THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE ENHANCEMENT OF CYBER SECURITY OF PAKISTAN

Zeeshan Javed*

Abstract

With rapid advances in technology related to Artificial Intelligence (AI), there has been an increase in the use of AI-based algorithms in automating processes. In terms of the cyber domain, there has also been the development of new architectures that utilize AI-based programming. This article seeks to understand what is the potential of current AI-based cyber-security architecture and what benefits does it present over traditional cyber-security approaches. It uses Pakistan as a case study to justify the use of an AI-based approach. And it argues that by preferring an AI-based architecture to a traditional cyber-security approach, Pakistan can bolster its cyber-security when it comes to defence against cyber-attacks.

Keywords: *Artificial Neural Networks, Artificial Intelligence, Cyber-security, Hacking, Malware, Cyber Kill-Chain*

Introduction

Cyber-attacks have become a common occurrence in the modern world. With the ever-increasing digitization, the menace of cyber-attacks have also increased manifold. However, a difficult aspect of cyber-attacks is their nature of anonymity and their ability to cause disruption on a wide scale. An example of this is the ransomware attack on Colonial Pipelines in the US, causing widespread fuel shortages in the country.[1] Similarly, data breaches are also an aspect of cyber-attacks where the aim is to sabotage or gather intelligence against an adversary in the cyber domain. With cyberspace being termed as a new global common,[2] such attacks in the cyber realm may bring about disruption and uncertainty in the near future.

* Lecturer at the Department of Strategic Studies, National Defence University, Islamabad. Email: zeeshan.javed@ndu.edu.pk

1 Grace Segers, "Cyberattack Prompts Major Pipeline Operator to Halt Operations," *CBS News*, May 9, 2021, https://www.cbsnews.com/news

2 Binu Joseph and Mohanan B. Pillai, "The Cyberspace as a Distinct Domain of the Global Commons: An Analysis of Cyberspace Governance," *Global Commons: Issues, Concerns and Strategies* (SAGE books, 2020), 125.

Pakistan is not immune to such cyber-attacks. A recent report by the International Institute for Strategic Studies (IISS) suggests that India's offensive cyber capabilities are more Pakistan-focused and that Delhi is increasing its offensive capabilities through modern technologies, shared by its international partners.[3] Recently, India-based espionage in Pakistan has also been uncovered. The revelations of the "Pegasus" program, a spyware designed to tap into mobile phones, shed light on the use of offensive cyber capabilities to conduct espionage on domestic as well as foreign elements. The chief among which were Pakistani politicians.[4]

Such offensive policies are reflected in an increase of cyberattacks on Pakistan in the form of government and military websites being hacked. After the Pulwama attack, Indian hackers took down over 200 Pakistani websites.[5] The modern-day attacks have become even more dangerous because they have directly targeted the financial institutions of Pakistan through offensive cyber capabilities.[6] With the increased digitization of the banking sector in Pakistan, this may pose a considerable threat and create widespread disruption and financial losses. India has also militarized its cyber capabilities by raising a tri-service command under the name "Defence Cyber Agency". This agency is responsible for Indian military's offensive cyber capabilities.[7] Therefore, one may argue that India is likely to increase cyberattacks against its adversaries, in particular Pakistan.

Besides, there are Non-State related cyber-security threats. Social media accounts of Pakistani embassies in Serbia and Argentina were hacked.[8] These hacks could be due to an insider but they present a cybersecurity threat to Pakistan. Due to the anonymous nature of the cyber domain, it is difficult to identify the origins of the attack and therefore the authorities can hardly distinguish a state-based attack from a Non-State Actor (NSA) originated attack. Thus, Pakistan faces multiple challenges to its cyber-security.

This study uses Pakistan as a case study to understand the potential advantages of AI-based cyber-security architecture. It uses an exploratory approach to investigate the potential of AI-based cyber-security models and

---

3 International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment*, (2021), https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

4 News Desk, "Pegasus Snooping: Pakistan Probes whether PM Khan's Phone Hacked," *AlJazeera*, July 20, 2021, https://www.aljazeera.com/news/2021/7/20/

5 News Desk, "Pulwama Attack: Pakistani Websites Hacked, Here's the List," *Times of India*, February 18, 2019, https://timesofindia.indiatimes.com/gadgets-news/

6 News Desk, "Cyberattack Disrupts National Bank of Pakistan Services," *Dawn*, October 31, 2021, https://www.dawn.com/news/1655059.

7 News Desk, "Agencies take Shape for Special Operations, Space, Cyber War," *The Times of India*, June 12, 2019, https://timesofindia.indiatimes.com/india.

8 Mateen Haider, "Twitter Account of Pak Embassy in Belgrade Hacked," *The Nation*, December 4, 2021.

their efficacy in dealing with threats. The research findings would provide guidelines for Pakistani policymakers and help developing an understanding about the future of Pakistani cybersecurity - using AI and ANN based cybersecurity. The reason why AI may be suitable is the fact that AI has the ability to recognize patterns in vast amounts of data. Through the utilization of data mining techniques, AI has now become a staple in modern cyber development. Many websites utilize AI to streamline their data usage and understand consumer patterns that is useful in developing an effective marketing strategy to cater to those patterns.[9]

Artificial Neural Networks (ANN) are AI models that rely on the use of various computational nodes integrated into connections much like those found in the biological brain.[10] These "artificial neurons" resemble the working of a biological brain and are aggregated in the form of layers.[11] Through these layers, data is computed and translated into information. The ANN models are unique because they take inspiration from the biological working of the human brain and try to recreate the neural pathways digitally.[12] These artificial neurons act as a filtration layer and are responsible for extracting a specific set of data from the data set and then the final layer is responsible for deducting a result.[13] This allows ANNs to have the ability to reproduce and even model complex non-linear tasks and processes.[14] Due to such properties, ANNs are used effectively in various fields from pattern recognition[15] to face identification[16] to medical diagnosis[17] to visualization.[18] Such vast applications of the ANNs allow them to be a versatile solution to a various problems.

---

9 Michael Negnevitsky, *Artificial Intelligence A Guide to Intelligent Systems* (Essex: Pearson Education, 2007) 26.

10 Marcel Van Gerven and Sander Bohte, "Editorial: Artificial Neural Networks as Models of Neural Information Processing," *Frontiers in Computational Neuroscience* 11 (2017): 12.

11 Utku Kose, "An Artificial Neural Networks Based Software System for Improved Learning Experience," *2013 12th International Conference on Machine Learning and Applications*, 2013, 7.

12 Kose, "Artificial Neural Networks," 8.

13 Ibid.

14 Guang-Bin Huang, Qin-Yu Zhu, and Chee-Kheong Siew, "Extreme Learning Machine: Theory and Applications," *Neurocomputing* 70, no. 1-3 (2006): 493.

15 Nandini Sengupta, Md Sahidullah, and Goutam Saha, "Lung Sound Classification Using Cepstral-Based Statistical Features," *Computers in Biology and Medicine* 75 (2016): 121.

16 Sengupta, Sahidullah, and Saha, "Lung Sound Classification," 122.

17 Ibid.

18 Sam Schechner, "Facebook Boosts AI to Block Terrorist Propaganda," *The Wall Street Journal*, June 15, 2017.

What has really allowed AI to become a revolution in the field of cybersecurity is its unique aspect of automation and self-sufficiency. The AI models, particularly the ANNs, have the potential to develop a complex machine that can predict and recognize patterns of attack and devise counterstrategies to combat the threat. This is done in an automated manner allowing for a fast, efficient and optimized response to the attack. Already ANN based models are used to predict electricity prices based on consumption and user patterns.[19] Through such models, there is a possibility to monitor and predict cyber-attacks on the infrastructure and formulate an effective response. ANNs can be designed to differentiate between authentic and malicious cyber activity and then take appropriate actions if the activity is deemed malicious.[20]

Traditional cybersecurity models have been designed for the involvement of humans in a large manner. Unfortunately, such models have their limitations. Human errors caused due to factors like fatigue either delay the response or are incapable of recognizing and predicting the attack. Such challenges may be countered through the development of a cyber-security architecture centered on an effective AI algorithm that monitors and contains threats as well as launch counter offensives.

In Pakistan, AI and in particular ANN-based cyber-security models may provide a more adept solution. In this regard, three research questions are important to answer. First, what are the traditional cybersecurity methods that are currently incorporated? By understanding these traditional models, the authorities can establish a premise of the advantages and disadvantages of the traditional approaches of cybersecurity. The also provides an understanding of how modern cyberthreats manifest themselves. The second question deals with the potential of AI in cybersecurity models. It helps us understand the potential that AI can have when it comes to the detection, prevention and response to threats in the cyber realm and what are advantages of AI-based cybersecurity models compared to traditional cybersecurity approaches. Finally, the question that this research will attempt to answer is that why should an AI-based cybersecurity model be implemented in Pakistan, and if it is to be implemented what can be the future trajectory? The final question serves as a policy-relevant finding for the decision makers of the country and it will help to provide an executable model. It also provides an assessment of the cyber eco-system of Pakistan and helps us understand whether it is relevant to employ AI-based cyber-security architecture? To answer these questions, this

---

19 Hong Chen, C.A. Canizares, and A. Singh, "ANN-based Short-Term Load Forecasting in Electricity Markets," *2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194)*, 56.

20 Robin Nix and Jian Zhang, "Classification of Android Apps and Malware using Deep Neural Networks," *International Joint Conference on Neural Networks (IJCNN)*, 2017.

study uses scientific literature to establish the premise of AI and ANNs to provide technically relevant research to the scope of cybersecurity.

Traditional Approaches to Cybersecurity and Cyberthreat

Cybersecurity has emerged as an important facet of security in the non-traditional paradigm. The conventional security tools employed in the initial stages of cybersecurity were designed to locate and identify viruses based on their signatures and to deny their execution. This meant, they would attempt to negate them before they did any damage to the target system.[21] However, with the advance in technology, states have enhanced the ability to provide effective security options. These systems are designed to provide a wide area of coverage and to ensure the protection of the systems from cyber threats. This is important, because with the widespread usage of computers in today's world, it has now become even more important to ensure that these systems are protected. Nonetheless, the threats have also evolved. Modern cyber threats comprise a variety of attacks and intend to harm a variety of target systems.

To ensure a more comprehensive coverage in the face of evolving cyber threats, the threat response needs to evolve as well. Conventional cybersecurity methods can be slow and inflexible in their response to these threats.[22] To that end, the modern role of AI can help bolster the strength of cybersecurity response to these threats. A modern cyber-attack consists of multiple phases that an attack goes through to ensure its success. This is termed the *Cyber Kill-Chain,* a term coined by Lockheed Martin.[23] The Cyber Kill-Chain is designed and aimed at systematically finding the opposition's weakness and inflicting maximum damage in the cyber domain. The Cyber Kill-Chain may consist of the following phases:[24]

- **Reconnaissance** – Attacker locates gaps and vulnerabilities of target system
- **Weaponizing** – Based on the weaknesses found, the attacker creates a targeted malicious code
- **Delivery** – The transfer of the malware/virus to the intended system
- **Exploit** – Execution of the malicious code

---

21 Nadine Wirkuttis and Hadas Klein, "Artificial Intelligence in Cybersecurity," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 109.

22 Amjad Rehman and Tanzila Saba, "Evaluation of Artificial Intelligent Techniques to Secure Information In Enterprise," *Artificial Intelligence Review* 42, no. 4 (December 2014): 22.

23 "Cyber Kill Chain," Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

24 Ibid.

- **Install** – The attacker installs their malicious code into the target system
- **Control** – The attacker now has control of the target system and uses it for malicious intent
- **Counteraction** – The target system realizes that an attack is taking place and takes action to prevent damage or even counterattack

It is noteworthy that cybersecurity is unique as compared to other forms of traditional security because there are a variety of threats emanating from different sources and each source brings with it, its own unique challenges. In the modern era, non-governmental organizations, governments and even individuals carry out cyber-attacks.[25] Moreover, there are no geographical boundaries to threats, suggesting that everyone is potentially at risk of cyber-attack from different entities. Reasons for these cyber-attacks can also vary from financial, military to political domains.

Keeping in view the Cyber Kill-Chain, attempts have been made to provide a more holistic approach to cybersecurity, like introduction of the Integrated Security Approach (ISA). The ISA aims to provide early warning by essentially installing systems that create awareness of a possible intrusion in the system.[26] In the Kill Chain, the ISA aims to limit the damage and access of the malicious entity. If early detection of the security breach is not possible, the ISA model implements damage containment and counteraction steps. Along with this, the ISA model aims to roll back the data to its initial state to negate any damage that the intrusion might have done.[27]

The ISA framework is a comprehensive and holistic framework designed to ensure cybersecurity. The emphasis of this model is on preventing attacks and ensuring early detection of intrusions. The aim of the ISA model in the first three phases of the Cyber Kill-Chain is to ensure a timely detection and alert of an intruder in the system. Once it is detected, the aim is to limit the damage caused by the attack and disable the malicious hack's execution. Considering Standard Operating Procedures (SOP) under the ISA framework, the aim is to deconstruct a cyber-attack to uncover clues and patterns that make one aware of the nature and purpose of attack. Using this, the ISA model can be made more robust in order to ensure that in the future such attacks are detected much earlier and neutralized without even giving a chance to reach the exploit stage. These *data tracks* are what enable cyber investigators to ascertain the motive of the hackers and the tools used to achieve those motives. To ensure an effective ISA,[28] it is important to have a robust method of cyber

---

25 Ibid.

26 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques," 19.

27 Ibid., 20.

28 Selma Dilek, Huseyin Cakir, and Mustafa Aydin, "Applications of Artificial Intelligence to Combating Cyber Crimes: A Review," *International Journal of Artificial Intelligence & Applications* 6, no. 1 (2015): 23.

intelligence, which requires the monitoring and collection of data that identify potential threats and weak areas in a system. However, gathering cyber intelligence is not as easy and straightforward as it may seem.

The collection of information from data is a complex and time-consuming process. It is not easy to extract useful information from a vast data set: in fact, the complexity increases during cyber intelligence. Due to the vast use of computers and the proliferation of the cyber realm, data has grown exponentially.[29] This means, to locate data tracks, an extensive combing of vast amounts of data sets, which is a tall order, given the massive array of data sets. This problem is further complicated by the lack of homogeneity in the dataset.[30] Due to the different systems being used to achieve different objectives, there is no uniformity in the data that is being produced. Topology and different behaviours of systems on networks also mean that there is a diverse array of data is being produced. This means that there is not only a massive amount of data but also diverse array of data. Finally, another issue in gathering cyber intelligence is the high data velocity, meaning the rate with which new data is being produced and processed. High data velocities indicate that there is a constant stream of data coming through at a higher rate and that means that there is more strain on the data collection system because it has to keep up with a constant stream of new data and then process it and convert it into useful intelligence.[31]

The challenges of data collection in the cyber domain indicate that there is a need to have a system in place that can constantly evolve and adjust to be more efficient in data collection and gathering intelligence. To achieve this objective, the development of Intrusion Detection Prevention Systems (IDPS) is an important facet. IDPS, in essence, is a tailor made hardware/software that is designed to protect networks and systems from intrusions by looking at the data that is gathered.[32] There are two main approaches to develop IDPS: the *Anomaly Detection Approach* and the *Misuse Detection Approach*--both approaches are designed on the similar approach of recognizing patterns. The patterns that these approaches recognize vary. The Anomaly Detection Approach primes IDPS to recognize and identify normal network or system behaviour.[33] Once the baseline is established, the IDPS then looks for patterns that are not similar to the baseline and immediately flags them. The Misuse Detection Approach, on the other hand, establishes a baseline of malicious activities by highlighting the patterns of malicious activity

---

29 Ibid., 24.

30 Ibid.

31 Ibid.

32 Enn Tyugu, "Artificial Intelligence in Cyber Defense," *Proceedings of 3rd International Conference on Cyber Conflict (ICCC)*, June 2011, 99.

33 Xiao-bin Wang et al., "Review on the Application of Artificial Intelligence in Antivirus Detection System," *Cybernetics and Intelligent Systems*, 2008, 506.

in a network or a system. If such a pattern is recognized by the IDPS, then that activity is flagged.[34] In both approaches, cyber experts identify the patterns on the basis of their practical knowledge of modern cyber threats. These methods are primed to use pattern recognition to determine threats and the nature or severity of these threats. However, a crucial issue that remains with IDPS is the fact that cyber threats are constantly evolving and changing. Newer threats are constantly emerging which may not be programmed in these IDPS as a pattern to raise alarms. IDPS is more of a traditional approach towards cybersecurity; it is designed to pre-program cyber threats and has systems constantly checking against these baselines. The main problem with these traditional approaches is that they rely on the existing body of knowledge and are not prepared or designed to innovate or be proactive.[35]

These systems are designed around pre-set patterns and programmed cyber threats, which creates issues regarding their ability to detect genuine threats. An IDPS' detection is based around the idea of detecting abnormalities or signatures of malicious software. However, this also leads to many cases being false negatives because of the IDPS' inability to recognize newer cyber threats[36] and conversely, it also creates false positives because of the erroneous definition of normal working patterns in a network.[37] This creates another major issue and that is scalability of the systems. As these systems are designed to operate on pattern recognition in large data sets, this means that IDPS are slow and unable to be replicated in large networks with a much larger traffic flow. The biggest issue with the IDPS is the lack of automation. These systems are not designed to learn new patterns by themselves or adapt to a change of the cyber domain. Instead, they rely on their programming to function as an effective ISA. From pattern recognition to error messages, everything has to be updated manually.[38] This means that a large number of manpower and time is required to maintain and update these IDPS and keep them effective in a large network. Thus, traditional IDPS require a large amount of human and financial resources to operate optimally and even then, they are slow and tend to produce false results.

The Role of AI in Cybersecurity

With the constant evolution and development of cyber systems, there has been an increase of their usage in modern businesses and infrastructure needs. From water filtration plants to nuclear plants, vast computer networks are now in place in various forms and functions. It is noteworthy that this vast computerization has enhanced coordination among different nodes of basic

34 Wang, 506.

35 Tyugu, "Artificial Intelligence in Cyber Defense," 99.

36 Ibid.

37 Ibid.

38 Ibid.

facilities. This phenomenon is not simply limited to government organizations but is also evident in the interaction of private businesses and corporations. With such a vast array of different networks communicating and coordinating with each other, there is the development of an intrinsic form of an ecosystem with a varied array of demands and potential threats.

Thus, the main issue with IDPS is that they are not autonomous and rely on humans for their optimum functioning, which is a time-consuming process. Ensuring cybersecurity in a system or a network requires a basic form of intelligence and cognizance that, unfortunately, traditional IDPS cannot provide due to their pre-programmed nature. In this regard, AI can provide a breakthrough to ensure an autonomous, holistic and robust network defense. AI, has demonstrated the ability to identify and recognize patterns much more quickly than their human counterparts. Moreover, IDPS are designed to function around the premise of pattern recognition to flag and thwart cyber-attacks. Therefore, the integration of AI into a cybersecurity model provides a reactive and flexible model that is autonomous and can effectively prevent and counter cyber-attacks. AI vastly improves data acquisition and can limit the effects of variables such as the amount of data or the velocity of data. These features allow cybersecurity experts to develop a much more adept and efficient system at dealing with cybersecurity threats emanating in various domains.

The incorporation of AI based components in the shape of an autonomous cognitive entity can ensure internal decision-making and act against cyber threats in a timely fashion.[39] These components are designed to be decentralized and of an interacting nature so that they can detect malicious activity and counterattack quickly. The Artificial Immune Systems (AIS) are a form of such a model incorporating the role of AI. The AIS sees the implant of detection agents and counterattack agents. The purpose of detection agents is to monitor network and system traffic for any anomaly and once such an anomaly is spotted, the counter attacking agents are mobilized to infiltrate the attacking system and launch a counterattack.[40] This whole function of detection and counterattack takes place autonomously without any human involvement. This means system's response against cyber threats is much more coherent and efficient than the traditional method of detection and response.[41]

---

39 Xia Ye and Junshan Li, "A Security Architecture Based on Immune Agents for MANET," *International Conference on Wireless Communication and Sensor Computing*, 2010, 3.

40 Ye and Li, "Immune Agents for MANET," 3.

41 Alessandro Guarino, "Autonomous Intelligent Agents in Cyber Offence," *5th International Conference on Cyber Conflict*, 2013, 13.

ANNs and Cybersecurity

The ANNs are designed to imitate the human brain's structure and are designed to solve real-world problems with a flexible algorithm. Rather than having a rigid algorithmic structure to the ANN, it is based on a statistical learning model, which allows the system to *learn* and improve its ability to solve problems.[42] ANNs have been used to create cyber security models. By incorporating ANNs in the ISA model, these cybersecurity models have been used to monitor traffic and to raise flags regarding possible intrusions. By utilizing ANNs in the cybersecurity model, malicious activity can be detected in the delivery stage of the Kill-Chain, well before any attack occurs.[43] This has always been one of the objectives of designing any form of a cybersecurity model, to be able to detect any malicious activity before it even has a chance to cause damage. Along with this, ANNs can learn the activity patterns and previous attacks on the system or network.

The biggest advantage of using the ANN model learning on its own can be coupled with the traditional IDPS models to ensure a robust security model. As IDPS models are designed on pattern recognition, one of their major strengths is that they can learn and recognize patterns and simultaneously appreciate the changing dynamics.[44] Given that such a model is completely autonomous, it also means a significant increase in efficiency and speed, with remarkable accuracy. Not only are ANNs only compatible with IDPS, but they can also be utilized in other facets of network security such as firewalls, network hubs, or even intrusion detection systems. There have also been advances in ANNs and now Deep Neural Networks (DNN) are being utilized to create a more elaborate and comprehensive mesh of network security. DNNs are computationally intensive form of networks, but given the massive improvements in hardware designs and capabilities over the years, DNNs are now quickly becoming a reality and are implemented in network security. Through the use of DNNs, the aim is not only to prevent cyber-attacks but to also predict any incoming cyber-attacks.[45]

The future of the modern cybersecurity architectures may see the development of an IDPS system incorporating ANNs and DNN to update the pattern recognition of these systems. Such systems would recognize patterns and update logs automatically and would require minimal to no human intervention. An advantage of this approach may be the swiftness of detection and then the appropriate response. Therefore, the AI may be able to replace or

---

42 Christian Bitter, David A. Elizondo, and Tim Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection," *World Congress on Computational Intelligence*, 2010, 950.

43 Linda Ondrej, Todd Vollmer, and Milos Manic, *2009 International Joint Conference on Neural Networks* (Atlanta, 2009), 1829.

44 Bitter, Elizondo and Watson, "Applications of Artificial Neural Networks," 950.

45 Guarino, "Autonomous Intelligent Agents," 13.

minimize the role of human operators in the IDPS. For it to be an optimal system, a few factors may need to be taken into consideration such as the size of the network, the sensitivity of data, and the threat environment of the system. By considering these factors, network administrators may be able to determine how much autonomy to be given to the AI-based architecture versus the human operators. There may also be a possibility that AI-based section of the network be given less autonomy due to organizational inertia. However, if the system can prove its capabilities versus the threats, it may be given more autonomy in the future.

In addition to this, using such dual layer architecture the victim network may also be able to launch an effective counter attack against the intruder. The aim of the counterattack, in cybersecurity, is to stop or in some cases, slow down the enemy's intrusion into the network. If the victim is unable to counterattack, the aggressor may occupy key nodes in the network and seize essential network functionality. Therefore, an AI-based IDPS may be able to recognize an attack faster and then launch effective counterattacks to stop the enemy from gaining hold of key functionalities of the network.

Findings

The developments in the field of AI and ANNs provide Pakistan an opportunity to develop a tailored-made framework for its security environment. Instead of relying on foreign IDPS, Pakistan can now design robust and comprehensive cybersecurity architecture. Even though, countries like Pakistan have not seen a vast utilization of computers and network systems in the delivery of basic services, the fact remains they are still used in these fields. As the goal of these organizations moves towards automation and optimization, the usage of computers and network systems will only increase.

At the same time, Pakistan is prone to vulnerable spots in its cyber ecosystem. For instance, the citizen data generated and stored by NADRA can be hacked and misused, which may pose a threat. A similar attack has already happened on the Federal Board of Revenue (FBR) database, where hackers were able to break into the Hyper-V software by Microsoft and eventually crash the website.[46] This may become a threat, as the FBR is responsible for housing the financial data of Pakistani citizens. Another example of such attacks is the selling Pakistani telecom users' data on the dark web. The sale of a massive data dump consisting of 115 million Pakistani citizens and their personal details (name, identity number, address, tax number, region, etc.) was uncovered on the dark web.[47] Similarly, malicious software can be used to interfere with the electrical grids and cause a massive blackout in the entire

---

46 Shahbaz Rana, "FBR Reels under a Major 'Cyberattack'," *Express Tribune*, August 15, 2021.

47 News Desk, "115 Million Pakistani Mobile Users Data Go on Sale on Dark Web," *Rewterz*, April 10, 2020.

country, leading to a failure of infrastructure and facilities. Even though, Pakistan does not currently rely on automised electric grids, with the inclusion of an increasing number of bi-directional electrical systems, there is a possibility that Pakistan will look towards upgrading their electrical grids to Smart Electrical Grids, which are digitized largely. There is also the issue of sensitive locations such as nuclear reactors, where the presence and execution of malicious software can be catastrophic. This is especially true in the military domain. Malicious software can be used to cause a communications blackout, or to hack into servers to steal critical information. Not only that, but in recent times, most of the Pakistani websites have come under constant attack from Indian originated hacks.[48] Considering these, one may assume that Pakistan is at risk of a plethora of cyber threats. These threats are not only limited to private individuals but also government organizations. The attacks use increasingly sophisticated architecture to cause a breakdown of services. If such an attack becomes successful, there could be a serious national security issue, as was the case in the Colonial Pipeline Ransomware attack in the US.[49]

In this context, Pakistan's strategic security policy makers must ensure and design a cybersecurity architecture that is most closely related to their needs and can ensure a robust line of defense in the face of any malicious activity. To achieve this, Pakistani authorities have to realize the importance of AI in the context of cybersecurity. ANNs and AI are now a niche field in Computer Science and are being constantly evolving and developing. Pakistani institutes are also researching and developing cybersecurity models that utilise these techniques. For Pakistani authorities, especially those involved with sensitive installations, there is a need to incorporate these institutes and present to them their need to develop a custom network security architecture that can plan and execute these network security protocols. Furthermore, an AI based cybersecurity model is a relatively cheaper option than the traditional IDPS because IDPS require a large work force to keep an effective cybersecurity response. On the other hand, an AI based model requires lower work force as it is automated. What it does need, however, is extensive computational power. With the constant advances in technology and improvement in processing speeds, hardware requirements are also getting cheaper and it becomes a much more financially feasible option to maintain an AI based security architecture.

Financial institutions are one of the most vulnerable systems in the Pakistani cyber eco-system. Therefore, these systems may be categorized as the most vulnerable and the ones that may pose a threat to the deterioration of cybersecurity architecture of Pakistan. It can be argued that this approach is also seen in the governmental and private financial institutions.

---

48 News Desk, "Check out the List of Pakistani Websites Hacked by Indian Group over Pulwama," *Outlook India*, February 17, 2019.

49 Grace Segers, "Cyberattack Prompts Major Pipeline Operator to Halt Operations," *CBS News*, May 9, 2021.

The development of an ANN based security model as a pilot case can be considered. By incorporating this pilot case in a Pakistani organization, the results can be analysed and further modifications can be made to ensure that an accurate and safe option is developed in terms of cybersecurity. A pilot case, to enhance the cybersecurity of financial institutions, may be envisioned. Evidently, Pakistani financial institutions have been at risk of cyberattacks from adversaries. Additionally, such cyberattacks pose a detrimental risk to the overall financial architecture of Pakistan. Therefore, a pilot study may develop, incorporating the double-layered cybersecurity architecture in a select few financial institutions, both government and private. A governmental committee, including renowned cybersecurity experts, may oversee the progress of such financial institutions under this two-layer approach. The findings of this project may be discussed with the relevant stakeholders and an executable policy maybe formulated, which may be applicable to wider institutions.

If AI and ANN-based cybersecurity are to be incorporated in military organizations or other sensitive organizations, a two-step approach may be opted for. The first line of defense may be an ANN based cybersecurity model that allows for the prediction of future attacks and then an ASI model be designed so that an effective counterattack is launched. In addition to this, these systems can be more oriented towards Whitelisting rather than Blacklisting.[50] Whitelisting offers an advantage as it may limit an unwanted or probing attempt at the network and the system.

It is worth mentioning that the Pakistani government has recently announced a Cybersecurity Policy that advocates for the establishment of "*…national Cyber Security forensic and screening setups*" that will be used to safeguard against advanced cyber threats in an AI driven environment.[51] However, the policy fails to provide any concrete steps or measures to include AI and ANN in its security architecture to protect against incoming cyberattacks. Although it is a step in the right direction, aspects related to cybersecurity are lacking, especially when providing a blueprint for the future inclusion of AI and ANN-based systems in the security ecosystem.

Finally, the federal and provincial governments must realize the importance of having an effective AI based cybersecurity organization. This can be initiated by developing an autonomous government body dedicated to developing cybersecurity in Pakistan. This department should be in constant touch with the AI programs in universities. Through this, the government department can either fund particular projects of the universities or induct

---

50 In a blacklisting architecture, the default is to allow access to entities. The focus is to stop malicious or suspicious entities. In whitelisting, the aim is to block access to all entities except for those that are allowed access.

51 Ministry of Information Technology and Telecommunication, *National Cyber Security Policy 2021*, (Government of Pakistan, 2021).

their best students into their own department so as to further the development of cybersecurity architecture in Pakistan.

Conclusion

As is the case with most of the technologies, there will always be potential threats designed to exploit the weaknesses of the enemy. The cyber realm is one such area of exploitation. Given the fact that there is a constant change and evolution in cyber technologies, it is of no surprise that the threats are constantly evolving as well.

Modern cybersecurity architecture is heading towards autonomy and self-sustenance which is a blessing but at the same time a major threat for cybersecurity experts. The exponential nature of modern technologies is playing the role of a catalyst in the evolution of such threats. In essence, the advent of AI and ANNs has resulted in the creation of algorithms that can adapt and change their program codes to pose a greater threat to the security checks. By systematically probing and challenging the cybersecurity architecture, such algorithms can find weaknesses at a much greater speed than any human. Therefore, this requires a change in approach in order to counter the threat of these emerging threats.

AI and ANNs have offered a toolkit to combat these threats and deal with these issues consistently and efficiently. These technologies offer a lot of potential due to the fact that they can learn on their own. In essence, they offer complete automation and develop robust and comprehensive security architecture with a minimum need for human involvement. Through the utilization of ANN and DNN, the world is now moving towards a more secure and encrypted form of communication. However, as solutions continuously evolve, so too do the threats. That, in essence, means that there is always the risk of newer threats coming to the fore and by emerging, can potentially challenge the comprehensiveness of the AI based security models as well.

Pakistan is also embracing the digital revolution taking place in the world. The digitization of various aspects of the government is a testament to this fact. This has made the job of policy makers a lot easier in terms of collecting data and service delivery. However, at the same time it has also created vulnerabilities in the cybersecurity ecosystem. If such vulnerabilities are not strengthened through the use of modern toolkits, this can create nationwide issues for the country in a few hours. The only way for Pakistan to counter such challenges is to create a proactive policy that caters and allows for the development of an effective AI based cybersecurity system that can be incorporated with the existing cybersecurity architecture. It must be kept in mind that the modern development path is that of automation, which also applies in cyber-attacks. Therefore, for Pakistan to keep such attacks at bay, it is necessary that effective steps must be taken to counter the ingress of automated attacks.