Center for Cyber Risk Research and Policy at the
Cyber Institute

5 Union Square W.
New York, NY 10003

PROPOSAL TO THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

THIRD SESSION: INTERNATIONAL COOPERATION, TECHNICAL ASSISTANCE, PREVENTION MEASURES AND THE MECHANISM OF IMPLEMENTATION

August 2022

Preface

This is a multi-stakeholder submission from a non-governmental organization in consultive status with the United Nations Economic and Social Council submitted after 29 July 2022, for consideration by the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes future sessions.

Introduction

Honorable Secretariate and Committee Colleagues thank you for allowing us the opportunity provided to the representatives of the international multistakeholder community to contribute concepts and collaborative covenants to protect

Proposed Provisions

Technological developments often outpace interrelated developments in law, regulations, policy, culture, and knowledge regarding their effective use[1]. New opportunities for perpetrators may contribute to a rise in the levels and complexity of crime. Emerging Technologies such as Artificial Intelligence, Quantum Computing, and Blockchain have become increasingly exponential enabling innovations for potential criminal actors exploiting Information and Communication Technologies[2]. Criminal use case; Artificial Intelligence could be employed as a *tool* for cybercrime, making use of its capabilities to facilitate actions against real world targets: predicting the behavior of people or institutions in-order-to discover and exploit vulnerabilities; generating fake content for use in blackmail or to sully reputations; performing feats that human perpetrators are unable or unwilling to do themselves, for reasons of danger, physical size, speed of reaction and so on. The use of adversarial artificial intelligence is projected to impact the global community in some of the following ways: impersonation of trusted users, threat actor stealth, and faster attacks with more effective consequences[3]. Although the methods are new, the crimes themselves may be of traditional type theft, extortion, intimidation, terror. AI systems may themselves be the *target* of a criminal activity:

[1] *Emerging Technology Trends and Their Impact on Criminal Justice, 2018* (https://www.rand.org/pubs/research_briefs/RB9996.html)
[2] *AI-enabled future crime, 2020* (https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8).
[3] *3 ways AI will change the nature of cyber-attacks, 2019* (https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/).

circumventing protective systems that present obstacles to a crime; evading detection or prosecution for crimes already committed; making trusted or critical systems fail or behave erratically in-order-to cause damage or undermine public trust. Online environments, where data is property and information power, is ideally suited for exploitation by AI-based criminal activity which can have substantial real-world consequences. Unlike many traditional crimes, crimes in the digital realm are often highly *replicable*: once developed, techniques can be shared, repeated, even sold, allowing the potential for *marketisation* of criminal techniques or provision of "crime as a service". This may lead to a lowering of technological barriers as criminals are able to outsource the more challenging aspects of their AI-based crime.

Recent cybersecurity reports have further shown that cybercriminals are getting better in their activities by using technologies. A predictive amplifier of AI-based crime is an even more nascent emerging technology, quantum computing. With quantum computing capabilities, every organization in the world that stores, and processes data will be wide open to accelerated cyberattacks. In September 2020, the first case of cybercrime causing death was recorded when a ransomware attack caused IT failure at a hospital in Dusseldorf, Germany. The case has caused havoc throughout the healthcare industry, with the expenses to protect against cyberattacks expected to cross the $125 billion mark by 2025. Other industrial areas such as energy pipelines, meat-packing plants, and water supply centers have also witnessed several cyber-attacks over the past year. In May 2021, cyber criminals hacked into the U.S.'s Colonial Pipeline, blocking their services and demanding a $5 million ransom, which was paid. Ransomware attacks increased 151% in 2021, according to the World Economic Forum[4], with an average of 270 cyberattacks per organization, a 31% increase from 2020. While these attacks are damaging (each breach costing about $3.6m), the damages are predicted to be even greater when amplified by emerging technologies such as AI and quantum computing[5].

Emerging Technology Alignment

To ensure alignment with the Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, the Global Programme on Cybercrime mandate to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance[6], this committee should therefore include emerging technology workforce development and training to ensure a wider adoption and integration of the conventions of our draft convention. There is an urgent need for cooperation among states to mitigate threats such as cybercrime, cyberattacks on critical infrastructure, electronic espionage, bulk data interception, and offensive operations intended to project power by the application of force in and through cyberspace. Emerging cyber threats could precipitate massive economic and societal damage, and international efforts need to be recalibrated to account for this new reality. Though, there are many challenges to international cooperation and establishing international guidelines to fight global cybercrime across borders. As further expressed by the United Nations General Assembly, Agenda Item 107, Resolution Adopted December 27, 2019, and taking into account the existing international and regional conventions on cooperation in the penal field, and comparable treaties that exist between United Nations member States and emphasizing that this present Convention is envisioned to complement those conventions, we implore this Ad Hoc Committee explore and *deliberately include aspects of emerging technologies* into our discussions as we collectively undertake this endeavor.

---

[4] https://www.investmentmonitor.ai/news/business-leaders-cyber-crime-wef-report

[5] https://www.zdnet.com/article/ai-quantum-computing-and-5g-could-make-criminals-more-dangerous-than-ever-warn-police

[6] UN Office of Drug and Crime, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html