Editorial

Leveraging Artificial Intelligence to Combat Electronic Crimes: The Case for Pakistan

Kaukab Jamal Zuberi

INTRODUCTION

In today's world, the importance of digital security cannot be overstated. Our reliance on electronic systems and internet-based transactions has created a vast digital ecosystem, but it has also paved the way for sophisticated cybercrimes. From financial fraud to corporate espionage and cyberterrorism, the range of electronic crimes is continually expanding, and so is the sophistication with which criminals operate. In many parts of the world, countries are countering these cyber threats by leveraging Artificial Intelligence (AI) as a core component of their cybersecurity strategies. Unfortunately, Pakistan lags in adopting these advanced measures, hampered by limited resources, underdeveloped infrastructure, and challenges in governance.

This editorial explores how AI is being used globally to combat electronic crimes, its potential benefits for Pakistan, and why there is an urgent need for Pakistan to bridge this technology gap.

AI and Cybersecurity: A Global Overview

In regions like North America, Europe, and East Asia, AI is increasingly central to cybersecurity, enhancing both proactive and reactive capabilities. Here are some of the ways AI has revolutionized cybersecurity globally:

1. Threat Detection and Prevention: Traditional cybersecurity solutions are rule-based and often detect only known threats. AI-driven systems, by contrast, use machine learning to identify unusual patterns and behaviors, detecting new and evolving threats in real time. For instance, unusual login patterns or unauthorized data access are flagged immediately, enabling rapid intervention.
2. Predictive Analytics: AI can analyze historical data to predict potential cyber-attacks before they occur. Companies like Darktrace and CrowdStrike use AI-driven models to assess vulnerabilities and enable proactive strengthening of security defenses.
3. Automated Responses: AI can automate responses to specific types of cyber threats. For example, if a network intrusion is detected, AI-driven systems can block IP addresses or isolate compromised areas without human intervention, saving valuable response time and minimizing damage.
4. Fraud Detection: Financial institutions worldwide rely on AI algorithms to monitor millions of transactions daily, identifying fraudulent transactions in real time by recognizing unusual spending patterns.
5. Digital Forensics: AI is also essential in digital forensics, enabling law enforcement agencies to quickly process vast amounts of data from

confiscated digital devices. This accelerates investigations, improves accuracy, and increases the chances of apprehending cybercriminals.

While these advancements are widely adopted in many parts of the world, Pakistan remains on the sidelines, relying on outdated cybersecurity measures that cannot keep up with the evolving nature of cyber threats.

The Alarming State of Cybersecurity in Pakistan

With rising internet penetration and a growing e-commerce sector, Pakistan has become a more attractive target for cybercriminals. Unfortunately, the country's existing cybersecurity measures are inadequate, creating an environment where cybercrime can proliferate. Key issues contributing to this weak cybersecurity landscape include:

1. Limited Awareness and Education: Cybersecurity literacy is low across Pakistan, affecting both the general public and professional circles. Poor awareness about online safety practices adds to Pakistan's vulnerabilities.
2. Inadequate Legislation: While Pakistan introduced the Prevention of Electronic Crimes Act (PECA) in 2016, it lacks the depth and enforcement necessary to counter sophisticated cybercrime. Moreover, enforcement remains weak, with law enforcement agencies facing shortages in specialized training and resources.
3. Shortage of Skilled Cybersecurity Professionals: Pakistan faces a significant shortage of trained cybersecurity professionals. The few experts available are concentrated in the private sector, leaving government agencies and small businesses particularly vulnerable.
4. Limited Investment in Technology: In other countries, substantial investments in advanced technologies like AI are made to bolster cybersecurity. Pakistan, however, allocates limited financial resources to cybersecurity, with many public and private organizations hesitant to invest in AI-driven solutions.
5. Weak Coordination Among Agencies: Effective cybersecurity requires strong collaboration among government agencies, private companies, and international partners. In Pakistan, however, coordination is often lacking, leading to siloed efforts that cybercriminals exploit.

Why Pakistan Needs AI to Combat Cybercrime

Traditional cybersecurity methods such as firewalls, antivirus software, and manual surveillance are increasingly ineffective against sophisticated cyber threats. With criminals using AI tools themselves, Pakistan must adopt AI-driven cybersecurity solutions to:

1. Enhance Threat Detection: AI systems can identify and neutralize cyber threats faster and more accurately than traditional methods. Continuous monitoring and real-time data analysis enable the detection of suspicious activities that would otherwise go unnoticed.
2. Improve Incident Response: Cyberattacks can cause widespread damage within seconds. AI-driven response systems can automatically

execute defensive measures, significantly reducing response times and minimizing damage.
3. Streamline Digital Forensics: For law enforcement agencies, the ability to analyze vast quantities of data quickly is essential to tracking down cybercriminals. AI-based digital forensics can help agencies process data faster, speeding up investigations and improving prosecution rates.
4. Address the Shortage of Cybersecurity Experts: Pakistan's shortage of cybersecurity professionals is a major obstacle. AI can help by automating many tasks that would otherwise require human analysts, allowing the country to make the most of its limited cybersecurity workforce.
5. Bolster National Security: Cybersecurity is also a matter of national security, with cyber espionage, cyberterrorism, and other forms of cyber warfare on the rise. AI-powered solutions can help protect Pakistan's critical infrastructure, including government networks, power grids, and financial systems, from hostile attacks.

Barriers to AI Adoption in Pakistan's Cybersecurity

Despite the compelling case for AI in cybersecurity, Pakistan faces several challenges that hinder its adoption:
1. Lack of Infrastructure and Investment: AI-driven solutions require a strong digital infrastructure, including powerful servers and reliable data storage, which Pakistan currently lacks. The cost of establishing this infrastructure is also a significant barrier.
2. High Costs of AI Solutions: Implementing AI-based cybersecurity measures can be expensive, especially for a developing country like Pakistan. Limited public and private budgets make the high initial costs of AI solutions prohibitive for many organizations.
3. Shortage of AI Talent: AI expertise is limited in Pakistan, with few educational institutions offering programs focused on AI and cybersecurity. To leverage AI effectively, Pakistan must invest in building a skilled workforce.
4. Privacy and Ethical Concerns: AI-driven cybersecurity often involves extensive data collection, raising concerns around privacy. Pakistan currently lacks robust data privacy laws, making it challenging to implement AI while protecting citizens' privacy rights.
5. Weak Institutional Support: AI adoption requires strong institutional backing, yet government support for AI-driven cybersecurity remains minimal, with few policies or incentives in place.

The Way Forward: A Strategic Approach to AI and Cybersecurity in Pakistan

For Pakistan to effectively combat cybercrime, a strategic approach that includes AI-driven solutions is essential. Here's how Pakistan can move forward:

1. Government-Industry Collaboration: Establishing public-private partnerships can help Pakistan leverage expertise and resources from its technology industry to advance cybersecurity capabilities. Joint efforts between the government and the private sector will strengthen the country's defenses.

2. Investment in Education and Training: Pakistan must invest in cybersecurity education, focusing on AI and related fields. Expanding specialized programs in universities will create a pipeline of skilled professionals to support cybersecurity efforts.
3. Creation of a National Cybersecurity Agency: Pakistan has previously attempted to establish a centralized cybersecurity agency to coordinate efforts across sectors. However, these efforts have temporarily failed, and cybercrime investigation responsibilities have reverted to the Federal Investigation Agency (FIA). For effective cybersecurity, Pakistan must renew efforts to establish a dedicated national agency that can lead AI-driven initiatives, promote public awareness, and foster international cooperation. This agency would also serve as a central authority for establishing and enforcing cybersecurity policies, addressing Pakistan's current fragmented approach.
4. Incentives for Technology Adoption: To ease the financial burden of adopting AI, the government could provide tax incentives, grants, or subsidies to companies investing in cybersecurity technologies. Encouraging AI adoption within the private sector is critical to building a robust cybersecurity framework.
5. Strengthening Legal Frameworks: Pakistan must update its cybersecurity laws, creating a regulatory framework that supports AI-driven solutions and addresses data privacy concerns. By establishing clear guidelines and penalties for cyber offenses, the government can enhance deterrence and streamline enforcement.

Conclusion

As cyber threats evolve, the need for advanced cybersecurity measures becomes increasingly pressing. AI has emerged as a powerful tool for combating electronic crimes, providing capabilities beyond traditional methods. For Pakistan, the adoption of AI in cybersecurity is not just a technological upgrade but a necessity to secure its digital future. With renewed efforts to establish a dedicated cybersecurity agency, investment in education, and robust government-industry collaboration, Pakistan can begin closing the gap in its cyber defenses. By embracing AI-driven solutions, Pakistan can protect its critical infrastructure, strengthen its national security, and create a safer digital environment for its citizens.