# ARTIFICIAL INTELLIGENCE IN CYBER SECURITY – THE NEW APPROACH TO CYBER CRIME REGULATION


- **Abstract**

*The World is fast moving toward a digital age, where there is a growing dependence on digital technology and use of internet. The recent pandemic situation has further increased this dependence. But as the familiarity to the digital world increases, so does the probability of frequent and more advanced cybercrime. There is hence, a need to upgrade the security measures to be able to face the advanced nature of cyber-attacks. This paper attempts to determine whether introduction of Artificial Intelligence in cybersecurity will create a better safeguard against cybercrime. The author will be using the doctrinal form of research for this paper, using secondary resources such as other papers, articles, case studies and existing legal provisions. The paper focuses on three main areas of research – possible positives and negatives of artificial intelligence in cybersecurity; the existing regulation measures and possible issues in regulation if artificial intelligence is used. The conclusion of the paper is formed from the author's opinion and suggestions.*


***Keywords**: Artificial Intelligence, Cybersecurity, Cybercrime, Hacking.*

- **Introduction And Background**

The 21st century has already been branded as the 'tech-savvy' century and the age of digital and technological advancement. Everything from banking to applying for a license to even ordering clothes and food can now be done online. Post the recent outbreak of the Coronavirus and the subsequent lockdown, several businesses suffered, and as a result, many of them started online services. This growing technological and digital industry now includes online gyms, online distribution of fresh produce and even online education for schools and colleges. The pandemic has thus increased our dependence on the digital and technological industry.

But with this growing dependence, there has been an increase in sharing and exchanging of data online, which has led to an increase in the incidence of cybercrime. And as the industry advances further, newer and more advanced forms of cybercrime have appeared. Hence, a major concern today is the security of data exchanged and the security of the devices involved in the exchange. Cybersecurity - and adequate cybersecurity, at that – is nowadays a hot topic today.

Another growing topic since the past few years is Artificial Intelligence (AI). Artificial Intelligence is essentially a mechanism or program that enables a hardware to think for itself and make its own decisions. Although AI is a discipline in itself, it has a very wide ambit and can include anything from an application that can figure out and solve a problem by itself to an application that can develop emotional intelligence and function

accordingly.[1] It has several subset disciplines too, such as Machine Learning and Deep Learning.
Over the last few years, there have been several uses of AI in different applications. Some examples include:

1. *Alexa by Amazon and Siri by Apple*: These two applications are examples of the AI based application that can understand and interpret human language by itself and act according to the command given, also known as Natural Language Processing.[2]

2. *Robot technology*: AI application can enable machines to think for self and identify some basic tasks. This has helped in creating robots that can do simple household tasks, such as vacuuming of floors, etc.

3. *Autopilot technology*: AI intervention has been used to enable automatic piloting of an airplane. This technology has even progressed to self-driven cars.

There is even research going on about developing of an intelligence superior to human intelligence. The matter of cybersecurity though, is different.

A superior form of artificial intelligence would be what is required in order to integrate AI into cybersecurity, since any application in cybersecurity would need to recognize the threats and possible incoming attacks on a device. The more invested we become in artificial intelligence, the more probability there is of the technology turning on us, such as the rise of Ultron in the Avengers movie. Ultron was initially created as a security program, which developed a further upgraded intelligence and tried to destroy the world instead.

This is where the problems begin. Not only is the nature of advanced AI difficult to manage and interpret, but the principle of cybersecurity in itself is slightly flawed. Cybersecurity usually follows the 'fixing the plumbing' approach, where the defense develop an ad-hoc response based on the attacks taking place.[3] Therefore, it can be said that cybersecurity solutions are usually limited to a short term vision, because they cannot be developed until the nature of the attack is known. Any preventive measure or experimental technique always carries the risk of causing more problems than solving them. AI can help solve the short-term vision problem, but the consequent risk associated with increases manifold in this situation.

At the same time, the people on the other side, the propagators have also discovered and developed artificial intelligence, resulting in more advanced and untraceable forms of cybercrime that cannot be prevented through hastily constructed firewalls. For instance,

---

[1]IBM Cloud Education (2020). *What is Artificial Intelligence (AI)?* [online] Ibm.com. Available at: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence [Accessed 19 Dec. 2020].

[2]*Id.*

[3]Benoit Morel (2011). *Artificial intelligence and the future of cybersecurity*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/254006500_Artificial_intelligence_and_the_future_of_cybersecurity [Accessed 19 Dec. 2020].

the start-up Darktrace has discovered several kinds of AI based attacks that could not be countered with available, human-paced thinking.[4] The issue of AI – influenced cybercrime hence, has already reached the stage that calls for 'fixing the plumbing'.
This papers focuses on the issue of integrating AI into mainstream cybersecurity and its impact. The paper begins with a background and introduction as stated above, followed by forming of the research question and the methodology to be used. This will then be followed by an analysis that will be two-fold, the first on the pros and cons of such a decision and the second on the existing regulation measures. The opinion formed on the basis of this analysis, along with recommendations, if any, conclude the paper.

- **Literature Review**

1. Benoit Morel's position paper titled *Artificial Intelligence: a Key to the Future of Cybersecurity*[5]: This position paper discusses on the position of AI in cybersecurity not as some individual application based on pre-existing techniques but rather as a specific type of security measure.

2. Forrester's study titled *The Emergence of Offensive AI*[6]: A study discussing the gradual increase of use of AI in cybercrime and its impact and concerns.

3. Library of Congress's study titled *Report on Regulation of Artificial Intelligence*[7]: A comparative study of the various regulatory measures taken in relation to AI at a global level.

- **Research Question**

The research question formed by the author for the purpose of this paper is whether the introduction of artificial intelligence in cybersecurity will create a better safeguard against cybercrime, or result in a worse situation for cybersecurity.

- **Research Methodology**

The research used for this paper is secondary or doctrinal research. The sources of doctrinal data for the purposes of this paper include other research papers, reports, articles existing regulations and legal provisions, all related to the topic. The method of referencing used by the author for this paper is the 19th edition Bluebook method.

- **Analysis**

---

[4]Forrester, *The Emergence of Offensive AI*, DARKTRACE, (Feb, 2020), https://www.darktrace.com/en/resources/research-forrester-offensive-ai.pdf [Accessed 19 Dec. 2020].

[5]*Supra* note 3.

[6]*Supra* note 4.

[7]Loc.gov. (2020). *Regulation of Artificial Intelligence*. [online] Available at: https://www.loc.gov/law/help/artificial-intelligence/index.php [Accessed 19 Dec. 2020].

The approach used for the analysis of the research question is two-fold, focusing on overall three areas – the pros and cons of AI in cybersecurity, the existing regulations on AI and the issues in regulating AI within cybersecurity. The first section deals with use and pros & cons of AI in cybersecurity, and the second sections analyses the regulation aspect.

### *Artificial Intelligence in Cybersecurity*

As discussed above in the introduction, AI already has quite a few applications developed in various areas. However, with respect to cybersecurity, although it is mentioned in the context, it is not a popular area of interest. Pre-existing AI techniques may be used in one of more applications of cybersecurity, but the focus here is on specific AI techniques which concentrate wholly on cybersecurity, i.e. mainstream integration of AI in cybersecurity. There are several reasons for this, the main among them being – lack of predictability and fear of vulnerabilities.

A study conducted by Deloitte[8] revealed that executives and proprietors are aware of the risks posed by AI since it is used in so many products and services, and as a result their major concerns are mostly related to AI based cybersecurity vulnerabilities.[9]

Identification of and recognition of a cyber threat is a tedious job, since it requires repetitively scouring compiled and non-compiled data and finding anomalies within it.[10] Post this, to be able to analyze the attack's consequence and line of response or counter – measures also, further data analysis and review is needed.[11] At a human pace, not only are these processes slow, they also become very time- consuming and tedious leading to human errors. AI on the other hand, can do the same thing at a much faster speed and more accuracy. AI also doesn't need to wait for an attack to actually take place as its inbuilt application can anticipate and predict attacks as well. Apart from this, there are several areas where monitoring the inflow and outflow of data can be conducted by AI at an accuracy that cannot be matched by a human analyst, such as network traffic, email communication, etc.[12] Further, AI can have successful integration in antivirus software as opposed to traditional antivirus software, as an AI based software can detect new viruses faster by detecting anomalies, without needing security updates.[13] Thus, mainstream integration of AI in cybersecurity can result in some beneficial applications.

---

[8]Deloitte United States. (2019). *AI and Cybersecurity Concerns*. [online] Available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/ai-and-cybersecurity-concerns.html [Accessed 19 Dec. 2020].

[9]*Id.*

[10]Raghav Bharadwaj (2019). *Artificial Intelligence in Cybersecurity - What's Possible Today*. [online] Emerj. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/ [Accessed 19 Dec. 2020].

[11]*Id.*

[12]*Supra* note 10.

[13]*Supra* note 10.

Another area which is a growing concern is the use of AI in cybercrime. Hackers are just as well acquainted, if not more, when it comes to AI. A study by Darktrace revealed that various new and offensive forms of AI based attacks have emerged which can cause stealthier and speedier attacks and wipe out/corrupt the data of an organisation easily.[14] There is another category of attacks as well, termed as 'under the radar' attacks or 'low and slow attacks' by Darktrace.[15] These are attacks which are several small individual actions compiled into a large threat. Each individual action is too small to classify as a threat and can easily bypass traditional security software, until it all compiles and becomes an attack. Both of the abovementioned concerns can only be defeated by using AI based security techniques or software. Considering this, AI integration becomes a necessity.

Despite this, there are several drawbacks to using AI in cybersecurity. Apart from the two concerns mentioned earlier, another major concern is distrust. Employers and employees alike have a general tendency to 'distrust' technology in securing their data and networks. There might also be a feeling of loss of control relating to another technology controlling one's privacy and security of data.[16] Further, AI being a self- dependent tool, doesn't need any human help in carrying out the process of cybersecurity. Therefore, probable unemployment is also a major concern.

Hence, AI has several beneficial aspects, but the threats of loss of privacy and control; fear due to unpredictability and threat to unemployment are equally important downsides that should be considered.

### *Regulation of AI in Cybersecurity*

Just like how integration of AI in cybersecurity has been considered in terms of individual application of pre-existing techniques but not on a mainstream basis; the regulation of AI in itself is at a nascent stage.

A report which made a comparative study of emergence of regulatory practices relating to AI at a global level states that the most comprehensive regulation is in relation to autonomous vehicles and the testing of such vehicles.[17]

As per the report, the first country to form an AI strategy was Canada in 2017 and in 2018, the European Commission released a draft of AI ethics guidelines that set out a framework

---

[14] *Supra* note 4.

[15] @Darktrace. (2018). *Flying under the radar: How Darktrace detects 'low and slow' cyber-attacks*. [online] Available at: https://www.darktrace.com/en/blog/flying-under-the-radar-how-darktrace-detects-low-and-slow-cyber-attacks/ [Accessed 19 Dec. 2020].

[16] Goldstein, P. (2017). *The Pros and Cons of Automated Cybersecurity*. [online] Technology Solutions That Drive Business. Available at: https://biztechmagazine.com/article/2017/07/pros-and-cons-automated-cybersecurity [Accessed 19 Dec. 2020].

[17] *Supra* note 7.

for designing trustworthy AI.[18] However, in terms of national AI strategies, most of the countries are still yet to develop a strategy.[19]

Hence it can be determined that there is a very weak base of regulation for AI, and as far as any cybersecurity specific legislation is considered, there is no step in relation to it, primarily because there isn't much integration of AI in cybersecurity. The existing regulatory framework, however, is not enough even to regulate AI in general.

- **Conclusion And Recommendations**

From the analysis in the previous section, it is clear that artificial intelligence has both pros and cons; and objectively, neither of the two outweigh the other. While AI can definitely advance cybersecurity to the next level and bring it on par with the newly emerging cybercrime issues, the risk it poses is equally high. A single malfunction or a mistake can easily result in opening a gateway for the hackers and cybercriminals. Added to this, is the complex nature of AI which causes unpredictability in its behavior. This causes a wary reception to the idea of handing over the security to an unpredictable component.
On the other hand, the hackers are not going to wait while the IT professionals find a middle ground. It is quite clear that AI based attacks are gaining ground. The only solution in this respect is to use AI based security solutions to beat the AI based cyberattacks.
Therefore, at an impasse on the pros and cons level, one way to figure out a solution is to see the regulation aspect of AI. As per the analysis, it can be concluded that regulation of AI is still at a nascent stage. The regulations that have emerged are attempts to regulate AI in different, narrowed areas; something which cannot happen if AI is used in cybersecurity. This is because a cybersecurity program/strategy will probably need multiple AI applications to enforce security in just one system.

Hence, without a much more advanced and specific regulation related to using AI in cybersecurity, it is not possible to integrate AI in cybersecurity system, which is a long journey to be completed. In the meantime, some recommendations can be made in an effort to bridge the gap:

1. Complete take-over of AI in cybersecurity system is virtually impossible, but a restricted integration, while ensuring necessary human intervention at key areas can be an effective mechanism. It will not only enhance the cybersecurity measures, but also result in some level of regulation through human intervention.

2. Multiple AI regulations have already started to come into being. If these emerging regulations were to adopt cybersecurity regulation measures at a smaller scale (i.e., restricted to the specific target area of the regulation), it could help toward making a more generalized regulation, even if only at State level.

[18]Loc.gov. (2017). *Regulation of Artificial Intelligence*. [online] Available at: https://www.loc.gov/law/help/artificial-intelligence/compsum.php [Accessed 19 Dec. 2020].

[19]*Id.*

3. There are no ethical or legal frameworks to regulate AI in general. A regulation under this category can also help make a contribution toward a regulation in the cybersecurity sector.

It is hence, concluded that while AI is most likely the future of cybersecurity; at this point of time, it is necessary to restrict it's integration within cybersecurity, at least until a specific regulation governing it's usage has been developed.

- **References**

**Articles and Papers:**


1. IBM Cloud Education, *Artificial Intelligence (AI),*IBM CLOUD HUB, (3rd June, 2020), https://www.ibm.com/cloud/learn/what-is-artificial-intelligence
2. Benoit Morel, *Artificial Intelligence: a Key to the Future of Cybersecurity*, RESEARCH GATE, (Oct, 2011), https://www.researchgate.net/publication/254006500_Artificial_intelligence_and_the_future_of_cybersecurity
3. Forrester, *The Emergence of Offensive AI*, DARKTRACE, (Feb, 2020), https://www.darktrace.com/en/resources/research-forrester-offensive-ai.pdf
4. *Report on Regulation of Artificial Intelligence*, LOC, (Last updated 24th July, 2020), https://www.loc.gov/law/help/artificial-intelligence/index.php
5. Karthik Ramachandran, *Cybersecurity issues in the AI World*, DELOITTE, (11th Sept, 2019), https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/ai-and-cybersecurity-concerns.html
6. Raghav Bharadwaj, *Artificial Intelligence in Cybersecurity – Current Use- Cases and Capabilities*, EMERJ, (22nd July, 2019) https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/
7. Dave Palmer, *Flying under the radar: How Darktrace detects 'low and slow' cyber attacks*, DARKTRACE, (3rd Dec, 2018), https://www.darktrace.com/en/blog/flying-under-the-radar-how-darktrace-detects-low-and-slow-cyber-attacks/
8. Phil Goldstein, *The Pros and Cons of Automated Cybersecurity*, BIZTECH, (6th Jul, 2017), https://biztechmagazine.com/article/2017/07/pros-and-cons-automated-cybersecurity
9. *Report on Regulation of Artificial Intelligence*, LOC, (Last updated 24th July, 2020), https://www.loc.gov/law/help/artificial-intelligence/compsum.php