Sri Lanka Institute of Information Technology

Artificial Intelligence for Smarter Cybersecurity

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT19029146	Eranda H.P.D

25/04/2020
Date of submission

Table of Contents

Abstract

This report on “Artificial Intelligence for Smarter Cyber Security” is submitted in order to fulfill the aim of creating awareness of current emerging topics in cyber security. This report is created as an assignment for the course Introduction to Cyber Security (ICS) – IE2022 for the degree BSc. (Hons) in Information Technology at Sri Lanka Institute of Information Technology.

This report would not have been a success without the kind support and guidance of the lecturer in charge for ICS module.

Firstly, I would like to thank our lecturer, Mr. Amila Senaratane for his kind, consistent support and guidance throughout the assignment. He greatly contributed in selecting a suitable topic for the assignment. He guided us which areas should be covered and how the topic should be changed accordingly.

So I express my greatest gratitude to my lecturer once again for giving me suggestions and recommendations to improve this report.

I can assure you that this report is designed according to the IEEE referencing standards and styles. All the undergraduate students at SLIIT who follow ICS module were asked to select and register an emerging topic in cyber security. The topic that I selected is “Artificial Intelligence for Smarter Cyber Security”.

I have divided the content of the topic under 5 main sections.

1) Introduction to the topic
2) Evolution of the topic
3) Future developments in the area
4) Conclusion
5) References

Under the “Introduction to the topic” section we are trying to achieve the basic and the general idea of the topic. This includes what is actually meant by “AI for smarter cyber security”. This also contains the combination and the explanations of both artificial intelligence and cyber security. Here, what we are actually trying to achieve is to get a basic and a broad understanding about “AI for smarter cyber security”.

Then under the section “Evolution of the topic”, we basically target the history of the usage of AI in cyber security. Not only about the history only, we are going to discuss about the gradual development of the usage of AI in cyber security. After that under this section we are going to discuss about the current situation, implementations and the modern trends related to that topic.

Then we are hoping to discuss about the “Future developments in the area”. Under this section we are going to discuss about the possibilities, predictions and the real world usage of artificial intelligence in cyber security.

After that we are going to wrap up the whole gathered information and create a final single conclusion.

Then at the end we are going to wind up the report by providing the necessary references that we used to gather information.

1. Introduction to the topic

What is Cyber Security?

“Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.” (cisco.com) Most of the cyber attackers’ aim is to access, change or destroy sensitive information. But some attackers’ one and only intension of performing a cyber-attack is to transfer or steal money from users. So in order to prevent and get protected from these kinds of cyber-attacks, a well-defined cyber security mechanism is a vital necessity for any organization.

In a successful cyber security mechanism, usually it contains not just only one layer of protection. It contains multiple layers of protection across the both software and hardware. In order to gain the trust of the customers, a proper cyber security mechanism is a must for any organization.

Cyber security is a massive specialization which affects and contributes each and every other sector in the society.

What is Artificial Intelligence (AI)?

“Artificial intelligence (AI) is wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence.” (builtin)

When people get to hear the term “Artificial Intelligence”, the first thing that comes into their minds is about the robots. The modern science-fiction movies have influenced a lot for the people who actually believe in that theory. But the reality about artificial intelligence is more advanced and interesting than you could ever imagine.

The main goal of AI is to give machines the intelligence that humans already have. Basically what it does is, machines are trained to think and act logically just like humans. The practical usage of artificial intelligence is massive when it comes to the modern world. Almost all the sectors in the society are affected and contributed by the AI.

Aggregation of Artificial intelligence with Cyber Security

Both artificial intelligence and cyber security can be considered as cutting-edge technologies. When these technologies combine with each other it becomes just like a double-edge sword. In modern world not only the organizations, but the attackers also had begun to get the help of artificial intelligence technology. There is a possibility of cyber criminals using AI-enabled malware to evade detection. So if AI is aggregated with cyber security properly, most certainly it becomes the most powerful and the dangerous weapon of all time. In modern world cyber security sector has become very much vital than ever in the past. Data breaching, identity thefts, malware attacks and may more cyber security related threats have risen up rapidly throughout the last few years. More than 42% companies of the world have been affected by such kind of threats.

As a more efficient and a timely solution, Artificial Intelligence comes in handy specifically for this problem. According to a research, two out of every three organizations are willing to pay any amount of money for strengthening cyber security with artificial intelligence. Artificial intelligence is a massive and a broad field of expertise which is growing day by day hugely. So AI has not been widely spread in the field of cyber security yet when compared to other sectors in the modern society.

As you already know, cyber security is a field which obviously has a never-ending cycle of offensive-defensive strategies and innovations. So when the strength of artificial intelligence is combined with cyber security, the data and the network vulnerabilities seems to be reduced in a considerable manner. But this does not mean that the data is completely breach-proof.

Artificial intelligence can systematically analyze user behaviors, understand patterns and identify all kind of abnormal situations within the network. So with help of AI, it has become much easier to find out the vulnerabilities of a system quickly.

How AI helps in intensifying the security level

AI uses very complex and sophisticated algorithms in order to analyze large amounts of data. In reference to cyber security, it is capable of learning new methods to detect and predict hidden patterns of threats and vulnerabilities in order to prevent cyber-attacks and security breaches. There are occasions that security breaches occur due to human vulnerabilities too.

As an example, consider a powerful phishing attack which is capable of breaching the security defenses of a system. In such a scenario AI can boost the security of the system by investigating the sources of emails for possible threats. An artificial intelligent software can be developed to identify the credibility of both the sender and the source before accepting or blocking the message. This software can be programmed to grasp and inspect the address, attached links and the message characteristics.

Usually security programs find out malicious software using the technique ‘known signatures’. But with the help of the AI tools, now it is possible to identify malware using equivalent characteristics, rather than just the signatures that are known before. Not only that, AI possesses the self-learning ability which is surely going to help in detecting new malware types. Currently most of the security solution companies want to implement AI at each and every layer of defense, including cloud apps, end-user devices and websites.

How AI contributes in saving time and money

Without artificial intelligence humans won’t be able to achieve the same level of protection against the potential cyber threats. Not only that AI increases the speed of security products and also it reduces the costs when maintaining those security products. Implementing AI in cyber security prevents security analysts from wasting their valuable time on researching false alerts and dead ends. It also helps a lot in reducing the risk of malicious activity running in background while they are working on false positives. If AI is implemented properly in cyber security, it can use human-like instincts to find out abnormal activity for further analysis by humans. So this helps a lot in saving the time of the security analysts.

2. Evolution of the topic

At the very beginning cyber security and artificial intelligence are completely different pieces of technology. There had not been just even a single connection among cyber security and artificial intelligence. Both of those massive technologies had their own paths and futures.

Actually, the artificial intelligence technology was discovered way before than the cyber security was discovered. The term “Artificial Intelligence” was first brought in by John McCarthy in 1956. His idea was to create a machine that can learn, think and work as a human by itself. Then his idea was developed more and AI powered algorithms were used to play chess games. But later on AI began to spread widely into massive amount of sectors in the society including the cyber security sector.

If we concern about the history of cyber security, it draws back us to 1970s. At those time periods there were no such words like ransomware, viruses, spyware, worms, SQL injection, cross-site scripting etc. Those days both computers and the internet were still under development. So that it was very easy to identify any kind of computer security related issues in 1970s. The most of the threats occurred because of the inside intruders. Not only that, network breaches and malware also existed up to some extent in those days too. Most of the attackers’ only purpose was to earn a financial gain from performing such kind of attacks.

Those days, Russians used them to show off their cyber power as a form of weapon. A German computer hacker named Marcus Hoss hacked into an internet gateway in order to connect to the Arpanet. Then he gained access over 400 military computers, including the Pentagon’s mainframes. His only intension was to sell the acquired information to the Russian spy agency, KGB. However an astronomer called Clifford Stoll used honeypot systems to detect the intrusion and was able to prevent it from happening.

The 1980s were called as the “The Era of Computer Worms”. The first worm in the world was called Creeper, and it was designed to travel in between Tenex terminals. It printed the message “I’M THE CREEPER: CATCH ME IF YOU CAN.” Then the 1990s era was the time period where the computer viruses began to rise up. So that the in early 1990s, companies began to create and retail antivirus products. Those products were capable of scanning the computer system for potential viruses and worms. At that time, the available antivirus solutions were created and tested with a database which consisted with signatures. But with the time, those antivirus solutions began to fail because it affected the performance and productivity of the system.

When we consider about the security, a security system should be capable of separating good from bad, normal from abnormal. So it is very much vital to implement anomaly detection for the sake of the security. An anomaly detection was begun in 1987 when researchers started building intrusion detection systems (IDS). Around 1998-1999, DARPA (the government agency that created the Internet) started to do researches in machine learning in cyber security. AI uses machine learning in order to detect similarities and differences within a data set and report any anomalies. Anomaly detection uses unsupervised learning, which is a type of self-organized learning mechanism. It is capable of finding previously unknown patterns in a data set without the use of pre-existing labels.

Machine learning is also actually a part of AI which helps to recognize patterns in data and predict effects based on past experience and data. Usually AI based systems use machine learning technology in order generate results that replicate human functioning. When machine learning is combined with application isolation, it prevents the drawbacks of malware execution; isolation eliminates the data breaching and it ensures that data is not compromised and that malware does not move sideways onto the network.

The year 2018 is considered as a record year for stealing highest amount of data as a result of cyber security breaches. In year 2016 only, 357 million malware were detected. The usage of the Internet of Things (IoT) caused a lot in increasing the threat of cyber-attacks. Not only the data security, but the network systems security is also a huge matter of concern especially for the business organizations.

So as you can see traditional methods of detecting malware and cyber security threats are failing again and again. Cyber criminals have also become more powerful than ever especially in bypassing the firewalls of organizations using very complex and advanced mechanisms. The one and only remaining solution to fight this is to be more prepared and smarter than the hackers.

So due to this prevailing situation, security analysts recognized that Artificial Intelligence (AI) is the only hope and the solution for this crisis. Humans are not capable of detecting the abnormalities at the speed that the attacks happen. However when AI is integrated into those systems, it get the ability to analyze a massive amount of data generated on a network in order to identify what doesn’t belong there.

A practical application of AI, machine learning helps in anti-malware, performing dynamic risk analysis and detecting anomaly. Not only that AI technology can be used to train or learn when removing the noise or unwanted data and it assists security experts in understanding cyber environment for detection of any anomalous activity.

In modern era, cyber security systems can be divided into two types.

1. Expert Systems (analyst-driven)
2. Automated Systems (machine-driven)

➢ Expert Systems (analyst-driven)

- Expert systems are mostly developed and managed by people. Those systems are usually based on identification of threat signatures to prevent attacks.

  ✓ Ex :- a fingerprint database is used to capture the intruders and criminals.

- But there is one drawback in expert systems. It is not possible to recognize and enter the threat signatures in to the base until the attack has been completed. So such systems do not possess the ability to protect against previously unknown attacks called zero-day attacks.

➢ Automated Systems (machine-driven)

- Automated systems are capable of identifying potentially harmful or dangerous actions in a system or network by analyzing the historical data. So automated systems is a very good solution for a typical classification problem like this. This approach is heavily successful when dealing with zero-day attacks.

Cyber security is a specialization which requires manpower a lot. So there are huge opportunities for artificial intelligence automation. AI is capable of transforming cyber security to a whole new different level. Not only that, AI makes all most all the cyber security related operations more accurate and effective. According to a current research white hat hackers are working on identifying vulnerabilities and suggest fixes using the AI technology. But the most important and the critical fact here is that the security developers need to empower the cyber security with AI at a faster rate. Because the attackers too have already begun to get use of this technology.

Artificial intelligence is an open technology. It can be used for both good and bad. So it is a huge responsibility of all cyber security employees to protect this technology from going into the wrong hands.

Currently, the majority of the data breaches occur at the application layer. There are multiple reasons that cause the application layer vulnerable to cyber-attacks.

1. The mistakes which are done by the developers when writing the code.
2. Lack of effective planning and testing.
3. Lack of knowledge in cutting edge technology such as cloud, serverless etc.

So as you can see, most of the systems become vulnerable to data breaches and cyber-attacks due to human error. So AI is perfectly capable of resolving this issue in a very efficient manner.

Practical usage of AI in cyber security

1) Automated Malware Defense

- Today most of the traditional security systems often fail to handle a great number of malware correctly. So that AI systems can be trained to identify even the slightest behaviors of ransomware and malware attacks before it enters the system. After identifying those, it isolates the ransomware or malware from that system.

- When it comes to the traditional systems, in order to identify potential threats, signatures are used to check for the existence of a specific sequence of characters in the binary code of a program. But as malware does not come from the binary code all the time, skilled hackers know how to be prevented from such a situation.

- As a solution for this problem, a behavior-based algorithm was created. This algorithm not only analyzes the code directly, but also uses probability models on order to take into account multiple scenarios and attributes of the malicious code. Even though this algorithm had huge amounts of drawbacks. The main downsides of those algorithms are the ineffectiveness and the higher cost.

- So later on a very effective algorithm was found out and it was called as “Heuristic algorithm”. It is very powerful weapon powered by the AI. This AI powered algorithm was totally capable of making decisions about whether the analyzed code is harmful or not. The main advantage of this algorithm is that it has the ability to evolve and adapt by itself.

2) Automated Phishing Detection

- Phishing attacks are created in order to grab or steal your sensitive information such as login credentials, phone number, credit card numbers etc.

- Rather than the general phishing attacks nowadays there is a very popular attack type called spear phishing attacks. Spear phishers obtain private information of a specific user by researching the background of that particular individual and companies on social media, linked websites and other publicly available information. So cyber criminals use those gathered information in order to convince the victim to perform a specific task.

- So in a case like this, AI helps to classify the messages just like in email spam filters. But initially you need to train the algorithm manually by labeling messages or reporting suspicious links. As AI is capable of self-learning, it constantly improves its accuracy.

3) Automated Data Theft Detection

- One of the most common threats that organizations are currently facing is data breaches. In such scenarios AI based algorithms can be heavily used to identify the stolen data. Most of those stolen data are usually laid on the dark web.

- So in order to reach the dark web a person needs to use special browsers such as the Tor browser.

- In such browsers, the connection is encrypted peer-to-peer. Not only that there are some certain safeguards like CAPTCHA need to be applied too.

- But with the help of the AI, it is possible to fool these systems by implying that the CAPTCHAs are done by a human. Not only that using machine vision, images could be analyzed in real-time in a very effective manner.

4) Honeypot-based Social Engineering Defense

- Exploiting human psychology is simply called as social engineering. Attackers use this technique in order to obtain personal information which leads for compromising security systems. Neither hardware nor software alone can prevent such kind of attacks from happening. The only possible countermeasure for this prevailing issue is utilizing social honeypots. That means in order to entrap the malicious attackers, fake persona decoys can be used.

- So in here, AI is used to make sure whether the sender is malicious or friendly. This classification is done automatically and then it is disseminated to the devices of all the employees. So that it automatically blocks further unnecessary communication attempts which are received from the offending party.

Integration of AI into Application Security

1) The Defensive Approach

Owing to the substantial ineffectiveness at securing applications at the development stage, is combined together with the disappointment at the WAF customer end due to a lack of automation and coverage of the emerging threats, defensive Runtime Application Self-Protection (RASP) technology is commonly used. This approach usually depends on the assumptions that malicious activity does abnormally rather than normal activity. So that it can be identified and the threats can be blocked at the real time. This defensive approach is very much effective and highly successful. But as you know an application cannot be protected fully due to many reasons.

- No AI model is 100% perfect and accurate. So the RASP technology is not capable of protecting against all kinds of vulnerabilities.

- More complex problems, such as business-logic flow vulnerabilities and valid feature exploitations are harder to detect because of the healthiness of that requests. This complexity issue caused the failure of the antivirus solutions in the 1990s, at detecting virus signatures in order to block them.

- RASP acts just like a shield. It is not capable of absorbing blows constantly.

2) The Semi-Automated Approach

Effectively and efficiently going through the vulnerabilities in order to detect the real vulnerabilities is a massive task and there are nowhere near enough human resources to tackle the volume of information and data that are produced, let alone to stay ahead of threats. At modern days, AI is used to guess the credibility of the vulnerabilities. So this helps a lot in reducing the manual time which is needed to identify the real vulnerabilities. Most advanced AI combined application security testing solutions are capable of reducing the number of false-positives by up to 98%, which actually saves valuable time and money both. But this approach also has its own disadvantages and problems.

- Only the known vulnerabilities are evaluated. So there is no way of finding new vulnerabilities.

- This method depends on significant updating of the database of vulnerabilities. But this problem can be solved using the AI.

- The manual completion of the final filtering process and assessment of the false positives is compulsory because this kind of AI will never be able to understand and identify the complexities of much more vulnerabilities and to correctly classify them.

3. Future developments in the area

There is no doubt that the future of cyber security is going to reach a whole new different level with the approach of artificial intelligence. Private business organizations and corporations have already deployed AI based cyber security systems. Not only that even some governments have also started using this technology. When AI is integrated with the cyber security, it helps a lot saving both the time and effort of all cyber security employees. So they can sit back and watch until the AI does its work perfectly.

Cyber Security is a specialization which keeps on evolving constantly with the time. So that, especially the business organizations need to remain updated on legal requirements like CCPA and GDPR.

There were some considerable amounts of cyber security trends in year 2019 too such as spear phishing attacks, Internet of Things (IoT) ransomware etc. But it is predicted that future trends of cyber security might heavily invest on artificial intelligence.

According to a research, currently one of every five organizations uses AI to enhance cyber security. It is estimated that 63% of the organizations are going to establish AI in cyber security in the future.

Not only that, it is predicted that companies will begin to move on with AI in order to assure data security, network security and endpoint security.

Future possibilities and predictions of AI based Cyber Security

1) Growth of Zero Trust Attacks

- In the year 2020, it is expected to see an increment in the preventative approach of deep learning environments which will sure become outdated and dangerous in near future. Real time data, analytics and AI together creates a very powerful and productive mechanism to secure the data. Currently there is a considerable amount of employee shortage of cyber security experts. So AI-based solutions is going to help in solving this evolving problem.

- Companies might also encourage their teams to look for modern ways of doing things, such as get the help of AI to implement more productive solutions that is capable of preventing data breaches.

- Scammers are considered as one of the most difficult problems to tackle with. So with the growth of AI, there might be new solutions in the future in order to detect such kind of scammers.

2) The end of passwords

- Currently most of the internet users create their own passwords when creating accounts online. But most of the people still use simple passwords or they use the same password for multiple user accounts. So this has clearly made their accounts vulnerable to cyber-attacks.

- But we have to admit that there have been improvements in password manager software in recent past. Currently those software use algorithms to suggest strong passwords for the users. But what this countermeasure actually does is that it only reduces the chances of been hacked.

- But with the help of artificial intelligence technology it is possible to create a much safer online environment without passwords. According to a research by "New advances in the world of identity and access management" (IAM) it is suggested that in near future passwords might actually be replaced by AI systems.

- By using this idea, AI gets the ability to track each and every user within an organization based on roles, privileges, and common actions. If any kind of abnormal deviation is detection, then that person is flagged and asked to use a second form of authentication, most probably the biometrics such as fingerprint ID or face ID.

3) Threat Hunting

- Threat hunting is a perfect AI based matured solution for disruption of data. As a traditional technique, signatures and indicators are used to identify the threats which have been previously encountered.

- However those traditional methods are not very effective and productive when it comes to identifying new threats. Not only that sometimes the detection gives false positives too.

- So in order to give a better solution for this issue, both AI and traditional methods are integrated together. So this technique can gain a huge success resulting in close to 100% detection rate while minimizing false positives.

- Not only that, AI can be used to escalate the hunting process by merging with behavioral analysis. Startups such as “ReaQta” are capable of influencing the AI models to develop profiles of every application within an organization’s network by absorbing the data which is produced in high volumes by different endpoints.

4) Minimize human involvement in Cybersecurity

- Any person who is dealing with cyber security needs to be observant at all the times. Since from the past it was done manually by a team of cyber security experts. But with the approach of AI, it is possible to shift the workload into the machines. When compared with humans, the speed and the accuracy of those AI based algorithms are at top level. Not only that, the errors which are done by the machines are also lesser compared to human.

- So this is going to help a lot in reducing the workload and the dependency of humans. Not only that AI algorithms can be developed in such a way to detect and track more than 10,000 phishing emails. If this process is supposed to be done by a team of humans, then it might consume a massive amount of time and labor. So powering up cyber security with AI is definitely going to increase the productivity and the effectiveness of detecting malicious activity in the future.

5) Bypassing Security Controls

- So as you have heard before, AI can be used for both good and bad in the field of cyber security. It's predicted that threat actors might influence analytics and AI in order to bypass security controls.

- So as predicted many of those threat actors might be state-sponsored in the future. They are surely going to increase their use of AI algorithms in analyzing the defense mechanisms of their organizations. So that the threat actors can adjust their attacks to their particular weak areas.

- Not only that, the cyber security experts have also given another prediction that the attackers might be able to affect artificial intelligence technology in order to plug into an organization's data streams. So that they could use those gathered information to organize more advanced and critical attacks.

6) Using AI for Account Takeovers

- According to The director of AI at Kount, Josh Johnston, there is a prediction that AI might be used as a weapon frequently in order to takeover user accounts. So in order to prevent such kinds of attacks, the solution must also have to be based on AI.

- Soon in the future, the average consumer will realize that the password protections are not up to the secure standards as it should be. Although there are some secure algorithms such as captcha, they are not reliable as much as they meant to be.

- So in the future, AI is going to become vital in protecting the users' sensitive data such as account credentials and transaction details etc.

7) Fighting AI with AI

- One of the most popular cyber security experts, Brian Foster predicts that cybersecurity in future years might alter the way we fight against threats.

- Nowadays there is a considerable amount of very talented hackers in all around the world. They are capable of using the AI technology in order to exploit vulnerabilities and gain access to valuable business systems and data. So such kinds of processes have automatically created a competition between the hackers and the cyber security experts.

- So in near future, there would be a massive competition or may be a war between those 2 parties, in order to gain more control over AI. So that the security experts need to keep keen eye on those hackers 24/7.

- So according to the predictions, AI based solutions might be used in the future in order to prevent AI based cyber-attacks.

4. Conclusion

So now, let’s wrap up all the things we have discussed so far related to this topic. Cyber threats are extremely increasing since from the past decade. Cyber criminals have begun to use more sophisticated and more complex mechanisms to perform cyber-attacks. So in order to mitigate such kinds of attacks, cyber security experts had no other options left rather than integrating AI technology with cyber security.

Both government and private sector have given their maximum attention in integrating AI with cyber security. The biggest advantage of AI based cyber security is that it has the ability to automate threat detection at a lightning speed. Not only that, AI powered cyber security is capable of minimizing the human involvement in security processes. So it helps greatly in saving both the time and effort of cyber security experts. As a positive side effect, reducing the human involvement in security processes causes less errors and mistakes.

In near future, password protection and authenticity detection systems are going to be compromised. So in order to prevent from AI based cyber-attacks, the only solution is to use AI powered authentication mechanisms. Biometric login mechanisms such as fingerprints, retina scans, palm scans and face scans have to be used in future in order to prevent form such kinds of attacks.

Artificial intelligence is an open technology. It can be used either to protect the systems or to exploit the systems. So it is perfectly fair to call the AI technology as a “double-edged sword”. White hat hackers intensify the cyber security using AI, while the black hat hackers try to exploit and steal data and money using AI. So it’s massive responsibility of the security experts to prevent AI technology from going into the wrong hands.

In the near future, there might be ransomware attacks on cloud storage technology too. So it’s better to do research complying with AI and stay on alert to face such kind of crisis in the future. Otherwise people's faith on cloud storage is surely going to explode in near future.

According to me, I believe that in future the traditional apps are not going to last much longer. Researches have to be done in order to give those apps the ability of self-healing from cyber-attacks.

5. References

1) https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

2) https://builtin.com/artificial-intelligence

3) https://www.sciencedirect.com/science/article/pii/S0020025519300763

4) https://www.vice.com/en_us/article/3knz98/dark-web-site-robocalls-to-steal-credit-card-pins

5) https://s3.amazonaws.com/envisioning/tdb/files/KGuSbXkxuM5GazuDC

6) http://www.freepatentsonline.com/10187407.html

7) https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.html

8) https://s3.amazonaws.com/envisioning/tdb/files/iG9CN88GNwtjt5XYS

9) https://s3.amazonaws.com/envisioning/tdb/files/onW6zKbwaWB7JYPPF

10) https://www.vice.com/en_us/article/3knz98/dark-web-site-robocalls-to-steal-credit-card-pins

11) https://becominghuman.ai/why-you-should-use-artificial-intelligence-in-cybersecurity-204dbe33326c

12) https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/