure was used in the survey, and data were gathered from academic and industrial sources. The research found that the use of AI in cyber warfare direct authority has both benefits and disadvantages; even so, the benefits outweigh the drawbacks. With the fast and efficient innovation necessary to drive AI systems, this detection approach is likely to boost business and customer security in the cyber world. This is demonstrated by the expanding use of AI motors instead of traditional scanners motors in cyber defense.</p>		

Table of Contents

Abstract

Concept Definitions

1	INTRODUCTION.....	1
2	ARTIFICIAL INTELLIGENCE	4
2.1	History of AI.....	4
2.2	Weak Artificial Intelligence.....	6
2.3	Strong Artificial Intelligence.....	7
2.4	Purpose and Scope of AI	8
2.4.1	Enhances decision-making.....	8
2.4.2	Particle	8
2.4.3	Machine Learning.....	9
2.4.4	Technological work.....	10
2.4.5	Medical care.....	11
2.4.6	Automobiles	12
2.4.7	Human Resources and Hiring	12
3	UNDERSTANDING CYBER SECURITY AND DEFENSES	14
3.1	What causes cyber-attacks.....	15
3.2	Types of Cyber Attacks.....	15
3.2.1	Web Vandalism	15
3.2.2	DOS	17
3.2.3	Malware	18
3.2.4	Zero-Day Attacks	18
3.3	Types of Cyber Defenses	18
3.3.1	Application Protection	19
3.3.2	Security in the Cloud	19
3.3.3	Security in the Field.....	19
3.4	Some cases of cyber attacks.....	22
3.4.1	Conficker	22
3.4.2	GhostNet	22
3.4.3	Stuxnet	23
4.	AI IN CYBER SECURITY	24

5 CONCLUSION.....	26
REFERENCES	27

List of Tables

Table 1: Types of attack with their prevention.....	21
---	----

List of Figures

Figure 1: Machine Learning	10
Figure 2: History of AI.....	5
Figure 3: Web hacking in Iran from 2003 - 2011	16
Figure 4: Hacking of website in Iran during war	17

Concept Definitions

AI: Artificial Intelligence

MI: Machine Learning

DL: Deep Learning

DOS: Denial of service

DDOS: Distributed Denial of service

ICT: Information and communication technologies

NLP: Natural Language Processing

1 INTRODUCTION

"Cognition" is one of the characteristics that distinguishes humans from other living beings on the earth. Despite the fact that computers do not have inheritable intelligence, the idea of bringing that intelligence into man-made devices is alluring. In terms of internet security, artificial intelligence is crucial. The goal of internet security is to create safeguards to protect information technology systems, connections, software, and data from unauthorized connectivity, modification (Winston 1992.) It also contains a wide range of approaches for safeguarding mutually supportive software and data against injury, unauthorized connections, and cyber-assault. New hazards emerge and occur rapidly as knowledge and connection innovation (ICT) progresses. AI has gained traction, affecting every part of the business and its survival. The technical discipline and technique of developing automation technologies are of special concern to AI. Videogames, production, medical services, training, language processing, and a variety of other fields have all benefited from AI (Russell 2009.)

These benefits may be observed in information security, where AI is utilized to attack as well as defend. The fields of computer security and artificial intelligence, which were previously thought to be separate, are increasingly being created to correspond in areas such as the designing stage, which attempts to repair knowledge spilling and improve agreed as assailants' core on duplicating the genuine preparedness at the sentient market level, among everyone else. When it comes to this, keep in mind that AI approaches and structures that mix AI can produce unexpected results, which can be exploited to influence intended advantages. As a result of the web's pervasiveness, there will be a greater emphasis on internet security and AI software. When it comes to creating computer viruses to exploit people, corporations, and governments, attackers are becoming savvier and more inventive. Scamming, password threats, computer viruses, and other types of threats could be employed in situations where traditional security measures are ineffective (Winston 1992.) The use of artificial intelligence (AI) has the potential to improve data security. AI solutions can assist in not only identifying dangers, but also in taking suitable counter-measures against cyber-attacks, such as grouping and classifying events and hazards, as

well as relieving professionals of tedious work. Artificial intelligence and internet security are linked in a complex web of interconnections.

AI is an umbrella term over many subcategories of endorsed terms and phrases that allude to essential aspects. The words sluggish AI and strong AI are frequently used in brand management to describe the complexity of an AI-based scheme. Weak AI is a pattern recognition answer that is focused on a single task, including maximizing the value of a commodity or the given moment of an electronic mail. Strong AI, on either side, relates to the broad framework that can sense by itself, finding solutions it has not previously been educated to solve (Bishop 2013.)

Artificial Intelligence's goal is to augment human capacity and assist us in settling on choices with far-reaching implications. From a technological standpoint, that is the solution. Artificial Intelligence is the ability to assist people to exist more fulfilling lives free of forced work, as well as handle the tangled network of interrelated people, businesses, countries, and countries to operate in a way that benefits all of civilization.

Presently, the goal of Artificial Intelligence is the same for all of the skills and equipment one has developed over the last thousands of years: to reduce human work and aid in decision-making. Artificial Intelligence has been dubbed the "Completed Discovery," a concept that would create ground-breaking software and applications which would drastically alter how one spend their lives, let people hope to eradicate conflict, unfairness, and human misery. AI is being used in a variety of fields to generate an understanding of user behavior and make data-driven suggestions. Google's forecasting search engine, for instance, used consumer historical information to anticipate what a user will indeed type first in the search field. Netflix utilizes user information to suggest what film a user should observe next, keeping them connected on the console and increasing their number of views. Facebook uses previous user information to instantly recommend tags for pals predicated on their facial characteristics in their photos. Large corporations use AI to make people's lives of their customers easier (Winston 1992.)

Scanning through data and fine-tuning the quest to produce the most useful result. If-then rationale supply chain which can be used to run a series of instructions given set of input variables. (Winston 1992.) Pattern-detection is a technique for identifying key trends in a huge

data set to gain new additional insight (Jordon 2015.) Clustering methods were used to build a predictive model.

2 ARTIFICIAL INTELLIGENCE

AI is a vital area of computational biology that deals with general intelligence, teaching, and the ability to adapt to machinery. It has a sturdy science fantasy undertone. AI research aims to develop machinery that can simplify tasks that require intelligence. Regulation, making plans, scheduling, the capacity to react to diagnosing and buyer questionnaires, cursive, utterance, and face recognition are just a few examples. As a result, it has evolved into an area of science dedicated to finding solutions to these problems. In addition to being constructed into many common household software packages, conventional games like computer chess, and other games consoles, AI systems are in widespread use in the economy, healthcare, technology, and the army.

2.1 History of AI

The concept of artificial cognitive ability had first been proposed in the mid-twentieth century, with the concept that a device is as smart as a living thing. John McCarthy and Alan Turing are widely regarded as the parents of machine learning. A lot of investigation is being undertaken on the notion of artificial intelligence as a result of this notion. "Natural Language" had become one of the divisions of artificial intelligence with an increase in technology in the 1970s. Other strands of artificial intelligence, such as deep learning technologies and neural nets, have been initiated briefly after. The rate at which artificial intelligence is evolving has influenced culture and human opportunities (Haenlein 2019.)

Sci-fi introduced the globe to the notion of artificial machine intelligence in the first half of the twentieth century. It started with the "coldhearted" Tin Man in *The Wizard of Oz* and progressed to the robotic exoskeleton that pranked Maria in *Megacity*. By the 1950s, humans had such an iteration of physicists, theorists, and intellectuals who had ethnically absorbed the notion of artificial intelligence (or AI). Alan Turing, a young British scholar who investigated the arithmetical potential of machine learning, has been one such individual (Benko 2009.) Turing

says that individuals use existing knowledge as well as purpose to solve problematic situations, so why cannot devices? This would be the rational template of his 1950 article, *Processing Forklifts and Insight*, wherein he mentioned how to construct autonomous robots and how to exam their intellectual ability. AI thrived from 1957 to 1974.

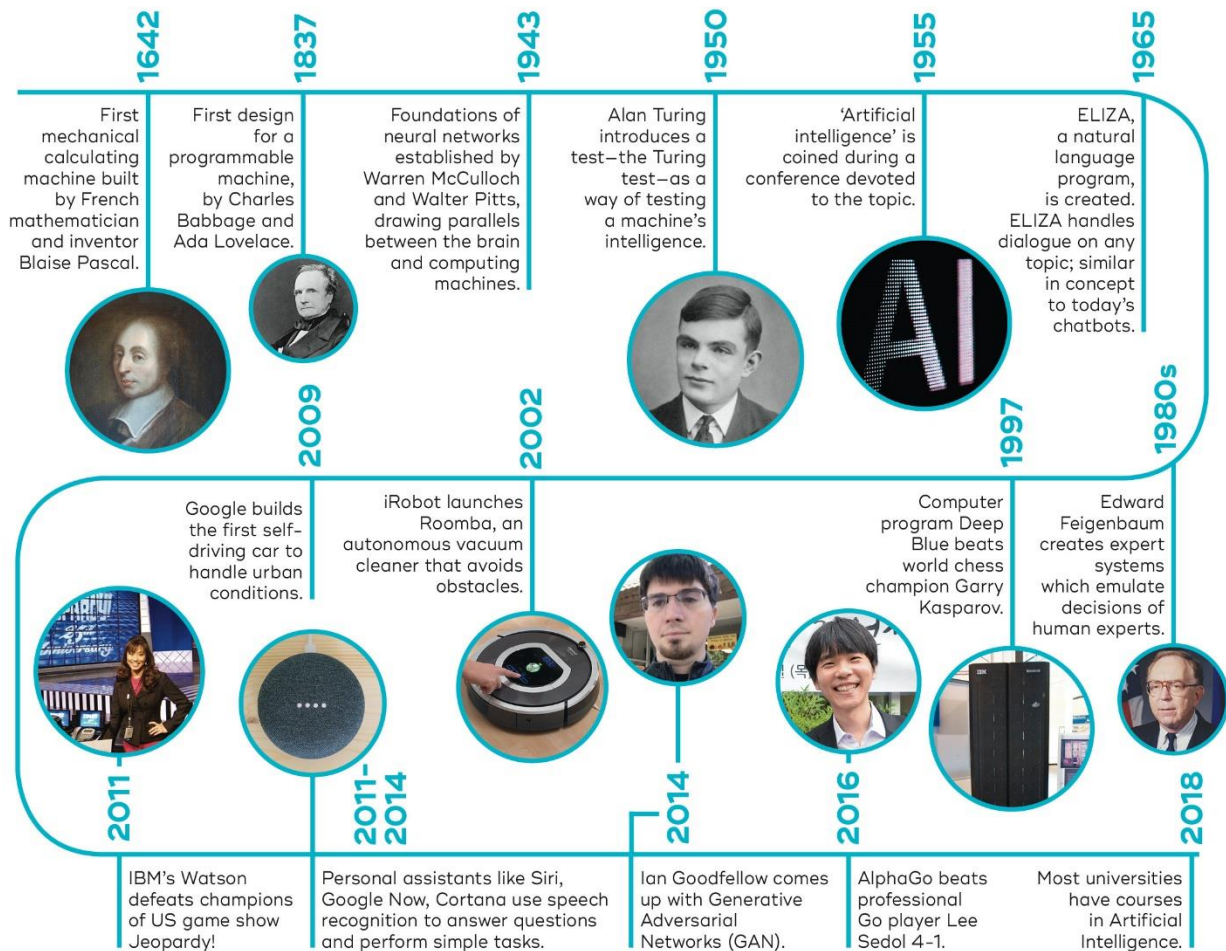


Figure 1: History of AI (*Haenlein 2019*.)

Laptops were capable of holding more data and have become quicker, inexpensive, and more usable (McCorduck 1977.) Machine learning heuristics got better as well, and individuals became more adept at determining which classifier to pertain to a specific problem. Initial protests, including Newell and Simon's *Public Critical Thinker* and Joseph Weizenbaum's ELIZA, showed potential in the areas of conflict resolution and spoken linguistic explanation,

respectively. Artificial intelligence is often thought to be a revolutionary innovation, but it is not. Researchers in the area of artificial intelligence is much wiser. The idea of machine intelligence is said to have originated in Greek myths. The following are some important milestones in the development of AI.

Warren McCulloch and Walter Pitts proposed an artificial neural prototype in 1943. (Buchanan 2015.) And Alan Turing published an article entitled "Computer Processes and Intellect" in 1950, wherein he invented the Turing Test. This testing is used to assess intelligent machines by determining whether or not the device is capable of rational thought. At the Democratic Convention in 1956, American software engineer John McCarthy invented the phrase Artificial Intelligence for the first moment. John McCarthy is recognized as the "Father of Artificial Intelligence." WABOT1, the first full-scale smart robot, was generated in Japan in 1972. With the progression of Intelligent Machines in the year 1980, AI was born. These are software applications that are used to solve difficult problems. IBM Deep Blue defeated world chess grandmaster Gary Kasparov in 1997, making it the first desktop to destroy a world chess winner. In the year 2006, artificial intelligence (AI) made its debut in the commercial world. Top businesses around the world, such as Facebook, Twitter, and Netflix, have begun to incorporate AI into their apps (Buchanan 2005.)

2.2 Weak Artificial Intelligence

Declares that "starting to think" capabilities could be introduced to desktops to produce high-quality living beings. Rich and Knight's meaning in their chapter "Artificial Intelligence" contains any computer-controlled device that substitutes or assists people in their job. In 1997, the IBM computer chip Deep Blue demonstrated its processing capability by winning numerous chess matches against the renowned chess player Gary Kasparov. Struggling to squeeze this incidence into the "weak" or "strong" definitions above, or the "strong" legal definition below, this would be classified as "Weak AI." Expert Systems are much more prime examples of Weak AI, but structures such as spell-checking apps and calculators also fall into this group. It is fair to

demonstrate that the last typical forms are not even remotely related to AI. However, this is entirely due to the wide range of AI interpretations (Bishop 2013.) Weak AI aids in the transformation of big data into actionable knowledge by sensing trends and anomalies forecasts. Meta's (previously Facebook's) newsfeed, Amazon's initially suggested transactions, and Apple's Voice recognition, the iPhone innovation that explains consumers' verbal questionnaires, are all examples of poor AI. Some other examples of poor AI are spam email filtration, where a computer performs a method to understand which notifications are probable to be spurious and then reroutes those from the mailbox to the spam box. (Bishop 2013.)

2.3 Strong Artificial Intelligence

"Strong" AI tends to make the audacious assertion that machines can be programmed to imitate thinkers' methods. In those other phrases, they order to mimic the brain's method. There is no obvious distinction in the ideology of strong AI among AI that is a slice of application that accurately mimics the acts of the neural network, and human decisions, such as comprehension and even cognition. Strong machine learning is a worldview rather than a process for developing AI. It is a fresh mindset on AI wherein AI is likened to living beings (Logan 2017.) It asserts that a device could be conditioned to start behaving like a human brain, to be smart in every meaning of the phrase, and can have perspective, opinions, and other intellectual regions typically associated with humans. Even so, because people cannot correctly describe intellect, it is tricky to provide an evident requirement for what constitutes accomplishment in the growth of good machine learning. Weak AI, on either side, is indeed very attainable due to the way it defines intellect. But instead of attempting to completely replicate mental processes, weak AI aims at building intellect focused on a specific job or course of study (Forster 2006.) That would be a series of practices that can be split into smaller mechanisms and thus accomplished on the level that has been established (Logan 2017.)

2.4 Purpose and Scope of AI

In multiple areas or regions, artificial intelligence has been used for a variety of reasons and attributes. Artificial intelligence's main goal is to create software applications that can fix troubles to accomplish objectives in the same way a human can. Robotics, machine learning, linguistic sensing, games, intelligent agents, voice recognition, and many other fields have opportunities for machine development (Verma 2018.) These are all the primary objectives of machine learning.

2.4.1 Enhances decision-making

The fundamental aim of artificial intelligence is to supply a decision-making process. This choice depends on unique information as raw data and will produce artificial intelligence results similar to those of the human condition. By streamlining numerous physiological and other duties, artificial intelligence can make better choices. These activities can minimize human workers while also improving efficiency. Decision-making in this manner greatly streamlines the task, but it eliminates people (and it is not always a good idea). Going to add AI to workloads is predicted to be more attractive to companies than increasing revenue and profit. According to Gartner, enterprises are being digitally format interrupted by the abundance of data they must cope with, which could overpower them. However, with AI, all that information can be turned into specific benefits, from marketing and advertising to request design and supply cords. Companies can make crucial decisions by rapidly analyzing huge data sources, such as what substance to establish for their target market or what to alter in a faltering marketing campaign. For beings, this takes a long time, but for a device, it takes seconds (Phillips 2012.)

2.4.2 Particle

The ultimate purpose of the application is to start taking over human effort. In the coming years, the rate of technological advancement will be unmanageable, resulting in large effects on human culture. Aside from their adverse reactions, these smart systems will help work easier and faster.

The singularity, for example, will indeed entail software programs to become so developed that machine learning Artificial intelligence (AI) outperforms human intelligence, conceivably removing the human-computer divide. One of the advanced components that will make singularity a truth is nanotech. This detonation of intellect will have a significant effect on patient humanity. This computer software and AI will evolve into truly intelligent computers with intellectual capacity far exceeding those of humans. While the phrase "technological particle" is frequently used in AI conversations, there is indeed a lot of debate and misunderstanding about what it means. However, most philosophes concurred that the advent of singularity will be a watershed moment. They also concurred on fundamental elements of singularity, such as rate and time. This appears to mean they consent those technological solutions will continue improving at a faster rate as time goes on (Zeng 2014.)

2.4.3 Machine Learning

The primary distinction between machine learning and artificial intelligence would be that deep learning is mainly worried about precision. Machine learning is a subcategory of AI technology that relies on information to generate results because it is more centered. Machine learning is essential for organizations to recognize patterns in consumer behavior and organizational business styles, as well as to aid in the introduction of new services. Several of today's most successful businesses, like Facebook, Google, and Uber, use machine learning. For many businesses, machine learning became a substantial critical advantage. Machine learning, like the human mind, tends to rely on input, like training examples or visualization techniques, to recognize entities, subject areas, and their links. Deep learning can start once enterprises have been described. Findings or data, such as illustrations, experience, or admonition, are used to start the machine learning operation. It searches for patterns from data so that it can draw conclusions based on the indicators offered (Jordon 2015.)

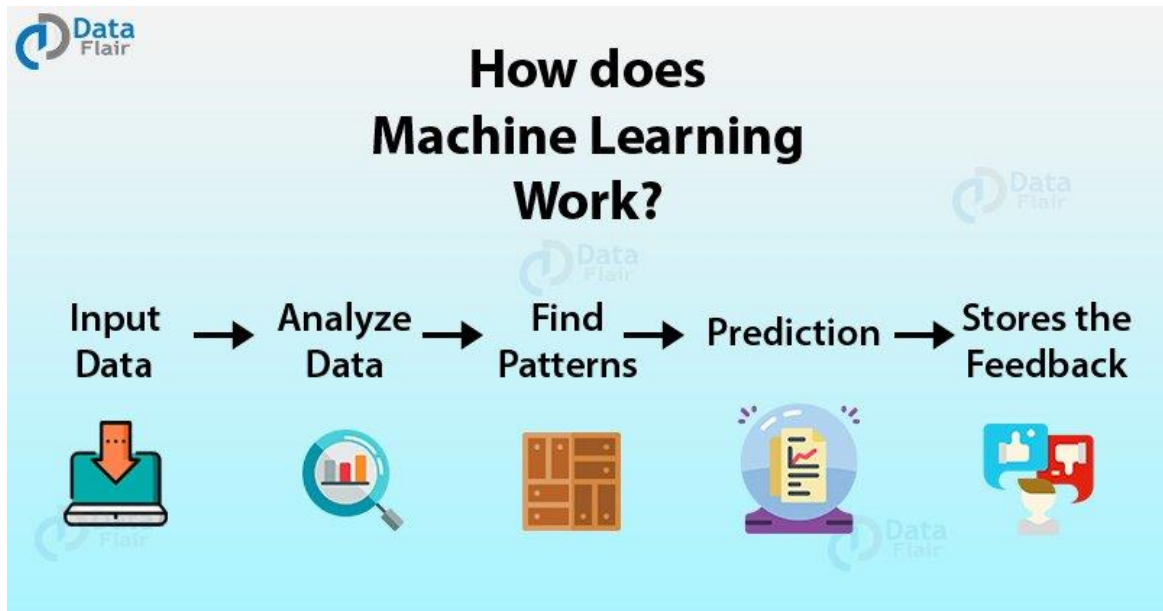


Figure 1: Machine Learning (*Goodfellow, 2013*)

The main goal of machine learning is to enable computers to understand and change their behavior on their own, without the need for human intervention. Machine learning is valuable because it can deal with problems at a size and speed that the human mind cannot match. Computers can be developed to spot trends in and connections among data input and optimize routine tasks using vast quantities of computer resources behind a single project or numerous specific activities (Jordon 2015.)

2.4.4 Technological work

A variety of methods are being used to ease process flow and are simple to combine across the company. These innovations are crucially significant and play an impact on many aspects' role in many aspects of living. Regardless of the lack of pervasive commonality, artificial intelligence (AI) is an innovation that is reshaping every aspect of life. It's a versatile tool that allows people to question how they incorporate data, evaluate it, and use the additional insight to make better decisions. Our goal with this complete analysis is to clarify AI to decision-makers, thought leaders, and intrigued watchers, as well as to show how AI is already making a difference and increasing critical questions for culture, economics, and leadership. Artificial intelligence has the

potential to vastly improve the effectiveness of the current industry. However, it has the potential to have an even bigger effect by trying to serve as a new general-purpose "technique of discovery" that can redefine the existence of the technology system and the implementation of R&D is organized. Humans find evidence of a "transition" in the significance of implementation of deep learning, distinguishing among system automation systems and the possibilities for the latest developments in "machine learning" to start serving as a general process of discovery. (Jordon 2015.)

2.4.5 Medical care

It is the greatest crucial component in which artificial intelligence has radically transformed. A huge majority of healthcare establishments are utilizing artificial intelligence machinery to best and more quickly identify ailments in sick people. IBM Williams is a well-known and effective health insurance technique that is predicated on a simple survey and reacts predicated on the illness, similar to an x-ray text. Artificial intelligence-based voice recognition tools are increasingly used in the health industry. Medical advancements energized by the artificial intellect are constantly advancing into workable solutions for clinical settings. Smartwatches, cell phones, or other phone surveillance detectors are providing digital information to learning algorithms, which can be used in a variety of medical applications. Artificial intelligence is presently used in only a few healthcare situations, like the identification of atrial fibrillation, epilepsy seizures, and low blood sugar, as well as the detection of diseases premised on histopathology or diagnostic devices. Clients have been waiting for the execution of amplified drugs since it allows for better independence and more targeted therapies; however, doctors have been resistant because they were not ready for such a change in medical care. This occurrence also necessitates the use of conventional drug testing to justify these technological techniques, as well as discussion of healthcare syllabus upgrades in light of electronic drug and ethical considerations of ongoing linked tracking. (iranintl 2022.)

2.4.6 Automobiles

Automobile artificial intelligence is having a significant effect on the market. It can be found all over, from the international automotive economy to driver surveillance and acknowledgment. For driving surveillance, artificial intelligence application is free. The technology can be used to modify the seat, mirrors, as well as heat. But since the introduction of artificial intelligence into the automobiles sector, the landscape has altered. In the auto market, autonomous cars (AVs) are the most visible implementation of AI. The crucial AI techniques affiliated with self are AI chips, computer vision, and machine learning. AI, on the other hand, is critical throughout the entire value chain. Upriver (tier-1, 2, and 3 distributors and auto companies) vision-based and intelligent machines in conjunction with machine learning and machine learning to directly benefited, while upstream (selling and the incredibly prominent aftersales) uses communicative technologies and context-aware devices in conjunction with data science and machine learning. Integrating selling and post-sale vehicle characteristics into forecasting, AI helps to close the feedback system from upstream to downstream, allowing manufacturing being more tightly controlled to request. In particular, are at risk from movement contenders, car manufacturers can now perform in an agile correlation with true occurrences, which is essential to counter disasters like the global epidemic and the automobiles chip scarcity. Automakers and distributors are realizing how far off the application behemoths are, and they are understandably wary of giving over value-added possibilities. (Phillips 2012.)

2.4.7 Human Resources and Hiring

The goal of artificial intelligence in HR and hiring is to improve the pace and finesse of strategic planning while also making choices more accurate and precise. If the hiring manager does not use artificial intelligence in the selection process, the company is wasting valuable assets such as time and funds. As a result, artificial intelligence implementations that automate processes for the recruitment procedure and administrative work contribute significantly to saving assets. Artificial intelligence (AI) for recruitment and selection is the software of artificial intelligence

to the skilled procedure, where computer vision can gain knowledge to blacklist your best replacement and optimize manual processes in the procedure. This technique is designed to optimize or optimize some aspects of the recruitment processes, particularly those that are repeated and high-volume.

For example, technology that performs sentiment classification on position description to predict possible misleading language or applications that relates computer vision to resumes to auto-screen applicants. Rulers in talent development say their employment quantity will boost next year, but their recruitment and selection groups will stay the same length or even shrink.

Interviewers will be anticipated to become more effective by "conducting more with less," as the saying goes. Artificial intelligence in HR means allowing processes to be tailored to the specific needs of employees and their positions to be detached. AI also keeps records of the company's major personal details as well as other complex jobs such as document verification. (Jatoba 2020.)

3 UNDERSTANDING CYBER SECURITY AND DEFENSES

Cyber threats are commonly defined as threats to computer systems. Individual people, collectives, and countries can launch an assault for a myriad of purposes. Whatever their incentive, they frequently seek to change or steal data or obstruct the device or network. Because there are many different kinds of assaults with highly variable degrees of severity, this section will concentrate on the more notable ones (Buchanan 2015.) This will go over existing protections against them as well as look at specific cyber threats that have had a major impact. While most groups have the tools to sense attack patterns, a few still happen. Halting unknown threats, which are designed primarily to get around the newest safeguards by modifying petitions and behavioral patterns, has traditionally been challenging. Many businesses have developed massive investments in building their threat intelligence squad and/or ceding the unavoidable and crucial assignment of continually shifting their defending technics and searching for better equipment and ways to maintain their copyright law and virtual investments protected to system integrators. Knowing how these opponents operate, as well as mapping the firm's defense policy to their life span, demonstrates how they can identify, halt, interrupt, and recoup from an invasion, as well as where their security forces must focus. Cybercriminals are the ones who bring out cyber threats. People who act on their own, trying to draw on their computer knowledge to design and implement serious offenses are known as malicious people, dangerous people, and hacking. They could also be members of a criminal gang that collaborates with other malicious attackers to find flaws or troubles in computer networks, known as security flaws that can be manipulated for financial gain. Cyber-attacks are also carried out by government-sponsored clusters of computer programmers. They've been labeled as nation-state aggressors, and they've been alleged of sabotaging other authorities' information systems (IT) architecture as well as non-government organizations like business owners, nonprofit groups, and utility costs.

3.1 What causes cyber-attacks

Cyber-attacks are intended to inflict harm (Buchanan 2015.) They can have a variety of goals, for example, as listed below here.

Firstly, gaining in terms of money: Cybercriminals initiate most of cyber-attacks presently particularly that are against corporate enterprises, for monetary gain. These threats frequently aim to steal confidential material, such as consumer credit card information or worker private information, which malicious hackers then use to gain entry to cash or products by impersonating the survivors (Nobanee 2018.) Interruption and retaliation. Attacks are also launched by malicious people with the intent of creating chaos, uncertainty, dissatisfaction, unhappiness, or mistrust. They may be acting in this manner as a form of retaliation for acts committed against them. They might be attempting to publicly humiliate the attacked organizations or harm the prestige of the nonprofits. Attacks on governmental agencies are common, but they can also target advertising or nonprofit institutions (Romanosky 2016.)

And secondly, cyberwarfare. Authorities all over the globe are implicated in cyber threats, with many admitting to or suspecting of designing and organizing threats against other nations as part of the ongoing ideological, financial, and cultural conflicts. Cyberwarfare is the term used to describe these kinds of attacks (Romanosky 2016.)

3.2 Types of Cyber Attacks

3.2.1 Web Vandalism

Web hacking attempts are violence that changes the substance of the internet or overpowers its web domain, diverting customers to a bogus site. According to Zone-H, 2003 a webpage repository of variants of graffiti webpages, the number of online defacement threats has already been steadily increasing. In 2003, there have been 300,000 internet defacements noted. Even so, by 2010, the figure had risen to an incredible 1,400,000. Approximately 400,000 defacements

were already noted as of May 2011. From plot kiddies to ideologically biased skillful hacking, the aggressors come in all shapes and sizes. (Buchanan 2015.)

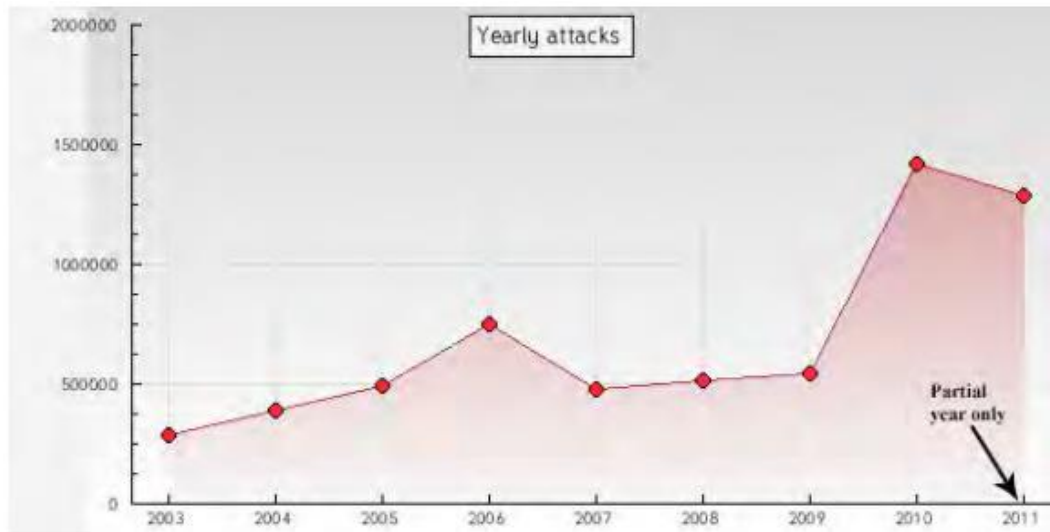


Figure 2: Web hacking in Iran from 2003 – to 2011 (*iranintl 2022.*)

During the 2003 invasion of Iraq, an excellent illustration of politically inspired internet graffiti took place. As per F-Secure, internet defacements began forty-eight-hour shifts before the invasion of Iraq and enhanced throughout the war. The liable hacking was divided into 3 groups, according to the website F-Secure: US-based nationalistic attackers, Islamic extremist organizations from all over the globe, and union activists opposed to the battle. The Figure 4 below depicts the number of online hackings that took place between the 10th and 12th days straight of the Iraq war. (*iranintl 2022.*)

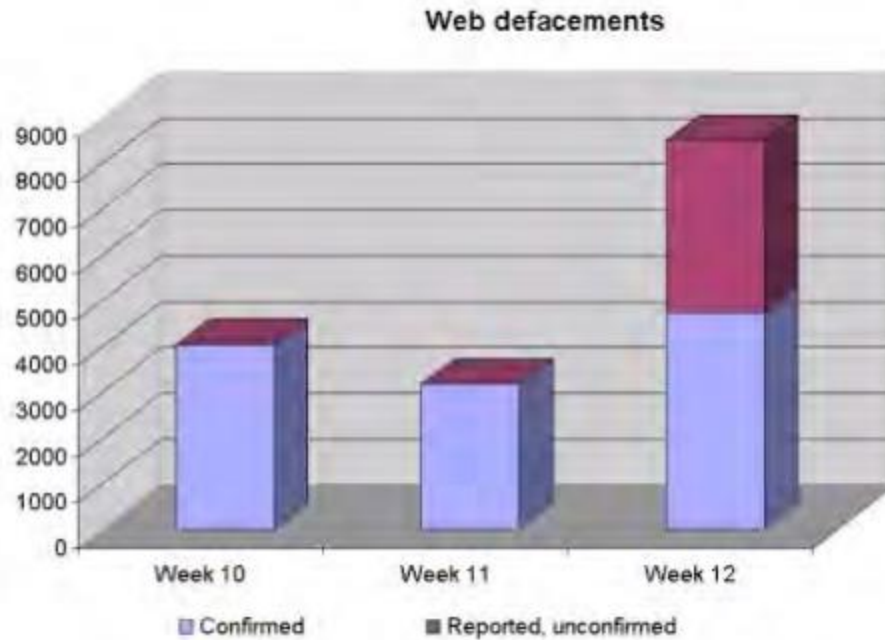


Figure 3: Hacking of website in Iran during war. (iranintl 2022.)

3.2.2 DOS

DOS protocols are launched to ruin or obstruct direct connections to their objectives. Generally, this is accomplished by ingesting the user's bandwidth utilization or emotionally draining reserves on the user's framework. DOS assaults are largely carried out by using bots, which are channels of infected computers infected with malicious code and positioned under the suspect's regulation (Zargar 2013.) Botnets typically remain stagnant once they are assigned by their main server, which can be positioned anywhere around the globe. They have been most commonly used to install malware, but those who are used for forgery and denial of service, with the bots overall carrying out what is known as a disbursed denial of service invasion (Zargar 2013.)

3.2.3 Malware

This segment covers spyware of diverse types including malware, bugs, and Trojan horses. Malicious codes that can connect to other applications and then recreate whenever that technology is run. The consequences can vary from trying to steal delicate details to creating havoc. Worms are spyware that replicates themselves. They could indeed search for and utilize security vulnerabilities. They could also be distributed through external devices including USB thumb drives, as demonstrated by the Stuxnet worm. Trojans are vulnerable to malware that hide their software within a computer system to encrypt. These are frequently models for enabling that give the assaulter complete access to the infected computers. Even if they do not distribute on their own, they have the potential to hit thousands of people through phishing and web uploads. (iranintl 2022.)

3.2.4 Zero-Day Attacks

Such assault happens once an assailant (people or AI-controlled spyware) utilizes a personal computer via an unproduced weakness where no component (fix) has been approved. Though such threats would be less common than those who just manipulate security weaknesses for which manufacturers have issued bug fixes, those who were harder to identify and safeguard against because their watermarks would not be included in anti-malware goods. Furthermore, after a supplier discovers or is alerted of a security vulnerability, this could take a bit of time for a safety precaution to be established and launched. (iranintl 2022.)

3.3 Types of Cyber Defenses

Numerous IT cyber security services manufacturers have aggressively promoted cutting-edge protection services and ideas to protect against varied types of cyber threats. Furthermore, groups have tightened and enforced more strict controls. These initiatives address the storage and disposal of classified intel, the context vetting of persons involved in responsive work activities,

passcode criteria, the examples of special data transmission permitted, the sets of information permitted to circulate among channels, and the recurrence with which services must be fixed (Tyugu, 2013). Types of cyber defenses are presented with a brief explanation below.

3.3.1 Application Protection

This is the procedure for safeguarding confidential material at the software level. The majority of these security protocols should be in place first before the app is released. Security testing may include measures such as mandating the user to enter a complex password. It may also include functionalities like two-factor verification, security codes, and other safeguards to make sure that a user is who they claim to be. (Tyugu 2013.)

3.3.2 Security in the Cloud

Services companies recorded and stored centers can also be included in cloud computing. Recognize the end-user functionality, digital storage protection, data backup, and human mistakes that uncover the system when maintaining adequate cloud security protocols are in place. Managerial subscribers and their network access (identification and security leadership), protecting cloud accounts from illegal access, cryptography and safeguards of cloud-based information assets, and handling its defense capabilities are all duties that fall to the client (compliance) (Tyugu 2013.)

3.3.3 Security in the Field

The risk control for all inner information security is referred to as this term. This approach to management generally incorporates a range of risk mitigation officials to make sure that if a user's information is compromised, there is a fallback clear plan. Employees must be informed of the guiding principles for maintaining personal or financial information safeguard as part of

security procedures. The table below summarizes many of the most recent defense systems for the sorts of threats previously described (Buchanan 2005.)

Table 1: Types of attacks with their prevention (*iranintl 2022.*)

Attack Type	Recommendations
Web Vandalism	<ul style="list-style-type: none"> - Make sure that services are plugged in daily. - Verification of user input to preclude SQL (Structured Programming Language) infusion by ensuring that web screenplays are well authored. - Mobilize applications, such as Tripwire Mitigation Supervisor, to instantaneously reinstate a benchmark replica of graffitied internet pages.
DDOS	<ul style="list-style-type: none"> - Guarantee that services are plugged on a constant schedule. - Deformed parcels should be filtered out by firewalls. - Keep an up-to-date list of banned targeting IP addresses. - Have duplication in your throughput. - Use resource sharing and anomalous demand filtration, such as Akamai.
Malware	<ul style="list-style-type: none"> - Deformed parcels should be filtered out by routers. - Install Intrusion Prevention Systems (IDS) / Intrusion Protection Systems (IPS) / Anti-Virus (AV) and keep their signers up to date. - Keep track of internet traffic. - Use software white ranking, for example, Bouncer.
Zero-Day Attacks	<ul style="list-style-type: none"> - Install an anomalous monitoring program, such as Netwitness.

A security vulnerability is frequently interrelated because it may engage a fusion of the above-mentioned breaches. In the scenario of a worm strike, for instance, this might be distributed by extracting poorly configured computers or both external and internal (zero-day) dangers. Malware including such Trojans and backdoors might be implanted in infected computers following the beginning breaches. This malware may be distributed via removable media, as was

the situation with Stuxnet, or via spam or web uploads. When fitted, the malware might converse with the server-side to earn commands for collection of data, destruction, or DDOS assaults. All of this demonstrates the intricacies and advanced threats, implying that established protections may be insufficient.

3.4 Some cases of cyber attacks

There are various types of cyber-attacks which are plaguing day to day lives of people. The victim of a cyber-crime is not limited in any way. It can happen to anyone from a personal level to a large corporate entity. Some of the cyber-attacks are presented below.

3.4.1 Conficker

The Conficker worm is directly to blame for one of the most widespread parasitic infections ever recorded. It was discovered on November 21, 2008, and has since expanded to over 7 million authorities, companies, and computers in over 200 nations. The French Navy, in which military aircraft have been rooted due to the invasive infections, as well as the United Kingdom's Naval force, as many as three-quarters of its naval vessels had contaminated machines, were among the more significantly affected survivors. The worm enhanced itself 5 times in 6 months, every moment developing extra features and functions including inflammation matrices, diffusion and connectivity techniques, and even self-defense processes (Shin 2011.)

This demonstrates how improvements exacerbate the struggles of protecting against these sophisticated viruses. When a fresh countermeasure, including a revised approval for an anti-virus or intruder preventative measures scheme, is implemented, the worm could be enhanced to beat that process. As a result, protections are always one stage underneath threats (Shin 2011.)

3.4.2 GhostNet

GhostNet relates to a humongous event of a cyber-spying reportedly fomented by China against the Tibetan public, India, as well as other objectives. According to a survey performed by

Cyberwarfare Screen, the GhostNet spyware afflicted over 1300 desktops in 103 nations, with up to 30% of those afflicted being high-value goals available at different agencies of global relations, embassy staff, and other federal buildings. The Information Warfare Screen discovered a "secretive, complicated, and extravagant computer hacker's framework good enough to take absolute authority of compromised systems" by the opposite pioneering the GhostNet framework. Even after the Intelligence Gathering Display's exhaustive investigation, no researcher can conclude who was entirely in influence by GhostNet. While the assailants' IP addresses have been copied to the Island of Hawaii, China, they were inadequate to entrap the Chinese legislature. The machines with all those IPs might have been undermined by proxy servers used to deceive the truthful aggressor (Deibert 2009.) This strike highlighted two key challenges. Numerous public sector connections face challenges, and identity in the cyber world is exceedingly hard to ascertain. The source is extremely crucial as, without it, corrective steps against an abuser cannot be taken (Deibert 2009.)

3.4.3 Stuxnet

The first malware to attack factory influence structures was Stuxnet. These types of technology are found in gas supplies and power stations. Threats on these structures are incredibly severe even though safety was never a priority in the configuration of several industrial systems, making them vulnerable. Whereas Stuxnet is equivalent to the Conficker worm in some ways, it is much more complicated. Stuxnet appears to contain a refined script to recalibrate a Logical Framework Control system in ways that cause structural damage (Stuxnet is presumed to have affected approximately 1000 equipment at Iran's nuclear enhancement institution at Natanz) and misuses four zero-day security problems, in addition to applying very innovative strategies to reach deception functionality and dissemination via USB drives (Langner 2011.) Even though this computer virus was only explored in July 2010, Security software Protection Reply has been able to determine that it originated at least a year before that. The SSR as well discovered over 40,000 distinct exterior IP addresses from 155 multiple nations. The dispersion of Stuxnet raises the issue of whether extant cyber protections are appropriate, especially in the form of equipment (Langner 2011.)

4. AI IN CYBER SECURITY

John McCarthy created the notion of AI in 1956, describing it as the science and technology of developing smart humanoid robots, particularly bright computer software solutions. It's about teaching computer systems to assume, work, learn, and evident especially like beings. Computer algorithms, data analysis, pattern matching, voice recognition, translation software, robotic systems, biometrics, and the internet of things (IoT) are just a few of the areas where AI is now being used. Even after AI's widespread use, human judgment is still designed to check its actions, because it can also be in use for obliteration. Cybercrime is becoming more prevalent, and it now poses a daily threat to the headway of authorities, lenders, and corporate interests through online hackers. Because of their versatility and versatility, AI solutions can help resolve the disadvantages of previous network security toolkits. Though AI is already helping to improve cyber security, there are a few things to keep in mind. Artificial intelligence is seen by some as a potential threat to the world. Researchers and law experts are concerned about the increasing role of self-contained systems. (Sarker 2021.)

The role that Ai systems compete in cyberspace, as well as their ethical justification. AI processes can be tampered with, neglected, and deceived to cause security concerns in application areas such as network surveillance systems, central banking, and self-driving cars. As a result, it's critical to use safe and adaptable strategies and processes. Artificial Intelligence has been used in cyber security to improve defense systems so far. AI can be used to analyze large volumes of data effectively, correctly, and quickly thanks to its powerful machine learning and data intelligent algorithms. Even though the method of strike shifts, Artificial Intelligence sensors detect comparable threats that happen in the future predicated on their understanding and knowledge of previous dangers. Moreover, AI sensors can monitor innovative and complicated changes in attack variation, organization means large amounts of data, and learn to recognize danger based on the specified conduct and networking devices, among many other benefits. Since they are predicted to adjust and improve to situations and are skillful in recognizing even the littlest based on network setups, AI methods do very well in intervention sensing and

enabling reaction to unnamed dangers. As a result, they can be timelier than people regarding evaluating unexpected kinds of cyber-attacks (Timmers 2019.)

Because of pervasive linked devices, cloud, and communications devices, cyber-attacks are more widespread and diversified. Cybercriminals have a lot of base stations thanks to a large number of devices. Furthermore, the connections are not secure. The rise of IoT has resulted in a rising tide of cyber-attacks that has spread further than ever before. Cyber fraud is a frequent topic in the media and social media. Effective cyber security features necessitate an enormous attempt to identify dangers, retrieve threat qualities, and encapsulate threat qualities into data to detect risks (Sarker 2021.) Furthermore, traditional means aren't nearly as refined as today's cyber-attacks. Previously, there was no link between AI and cyber security. However, as time passed, the lines between the two became fragmented. The CAPTCHA is a perfect example of AI and cyber-security working together. The user will be asked to write a letter in a disguised picture or with another distortion in this test. "Signature-based methods" is how effective cyber methods are referred to (Sarker 2021.).

5 CONCLUSION

Cyber threats are becoming more common and dangerous. This could be due to several considerations, such as an increment in the use of machines in several areas, including authorities, army, business, and funding. All recently identified dangers which have not been repaired in infected computers can also be seen as a cause of cyber threat. As evidenced by the numerous cases mentioned, the threats also became more refined. Not only were they successful in overcoming several of their targets' virtual protections, but their culprits were also hard to locate and define. Aside from working to develop detached defensive lines, a need to recognize utilizing active security systems. The research will analyze how energetic safeguards have contributed to ground warfare in the subsequent paragraphs, as well as how several of the notions might be implemented in cyber defending.

REFERENCES

- Ai, Y., Zeng, Z. and Qian, S., 2014. Direct numerical simulation of AC dielectrophoretic particle–particle interactive motions. *Journal of colloid and interface science*, 417, pp.72-79. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0021979713010187>
- Al-Rifaie, M.M. and Bishop, J.M., 2013, March. Swarm intelligence and weak artificial creativity. In 2013 AAAI Spring Symposium Series. Available from: <https://www.aaai.org/ocs/index.php/SSS/SSS13/paper/viewPaper/5728>
- Al-Suwaidi, N., Nobanee, H. and Jabeen, F., 2018. Estimating causes of cybercrime: evidence from panel data FGLS estimator. Available from: <https://dspace.adu.ac.ae/handle/1/2590>
- Bendovschi, A., 2015. Cyber-attacks—trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28, pp.24-31. Available from: <https://www.sciencedirect.com/science/article/pii/S2212567115010771>
- Benko, A. and Lányi, C.S., 2009. History of artificial intelligence. In *Encyclopedia of Information Science and Technology*, Second Edition (pp. 1759-1762). IGI Global. Available from: <https://www.igi-global.com/chapter/historyartificial-intelligence/13814>
- Braga, A. and Logan, R.K., 2017. The emperor of strong AI has no clothes: limits to artificial intelligence. *Information*, 8(4), p.156. Available from: <https://www.mdpi.com/2078-2489/8/4/156>
- Buchanan, B.G., 2005. A (very) brief history of artificial intelligence. *Ai Magazine*, 26(4), pp.53-53. Available from: <https://ojs.aaai.org/index.php/aimagazine/article/view/1848>
- Deibert, R.J., Rohozinski, R., Manchanda, A., Villeneuve, N. and Walton, G.M.F., 2009. Tracking ghost net: Investigating a cyber espionage network. Available from: <https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651>
- Forster, D.A., 2006. Validation of individual consciousness in strong artificial intelligence: An African theological contribution (Doctoral dissertation, University of South Africa). Available from: <http://www.spirituality.org.za/files/D%20Forster%20doctorate.pdf>
- Haenlein, M. and Kaplan, A., 2019. A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, 61(4), pp.5-14. Available from: <https://journals.sagepub.com/doi/abs/10.1177/0008125619864925>
- Jha, S.K., Bilalovic, J., Jha, A., Patel, N. and Zhang, H., 2017. Renewable energy: Present research and future scope of Artificial Intelligence. *Renewable and Sustainable Energy Reviews*, 77, pp.297-317. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S136403211730518X>

Jordan, M.I. and Mitchell, T.M., 2015. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), pp.255-260. Available from: <https://www.science.org/doi/abs/10.1126/science.aaa841>

Langner, R., 2011. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), pp.49-51. Available from: <https://ieeexplore.ieee.org/abstract/document/5772960>

Mariana Jatoba. (2020) "The "Artificial" Consumer: Approaches between Artificial Intelligence and Marketing." In: ANPAD Meetings–Enanpad, 2018. Curitiba/PR–3-6.
<https://www.sciencedirect.com/science/article/pii/S1877050919322045>

McCorduck, P., Minsky, M., Selfridge, O.G. and Simon, H.A., 1977, August. History of artificial intelligence. In *IJCAI* (pp. 951-954). Available from: <https://www.ijcai.org/Proceedings/77-2/Papers/083.pdf>

Noura Al-Suwaidi, Haitham Nobanee, & Fauzia Jabeen. (2019). Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator. <https://doi.org/10.5281/zenodo.3365895>

Phillips-Wren, G., 2012. AI tools in decision making support systems: a review. *International Journal on Artificial Intelligence Tools*, 21(02), p.1240005. Available from: <https://www.worldscientific.com/doi/abs/10.1142/S0218213012400052>

PK, F.A., 1984. What is Artificial Intelligence?. “Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do”., p.65. Available from: https://www.researchgate.net/publication/358058444_Artificial_Intelligence_and_its_Increasing_Importance

Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), pp.4-37. Available from: <https://ieeexplore.ieee.org/abstract/document/8240774/>

Romanosky, S., 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), pp.121-135. Available from: <https://academic.oup.com/cybersecurity/article/2/2/121/2525524?login=true>

Russell, S. and Norvig, P., 2002. Artificial intelligence: a modern approach. Available from: [http://unina.stidue.net/Intelligenza%20Artificiale/Materiale/Artificial%20Intelligence%20-%20A%20Modern%20Approach%202nd%20ed%20-%20S.%20Russell,%20P.%20Norvig%20\(Prentice-Hall,%202003\).pdf](http://unina.stidue.net/Intelligenza%20Artificiale/Materiale/Artificial%20Intelligence%20-%20A%20Modern%20Approach%202nd%20ed%20-%20S.%20Russell,%20P.%20Norvig%20(Prentice-Hall,%202003).pdf)

Sarker, I.H., Furhad, M.H. and Nowrozy, R., 2021. Ai-driven cybersecurity: an overview, security intelligence modeling, and research directions. *SN Computer Science*, 2(3), pp.1-18. Available from: <https://link.springer.com/article/10.1007/s42979-021-00557-0>

Shin, S., Gu, G., Reddy, N. and Lee, C.P., 2011. A large-scale empirical study of conficker. IEEE Transactions on Information Forensics and Security, 7(2), pp.676-690. Available from: <https://ieeexplore.ieee.org/abstract/document/6807753>

Timmers, P., 2019. Ethics of AI and cybersecurity when sovereignty is at stake. Minds and Machines, 29(4), pp.635-645. Available from: <https://link.springer.com/article/10.1007/s11023-019-09508-4>

Tyugu, E., 2011, June. Artificial intelligence in cyber defense. In 2011 3rd International conference on cyber conflict (pp. 1-11). IEEE. Available from: <https://ieeexplore.ieee.org/abstract/document/5954703/>

Verma, M., 2018. Artificial intelligence and its scope in different areas with special reference to the field of education. Online Submission, 3(1), pp.5-10. Available from: <https://eric.ed.gov/?id=ED604401>

Winston, P.H., 1992. Artificial intelligence. Addison-Wesley Longman Publishing Co., Inc. Available from: <https://courses.csail.mit.edu/6.034f/ai3/rest.pdf>

Zargar, S.T., Joshi, J. and Tipper, D., 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), pp.2046-2069. Available from: <https://ieeexplore.ieee.org/abstract/document/6489876/>