Forum: Interpol

Issue: Addressing the Surge in Cybercrime utilising Artificial Intelligence

Student Officer: Ashish D Bansal

Position: Deputy Chair

Introduction

As technology continues to advance and connect the world, cybercrime has emerged as one of the most significant challenges for governments, businesses, and individuals. Increasing reliance on digital platforms for communication, financial transactions, and essential services has left systems vulnerable to exploitation by cybercriminals. These criminals exploit weak security to steal sensitive data, disrupt operations, and harm individuals.

Artificial Intelligence (AI), a revolutionary technology strengthens cyber defenses by automating threat detection, predicting potential vulnerabilities, and accelerating responses. But on the other hand, cybercriminals use AI to create more sophisticated and targeted attacks.

Cybercrime is surrounded by various malicious activities, including identity theft, ransomware, phishing, and data breaches. According to the International Data Corporation , cybercrime damages are projected to exceed $8 trillion this year. This staggering figure highlights the immediate need for robust global action.

Definition of Key Terms

Cybercrime

Refers to criminal activities conducted using computers or the internet. Examples include hacking, phishing, ransomware attacks, and cyber fraud.

Artificial Intelligence (AI)

The simulation of human intelligence by machines, enabling them to perform tasks such as decision-making, pattern recognition, and problem-solving.

Ransomware

A type of malicious software that encrypts a victim's data and demands a ransom for its release. These attacks have become more frequent and sophisticated due to advancements in AI automation.

Deepfake

AI-generated media that manipulates an individual's likeness in videos or images, often used maliciously for fraud, identity theft, or misinformation campaigns.

Phishing

A cybercrime technique where attackers impersonate legitimate entities through emails, websites, or messages to deceive individuals into sharing sensitive information.

Background Information

The Evolution of Cybercrime

Cybercrime has changed a lot since the internet was first introduced. In the early days, cyber threats were simple and mostly targeted individual systems. But as technology and the internet grew, cybercrime became more advanced and widespread, affecting people, businesses, and governments worldwide. Today, cybercrime includes activities like ransomware attacks, identity theft, and phishing, all of which take advantage of weaknesses in digital systems.

Artificial Intelligence (AI) has made this problem more complicated. While AI has many benefits for improving cybersecurity, it is also being used by cybercriminals to create more advanced and targeted attacks. Criminals use AI to automate phishing campaigns, bypass security systems, and even make fake videos (deep fakes) that are used to trick people or spread false information.

Economic and Social Impact

Cybercrime costs a lot of money globally. According to the International Data Corporation (IDC, 2023), cybercrime damages are expected to exceed $8 trillion worldwide. Ransomware attacks alone cost businesses billions of dollars each year, while data breaches can harm a company’s reputation and lead to financial losses. Developing countries, which often have weaker cybersecurity systems, are especially affected by these attacks.

Cybercrime also damages trust in digital systems. Victims of identity theft suffer both financially and emotionally. At the same time, fake videos and other misinformation spread through AI tools can create confusion, influence elections, and increase tensions in society. Groups like older people and those who are not familiar with technology are especially at risk.

Challenges in Addressing Cybercrime

To reduce the technology gap, wealthier nations and international groups should provide money and technical help to developing countries. Many countries lack the necessary infrastructure for strong cybersecurity, making them easy targets for attacks.

One big issue is the shortage of skilled professionals in cybersecurity in these nations. Without trained experts, it is hard to manage and stop cyber threats effectively. Partnerships between wealthier and developing countries can help by funding better internet systems, secure data storage, and cybersecurity tools. Providing affordable AI tools that can quickly detect threats would also help protect these countries.

Another problem is the low awareness of cybersecurity risks in many regions. Teaching citizens, businesses, and officials through campaigns and workshops on basic cybersecurity practices can greatly reduce risks.

The high cost of keeping and improving cybersecurity systems is another challenge. Financial aid from wealthier countries or grants from international organizations can help developing nations afford these improvements over time.

By focusing on funding, tools, training, and awareness programs, developing countries can improve their defenses against cyber threats and contribute to global cybersecurity efforts.

Causes

Economic Disparities

Economic inequality is a major reason why cybercrime happens. In areas where jobs are scarce and poverty levels are high, some people turn to cybercrime as a way to make money. The availability of cheap and easy-to-use hacking tools has made it possible for people with little technical knowledge to carry out cyberattacks.

Advancements in Technology

Rapid advances in technology, especially AI, have made cybercrime easier to commit. AI tools help criminals automate attacks, create smarter malware, and avoid being detected. For example, machine learning can identify weak spots in systems, and deepfake technology can be used to impersonate people or create fake content for fraud.

Lack of Cybersecurity Infrastructure

Many developing countries do not have the money or skills needed to build strong cybersecurity systems. This makes it easier for cybercriminals to exploit weak systems. The lack of consistent funding for cybersecurity programs makes the situation worse, leaving important infrastructure and sensitive data unprotected.

Weak Legal and Regulatory Frameworks

Many countries do not have strong or consistent laws to deal with cybercrime. Criminals often take advantage of these gaps, especially in countries where enforcement is weak. The lack of global standards makes it hard to investigate and punish cybercriminals, especially when they operate across borders.

Anonymity and Accessibility of the Dark Web

The dark web allows cybercriminals to stay anonymous while buying and selling illegal goods and hacking tools. This makes it easier for people to get involved in cybercrime and has contributed to its growth.

Globalization and Interconnectedness

As the world becomes more connected through technology, a weakness in one system can affect many others. For example, global supply chains and shared digital platforms mean that a single cyberattack can disrupt businesses and governments across multiple countries.

Major Countries and Organisations Involved

United States

The United States faces significant threats to its critical infrastructure, government institutions, and private sector from cybercriminals. The Cybersecurity and Infrastructure Security Agency (CISA) leads national efforts to safeguard systems, employing AI-driven tools to monitor and mitigate threats. American technology companies such as IBM, Microsoft, and Google are pioneers

in developing AI-based cybersecurity solutions. The U.S. also emphasizes international cooperation through initiatives like the Budapest Convention on Cybercrime.

China

China is a dual actor in the cybersecurity landscape. While the country invests heavily in AI-driven cybersecurity to protect its national infrastructure, it has faced accusations of state-sponsored cyber-crime targeting other nations. China's Cybersecurity Law and its focus on AI research demonstrate its commitment to strengthening domestic defenses. However, its strategic use of AI in cyber operations often leads to geopolitical tensions.

European Union (EU)

The European Union is a leader in establishing regulatory frameworks for data protection and cybersecurity. The General Data Protection Regulation (GDPR) sets global standards for safeguarding personal data, while the EU's Cybersecurity Act establishes certification frameworks to enhance trust in digital systems. Europe plays a key role in coordinating cross-border investigations, leveraging AI tools to identify and neutralize cyber threats.

Interpol

Interpol plays a central role in the global fight against cybercrime. Through its Global Complex for Innovation in Singapore, Interpol provides training and resources to member states to strengthen their cybersecurity capabilities. Initiatives such as the Cyber Fusion Centre and the Cyber Response Toolkit enable countries to detect, investigate, and respond to cyber threats more effectively. Interpol also fosters international collaboration by sharing intelligence and best practices among its members.

India

As one of the world's fastest-growing digital economies, India is highly susceptible to cyber threats. The National Cybersecurity Policy emphasizes the use of AI to protect critical sectors, such as healthcare, finance, and transportation. India collaborates with international organizations, including the UN and Interpol, to address cybercrime. However, challenges like outdated infrastructure and a shortage of skilled cybersecurity professionals hinder its progress.

Russia

Russia's role in global cybersecurity is controversial. While it possesses advanced AI capabilities for defending its digital infrastructure, it has faced allegations of state-sponsored cyber activities,

including election interference and ransomware attacks. Russia's stance on cybersecurity is often shaped by its geopolitical interests, leading to strained relations with other nations. Despite these challenges, Russia participates in multilateral discussions on cybercrime prevention, including those organized by the UN.

Private Sector and NGOs

The private sector and non-governmental organizations (NGOs) play a crucial role in addressing cybercrime. Technology companies like Palo Alto Networks, IBM, and Cisco develop advanced AI-driven cybersecurity tools used by governments and businesses worldwide. NGOs, such as the CyberPeace Foundation, work to raise awareness, advocate for stronger regulations, and provide support to victims of cybercrime. Public-private partnerships are essential for fostering innovation and sharing expertise in this rapidly evolving field.

Timeline of Events

Date	Description of event
1990s	The rapid expansion of the internet in the 1990s marked the beginning of global cybercrime. Early hacking incidents, such as the Morris Worm in 1988, revealed the vulnerabilities of interconnected systems. Governments worldwide began to recognize the need for stronger cybersecurity measures. However, the lack of international frameworks allowed cybercrime to grow rapidly largely unchecked.
2010s	The 2010s saw an explosion in cybercrime activities, with ransomware attacks becoming a preferred tactic. The WannaCry ransomware attack in 2017 affected over 200,000 computers across 150 countries, targeting healthcare systems, financial institutions, and government agencies. This highlighted the global impact of cybercrime and the critical need for international cooperation.
2016	AI-powered phishing campaigns and malware tools became widespread. Cybercriminals began leveraging machine learning to craft realistic phishing emails and automate attacks, significantly increasing their success rates.
2018	Interpol launched the Global Complex for Innovation (GCI) in Singapore. The facility became a hub for cutting-edge research, training, and the development of AI tools to combat cybercrime. Initiatives like the Cyber Response Toolkit and the Cyber Fusion Centre were established to enhance member states' cybersecurity capabilities.
2019	The European Union implemented the Cybersecurity Act, introducing certification frameworks to improve the security of digital systems. The Act also emphasized AI's role in detecting and responding to cyber threats. Europol intensified its collaboration with Interpol to address cross-border cybercrime.

2021	The United Nations adopted the Cybercrime Prevention and AI Ethical Use Framework, a treaty outlining ethical guidelines for AI development and application in cybersecurity. The treaty emphasized international cooperation and capacity-building initiatives to bridge technological gaps between nations.
2023	Global damages from cybercrime surpassed $8 trillion (IDC, 2023). Major ransomware attacks disrupted healthcare systems and critical infrastructure, underlining the urgency for enhanced global measures. AI-driven cybersecurity tools played a pivotal role in avoiding some of these threats, showcasing their potential in safeguarding digital ecosystems.
2024	Interpol unveiled its Advanced Cybercrime Analysis Unit, which uses AI to predict emerging cybercrime trends and coordinate international responses. The initiative brought together experts from over 100 countries to collaborate on developing cutting-edge solutions for combating cyber threats.
2025	A significant cyberattack targeted multiple financial institutions globally, exploiting vulnerabilities in AI-powered banking systems. The incident prompted the UN to convene an emergency summit, resulting in the adoption of the Global Cybersecurity Cooperation Pact, which emphasizes real-time intelligence sharing and stronger regulatory measures.

Relevant UN Treaties and Events

United Nations General Assembly Resolution 74/247, 27 December 2019 (A/RES/74/247)

This resolution highlighted the growing threat of cybercrime and called for increased international collaboration. Member states were urged to strengthen legal frameworks, share intelligence, and enhance their technological capabilities to address cyber threats effectively.

United Nations Cybersecurity Treaty, 15 March 2021

The treaty established international norms for the ethical use of AI in cybersecurity. It emphasised transparency, accountability, and inclusivity in AI development, ensuring that these tools are not weaponised by malicious actors. The treaty also supported developing nations by providing technical assistance and training programs.

Declaration on AI for Peace and Security, 2 December 2022 (A/RES/76/183)

Adopted during the UN General Assembly, this declaration encouraged the development of AI technologies specifically designed to enhance global cybersecurity. It promoted the sharing of best practices, innovations, and technical resources among member states.

UNODC Regional Cybercrime Framework, 2020

The United Nations Office on Drugs and Crime (UNODC) launched this framework to address regional disparities in cybersecurity. It involved organizing workshops, simulations, and training sessions to equip law enforcement agencies with AI-driven tools for combating cybercrime.

UNESCO Guidelines on AI Ethics, 16 November 2021

These guidelines provided a roadmap for the responsible design and deployment of AI systems, focusing on preventing misuse in cybercrime. The document stressed the importance of safeguarding human rights, privacy, and inclusivity while leveraging AI.

Previous Attempts to solve the Issue

Global Collaborations

Organizations like Interpol and Europol have made significant strides in combating cybercrime through joint operations and intelligence-sharing platforms. The establishment of the Cyber Fusion Centre has enabled real-time collaboration, allowing member states to respond swiftly to emerging threats. However, the effectiveness of these collaborations is often hindered by political tensions and the lack of standardized legal frameworks across jurisdictions.

AI-Driven Security Tools

Private sector innovations, such as IBM's Watson for Cybersecurity and Palo Alto Networks Cortex XCSOAR, have revolutionized threat detection and response. These tools analyze vast amounts of data to identify vulnerabilities and neutralize threats. While these advancements are promising, their accessibility is often limited to wealthy nations, leaving developing countries vulnerable.

Capacity-Building Initiatives

The UNODC's workshops and training programs have been instrumental in bridging the technological gap between nations. By equipping law enforcement agencies with AI-driven tools and expertise, these initiatives have improved cybersecurity capabilities in several regions. However, the scalability of these programs remains a challenge due to funding constraints.

Public Awareness Campaigns

Governments and NGOs have launched numerous campaigns to educate individuals and businesses about cybersecurity best practices. While these efforts have raised awareness, they often fail to reach vulnerable populations, such as the elderly or those in rural areas, who remain prime targets for cybercriminals.

Possible Solutions

Enhancing International Cooperation

Interpol should expand its data-sharing platforms to enable real-time intelligence exchange between member states. Collaborative AI research initiatives could foster innovation while ensuring ethical standards are upheld. Establishing a global cybersecurity task force under the UN's guidance could also streamline efforts.

Developing Global Legal Frameworks

Countries must work together to create standardized legal frameworks that address the complexities of cybercrime. These frameworks should include provisions for prosecuting AI-driven cyberattacks and mechanisms for resolving jurisdictional disputes. The UN Cybersecurity Treaty can serve as a foundation for these efforts.

Investing in Research and Development

Governments and private organizations should allocate more resources to develop advanced AI-driven cybersecurity tools. Public-private partnerships can accelerate innovation, ensuring that even resource-constrained nations can access cutting-edge technologies. Incentives should be provided for research focusing on proactive threat prevention rather than reactive measures.

Promoting Education and Awareness

Public awareness campaigns should be tailored to target vulnerable groups, such as the elderly and individuals with limited digital literacy. Educational programs in schools and workplaces can equip individuals with the knowledge to recognize and avoid cyber threats. Additionally, training programs for law enforcement agencies should focus on enhancing their understanding of AI and its applications in cybersecurity.

Strengthening Infrastructure in Developing Nations

To close the technology gap, wealthier nations and international organizations should provide financial and technical support to developing countries. Many nations lack the infrastructure needed for strong cybersecurity, leaving them vulnerable to attacks.

Partnerships between developed and developing nations can provide funding to improve internet connections, secure data systems, and cybersecurity tools. Access to affordable AI tools that detect threats can also help these countries protect themselves better.

Additionally, training programs for local experts, government staff, and law enforcement are crucial. Workshops on basic cybersecurity practices and threat detection can make a big difference.

By focusing on funding, tools, and training, developing nations can build stronger defenses and contribute to global cybersecurity.

Regulating AI Development and Usage

International guidelines should be established to regulate the ethical development and deployment of AI technologies. These guidelines must address issues like transparency, accountability, and the dual-use nature of AI, ensuring that advancements are not weaponized by malicious actors.

Establishing Cyber Crime Task Forces

Regional cybercrime task forces can provide localized solutions while maintaining coordination with global efforts. These task forces should be equipped with AI-driven tools and staffed by experts in cybersecurity and international law.

Bibliography

European Commission. “European Commission.” *Commission.europa.eu*, 2024, commission.europa.eu/index_en.

IBM. “IBM - United States.” *Www.ibm.com*, 1 Oct. 2015, www.ibm.com/us-en.

IDC. “IDC: The Premier Global Market Intelligence Firm.” *IDC: The Premier Global Market Intelligence Company*, 2019, www.idc.com/.

INTERPOL. “INTERPOL | the International Criminal Police Organization.” *Interpol.int*, 2017, www.interpol.int/.

UN. “Official Document System of the United Nations.” *Documents.un.org*, documents.un.org/.

UNESCO. *Unesco.org*, 2019, unesdoc.unesco.org/.

United Nations Office on Drugs and Crime. “United Nations Office on Drugs and Crime.” *Unodc.org*, 2019, www.unodc.org/.