PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 15 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Artificial Intelligence, geopolitics, and online fraud are transforming the cyber risk landscape

The digital world is evolving faster than ever, and the previous rules of security and safety are no longer applicable. We need to rethink how we maintain online security

By **Muhammad Haseeb** | University of Agriculture | Published: August 2026
haseebsharif.direct@gmail.com | Position: Software Engineer

Introduction

Major transformation is happening at the core of global security; something is evolving more rapidly than most people are willing to acknowledge. Instead of dealing with opportunistic hackers, we are dealing with a potent collaboration of advanced fraud, global politics, and artificial intelligence all at once. Our digital environment is shifting as a result of this collision, which is creating a new type of threat.

Pakistan is facing a very real and urgent threat. From January to September 2025, there were over 5.3 million cyberattacks on Pakistani users and organizations, which is a staggering number. What's even more concerning is that seven advanced threat groups are specifically targeting the country's telecom, banking, and government systems. This is not just a matter of statistics; it's a warning sign that the country's cybersecurity is under attack.

> ***"Cyber-enabled fraud has emerged as one of the most disruptive forces in the digital economy, undermining trust, distorting markets, and directly affecting people's lives," said Jeremy Jurgens, Managing Director, World Economic Forum"***

Technology Overview

The internet may quickly transform from a helpful tool into a war zone as international tensions increase. The attacks frequently aim at essential infrastructure, such as industrial, healthcare, and energy systems, and they can cause major damage. Sending a strategic message is the aim; data theft and disorder are not the only aims. Data centers, supply chains, and cloud infrastructure are now major targets in modern conflict, as the World Economic Forum observed in a 2026 study. To safeguard Pakistan's vital systems and infrastructure, a full and coordinated response is needed, as cybersecurity is not only a national but also a global issue. Because the stakes are so great, the nation must take immediate action to build its cybersecurity foundations and protect itself from these threats.

Artificial intelligence is giving fraud an important boost. Deepfakes, or artificial intelligence-generated audio and video, let scammers steal more than $200 million in just the first three months of 2025. According to experts, AI-assisted fraud is likely to rise by 32% annually, from $12.3 billion in 2023 to $40 billion by 2027. According to a World Economic Forum survey, almost nine out of ten cybersecurity leaders worldwide said that the fastest-growing threat they face in 2025 is AI problems. This is a serious issue because as AI becomes more strong, it will be easier for hackers to use it for criminal activities, such as creating false identities, fake news, and even fake people, which can be used to trick others into giving away money or sensitive information.

Geopolitics is a direct and verifiable cause of cyber risk, not just a background. State-aligned hacking occurs when traditional battle increases. These actors target industrial infrastructure, healthcare systems, and energy grids to send a planned signal in addition to causing disruption. Data centers, supply chains, and cloud infrastructure are currently involved in the front lines of present-day conflict, as noted in the WEF's 2026 study.

Key Findings & Impact

The decline of ransomware is the most significant change in worldwide cyber priorities. For the first time, CEOs across the world are more concerned about cyber-enabled fraud. In 2025, 75% of participants in the WEF survey reported that they or a loved one had been directly impacted by cyber-enabled fraud.

Constant threats that the modern world faces:

- Generative AI scams
- Industrial-level frauds
- Loss of online trust
- Financially and mentally invested
- loss of personal privacy

In Pakistan, where cybersecurity institutions are still relatively new relative to peer nations, 31% of the participants who responded to the global WEF research said they had little trust in their country's ability to deal with a major cyber disaster. Every year, this percentage increased.

What's Next?

Nowadays, removing harmful software is the world's top cybersecurity target. CEOs worldwide are becoming more concerned about technologically dependent fraud for the first time. According to a World Economic Forum survey conducted in 2025, an astounding 75% of the participants claimed to have been harmed by tech-based fraud. Business email scams cost an astounding $2.77 billion in 2024, according to the FBI's Internet Crime Complaint Center. In just one year, the total number of cases using artificial intelligence increased by 37%. This indicates how severe the issue of cybercrime has grown and how important it is for businesses to protect both themselves and customers from these kinds of threats.

The exposure from Pakistan reflects these worldwide trends. According to Kaspersky's 2025 data, over 42,000 ransomware attacks, 126,000 spyware incidents, and 166,000 banking malware detections were recorded in just nine months. Over 10,000 significant security alerts, 534 malicious domains banned and over 100 dark web threats were identified by the Pakistan Telecommunication Authority in its 2024–2025 reporting cycle. In Pakistan, whose cybersecurity institutions are still relatively new relative to peer economies, 31% of WEF survey participants nationwide showed low trust in their nation's preparedness for a significant cyber tragedy. The percentage has increased year over year.

About the Author

Muhammad Haseeb is a student of software engineering from Faisalabad. His areas of expertise are software architecture and the creation and use of intelligent systems. His email address is haseebsharif.direct@gmail.com.

Keywords: Artificial Intelligence; Cybersecurity; Geopolitics; Online Fraud; Pakistan Tech; Deepfake; Cyber Resilience

References

[1] World Economic Forum (2026) Global Cybersecurity Outlook 2026. Geneva: WEF/Accenture. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/digest// [Accessed 2 April 2026].

[2] Kaspersky (2025). 'Kaspersky Unveils Over 5.3M On-Device Cyberattacks in Pakistan from January to September 2025.' CybersecurityAsia.net, 21 November. Available at: https://cybersecurityasia.net/kaspersky-unveils-5-3m-attacks-on-pakistan/ [Accessed 2 April 2026]

[3] Dawn (2026). 'AI, geopolitics and online fraud reshaping cyber risk landscape.' Available at: https://www.dawn.com/news/1966691/ai-geopolitics-and-online-fraud-reshaping-cyber-risk-landscape [Accessed 13 Jan 2026].

[4] The Network Installers (2025) 'AI Cyber Threat Statistics: The 2025 Landscape of AI-Powered Cyberattacks.' Available at: https://thenetworkinstallers.com/blog/ai-cyber-threat-statistics/ [Accessed 2 April 2026].

[5] ProPakistani (2025). 'Pakistan Hit by Wave of AI Cyber Attacks Targeting Telecom and Govt Systems.' 9 October. Available at: https://propakistani.pk/2025/10/09 [Accessed 2 April 2026].

[6] Pytlak, A. (2025) 'Assessing Cyber Risks and Resilience in India and Pakistan.' Stimson Center, 30 September. Available at: https://www.stimson.org/2025/assessing-cyber-risks-and-resilience-in-india-and-pakistan/ [Accessed 2 April 2026].

[7] World Economic Forum (2025). 'How Identity Fraud Is Changing in the Age of AI.' 11 December. Available at: https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/ [Accessed 2 April 2026].

[8] Bandukda, Z. et al. (2025) 'Pakistan's Cyber Defense Revolution: AI & Machine Learning for Threat Mitigation.' Advance Social Science Archive Journal, 4(1), pp. 38–47. DOI: 10.55966/assaj.2025.4.1.041