Promoting the responsible use of emerging technologies, including Artificial Intelligence, to address crime and exploitation (10 min)

G7 - Roma-Lyon Group
Heads of Delegation Meeting

18 April 2024 14:00 – 15:30

Topic 7: Artificial Intelligence

Excellencies, Ladies and Gentlemen,

It is a pleasure to attend this important debate here today on behalf of the United Nations Interregional Crime and Justice Research Institute (UNICRI) and to share UNICRI's experience in relation to the responsible use of emerging technologies, including Artificial Intelligence, to address crime and exploitation.

(Slide 2) The role of new and emerging technologies as disruptors, enablers, and tools of crime is transforming the criminal justice landscape. Criminals can leverage these technologies for tracking, profiling, and accessing targets and victims with frightening efficiency. This has led to an extensive spectrum of cybercrimes becoming commonplace. Platforms, virtual spaces, and social media have fundamentally changed how we experience crime and victimization.

However, these same technologies offer powerful solutions. New and emerging technologies have also encouraged innovations in crime prevention, detection, and control. Artificial intelligence (AI) tools and even large language models (LLMs) can be applied to detect and combat crimes related to illicit financial flows, online child sexual exploitation, counterfeit goods to name few.

Facial recognition technology has also been adapted to support law enforcement investigations for identification and authentication.

This rapid uptake of technology is not without threats to public safety, human rights, and digital inclusivity. It also has significant implications for population groups, for example ethnic minorities, women, and children, who may find themselves increasingly vulnerable to technology tools related to surveillance and data collection.

As a UN research and training institute mandated in the field of criminal justice and crime prevention, UNICRI has closely monitored and analyzed new trends and developments in the use of information and communication technologies (ICTs), artificial intelligence (AI), the Internet of Things, biometrics, and augmented and virtual reality. Our work and research, guided by the 2023-2026 Strategic Programme Framework, is focused on promoting the responsible use of these technologies to address crime and exploitation. Let me give you a few examples.

(slide 3) In November 2023, UNICRI released a comprehensive study on SDG 16, which explored the impact of digitalization on peace, justice, and strong institutions. This study delved into issues such as the digital divide, legal and digital identity, illicit financial flows, misinformation, and disinformation online, and conflicts in the digital space. As follow-up to this activity, we are leading a research project with ITU's Africa Regional Office to assess the multifaceted challenges faced by cybercrime victims and the implications on cybercrime investigations in the African context, spotlighting the complexities at both the individual and systemic levels, and paving the way for informed interventions that enhance the accessibility and efficacy of justice in the aftermath of cybercrime.

This initial research will focus on Eritrea, Namibia, Sierra Leone and South Africa, with the possibility to extend the research on other African Member States in a later stage.

UNICRI has undertaken significant efforts to understand and combat cybercrime and cyberterrorism. We are currently conducting a study, in partnership with the UN Office of Counter-Terrorism, on the use of the Dark Web by terrorist groups. This research enhances the knowledge and understanding of how terrorist and violent extremists use the dark web and the degree to which the crime-as-a-service model's role is being utilised to augment the existing capabilities of terrorist and violent extremist groups and individuals to carry out cyber-enabled terrorism. Additionally, this research aims to support law enforcement and counter-terrorism agencies in their investigations into illicit activities on platforms such as Discord, Telegram, and Rocket.Chat.

Connected to this, UNICRI is also leading a research project into the cyber-enabled threats posed by right-wing and left-wing extremist movements, particularly in the Global South. This project strives to analyse and assess the threats posed by the illegal abuse of technologies and ideologically motivated cyberattacks by focusing on how these threats manifest.

Since 2017, UNICRI has actively explored advancements in the field of AI through its Centre for AI and Robotics. The Centre, located in the Hague, The Netherlands, has focused on advancing understanding of AI use cases in the context of law enforcement, in particular in domains such as child sexual exploitation and abuse and countering terrorism online, and the promotion of responsible AI innovation in law enforcement. In 2023, UNICRI notably released its Toolkit for Responsible AI innovation in Law Enforcement.

UNICRI has also explored the malicious uses of such technology, analyzing the impact of AI in cybercrime and the risk of terrorist and violent extremist use of AI in respective studies with Europol, Trend Micro and the UN Office of Counter-Terrorism.

In 2020, responding to the alarming rise in child sexual exploitation and abuse materials, UNICRI and the Ministry of Interior of the United Arab Emirates launched the AI for Safer Children initiative. This initiative aims to empower law enforcement agencies worldwide by building their capacities to leverage AI and related technologies effectively. The exponential increase in child abuse materials has overwhelmed law enforcement capacities globally. For instance, reports surged from approximately 100,000 in 2010 to an astounding 36.2 million by 2023.

(Slide 4) To address this crisis, we developed the AI for Safer Children Global Hub in July 2022. This online platform provides investigators access to over 80 cutting-edge AI tools, available in all six UN official languages, designed to expedite investigative workflows and enhance international collaboration.

The Hub, currently servicing over 700 officers from 111 countries, not only offers tools for object detection, voice recognition, and geolocation but also serves as a community for law enforcement to share insights and strategies, and offers tailor made direct capacity building trainings. Since last summer, UNICRI provided training to 24 countries through national or regional training programs.

In 2023, UNICRI launched a Master's Programme in Cybercrime, Cybersecurity, and International Law, in partnership with UPEACE. This program equips participants with advanced knowledge and skills to combat cybercrime and understand cybercrime prevention strategies on an international scale.

Misinformation, disinformation and hate speech online is an issue of cross-cutting interest for UNICRI. Notably, UNICRI runs an annual Summer School on Misinformation, Disinformation and Hate Speech, an introductory course aimed at understanding the phenomenon of disinformation, misinformation, and hate speech, how they manifest and the tools available to combat them. In the specific domain of CBRN risks, UNICRI has conducted a study on misinformation and disinformation and, in January 2023, released a handbook on combatting CBRN disinformation. The role of AI in the generation of such fake content, and in particular deepfakes, is also an area of relevance for UNICRI, with UNICRI having run deepfake detection hackathons in 2019 and various workshops focused on deepfakes and deepfake detection.

Starting in 2023, we began exploring the use of ICTs in prison rehabilitation. This initiative seeks to leverage technology to support rehabilitation, reduce reoffending, and establish ethical and human rights principles for digital rehabilitation in prisons.

Finally, a noteworthy example of our collaborative efforts involves the International Atomic Energy Agency (IAEA). Together, we are intensifying efforts to use nuclear science to combat various forms of illicit trade, including trafficking in cultural goods, a market estimated at US $1.2 billion to $1.6 billion annually. Such criminal activities cover theft of cultural property from museums, illicit excavation and looting of archaeological sites and illicit transfers in ownership. Trafficking in cultural property, together with the destruction of cultural heritage, has been recognized as a threat to international peace and security by the United Nations Security Council.

From a broader perspective, nuclear analytical techniques can play a pivotal role in supporting national authorities in Member States in investigating and prosecuting different forms of illicit trade and forgeries. These techniques can contribute at least in three important ways. Firstly, to identify non-original products which fraudsters intend to pass off as originals; secondly, in the area of cultural property to identify trafficked works of art and cultural property; and thirdly in the area of precious metals, to support the identification of the exact geographical provenance of gold, platinum, and other metals, also contributing to the discovery of illegal mining operations and illicit trafficking of precious metals. In partnership with the IAEA, we aim at establishing a platform that will leverage IAEA's expertise in nuclear analytical techniques and UNICRI's knowledge in crime prevention to provide law enforcers and forensic experts with more effective tools to detect, identify, investigate and prosecute various forms of illicit trade.

As we navigate this dynamic landscape, UNICRI remains committed to ensuring that technological advancements in criminal justice serve to enhance, not hinder, our collective efforts to uphold justice and human rights. Our focus is to balance innovation with integrity, ensuring that the tools we deploy in our fight against crime are used wisely and ethically.