Unitar Online Catalogue

CIFAL Jeju - AI and Transnational Organized Crimes

People

Date limite: 14 Aug 2025

Type:	Workshop
Emplacement:	Jeju, Republic of Korea
Date:	16 Sep 2025 to 29 Sep 2025
Durée:	4 Days
Zone du programme:	Decentralize Cooperation Programme
Site internet:	http://www.cifaljeju.org/index.php
Prix:	0.00 $US
Personne de référence de l'évenement:	jwshin.jitc@cifaljeju.org
Partenariat:	CIFAL Jeju, , Jeju Special Self-Governing Province

CONTEXTE

Artificial intelligence (AI) technologies are advancing at an unprecedented rate, promising transformative potential across a wide array of sectors, from healthcare and education to governance and economic development. Yet, alongside these positive advancements, the rapid proliferation of AI is concurrently giving rise to substantial security and governance challenges that demand urgent attention. While AI undeniably offers significant efficiency,

decision-making, and automation advantages, it's increasingly being exploited by organized criminal networks to facilitate transnational crimes. These emerging AI-enabled transnational crimes manifest in various insidious forms. We're witnessing the use of deepfake technologies for sophisticated fraud and extortion schemes, the deployment of generative AI to power large-scale phishing and social engineering attacks, the development of AI-assisted money laundering operations, and, disturbingly, the abuse of AI tools in human trafficking and child exploitation. The inherently anonymous and borderless nature of cyberspace allows these crimes to proliferate with astonishing speed and scale, frequently outpacing the capabilities of current law enforcement. These concerning trends are particularly pronounced within the Asia-Pacific region. In the Asia-Pacific region, many nations are eagerly embracing AI-driven innovation to propel their digital economies and foster sustainable growth. The region's expansive digital ecosystem, rapidly growing economies, persistent digital divides, and varied levels of cyber governance create fertile ground for AI-enabled criminal activities. Also, underdeveloped regulatory frameworks and disparities in law enforcement capacities exacerbate the problem. High rates of cross-border data flows, porous digital borders, and the rapidly evolving nature of AI applications make transnational crimes involving AI both frequent and exceedingly complex to address. Despite mounting enforcement efforts, cyber-enabled fraud has continued to intensify. According to UNODC estimates, financial losses from scams targeting East and Southeast Asian victims reached between USD 18 billion and 37 billion in 2023. Furthermore, its studies also report a staggering 1,530 per cent increase in deepfake-related crimes in the Asia-Pacific between 2022 and 2023. On average, organizations in Asia Pacific faced 1,835 new cyberattacks every week, a figure significantly higher than the global average of 1,248 . This challenging environment is further complicated by the fact that cybercriminals often leverage legally and technologically vulnerable nations as bases for activities like ransomware distribution, and illegal server operations, exploiting the physical distance between the crime's origin and its victims to evade international investigations. In response, many Asia-Pacific governments are adopting multifaceted strategies. For example, Australia published its AI Ethics Principles in 2019 and updated its Voluntary AI Safety Standard in September 2024, establishing 10 “AI guardrails” to ensure systems are safe, secure, and reliable, while Malaysia launched a National AI Office in December 2024 with mandates to develop ethical AI codes, craft a five-year AI strategy, and regulate the responsible use of AI. International organizations such as the United Nations are also playing key roles. UN Women emphasizes the adoption of a zero-tolerance policy towards all forms of violence and harmful behaviour in digital environments , while the OHCHR recommends bans on AI applications that

cannot comply with international human rights law, and moratoriums on the sale and use of AI systems that carry a high risk of adverse human rights impacts, unless and until adequate safeguards are in place . These initiatives support capacity building, responsible AI governance in criminal justice, and stronger legal cooperation across borders. Given the rapidly evolving threat landscape, proactive engageme

OBJECTIFS D'APPRENTISSAGE

By the end of the workshop, participants will be able to: • Provide a shared understanding of the AI-enabled crime landscape, new attack vectors, and evolving criminal tactics. • Strengthen networks for knowledge sharing, operational coordination, and joint responses, especially on cybercrime and trafficking. • Identify innovative policy, technological, and capacity-building solutions addressing regional cybersecurity and AI risks. • Develop concrete proposals for public-private partnerships, legal cooperation, and asymmetric defence strategies. • Create or design a strategic roadmap guiding future policy, resource allocation, and targeted interventions.

CONTENU ET STRUCTURE

Opening Lecture 1. The New Frontier of Crime: Understanding AI and Its Transnational Impact Lecture 2: AI-Driven Financial Crime: Emerging Trends and Strategic Responses Lecture 3. AI-Facilitated Human Trafficking & Sexual Exploitation Lecture 4. Countering AI-Driven Disinformation Lecture 5: AI for Preventing Crime Lecture 6: The Use of AI in Digital Forensics and AI-Powered Detection Tools Site Visit: National Information Society Agency Field Trips Action Planning Case Sharing

MÉTHODOLOGIE

The workshop consists of: • Expert-led lectures • Community/City/Country-level case study sharing • Group Activities • Field Trips

AUDIENCE CIBLE

This training is open to relevant policymakers, law enforcement officials, judicial officers, cybersecurity experts, intelligence analysts, and representatives from civil society organizations and the private sector from the Asia Pacific region, who have been engaged in tasks for sustainable development in line with SDG 16 (Peace, Justice and Strong Institutions) and SDG 17 (Partnerships for the Goals).