International Convention on Countering the Use of Information and CommunicationsTechnologies for Criminal Purposes

Remarks by the Center for the Study of Crime (GR)

DIGITAL CRIMINOLOGY & CYBERCRIME LAB

Athens, April 10th 2023

Principal Investigators:

Dr. Fotios Spyropoulos, PostDoc – University of West Attica (GR), PhD on Penal Law & Criminology – University of Athens (GR), Attorney at Law, Master on criminologist, Master on criminal justice, VP – Center for the Study of Crime

Evangelia Androulaki, PhD can. – University of West Attica, Attorney at Law, Master on criminology

Members of the working team:

1. Sofia Alexopoulou, Doctor of Political Science, Örebro University of Sweden and Public Servant at the General Secretariat for Coordination (Greek Ministry of Digital Governance).
2. Maria Patriki, Sociologist, MSc student of Sociology and Social Research at Universität zu Köln.
3. Andriana Selianiti, Sociologist, Criminologist & Support Coordinator for victims of crimes and their families.
4. Marina Tsaloupi, Sociologist, MSc student of Criminology and Criminal Psychology at the University of Essex.
5. Panagiota Vlachou, Ph.D. Candidate of the Aristotle University of Thessaloniki, Attorney at Law.

Dear Secretariat to the Ad Hoc Committee,

Introduction

The Center for the Study of Crime (CSC) hails your initiative on drafting a comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Its importance lies in four key reasons. This convention constitutes a unique tool for the harmonization of national laws in this field, ensuring that countries will be in a position to share a common understanding of the actual content of cybercrime and possible ways to tackle it. Furthermore, the convention incorporates several provisions that aim at protecting human rights not only at the individual level but also at the level of social groups.

It is suggested by our Center that different disciplines such as political science, law, forensics and criminal psychology, among others, should be integrated into the collaborative efforts between agencies to strengthen their effectiveness. These fields of study encompass a comprehensive analysis of criminal behavior, including victims, perpetrators, motivations, and other factors. Observing and incorporating insights from such experts into the development of the Convention would prove highly advantageous. The key goal is to enhance preventive measures by leveraging the expertise of specialists who can anticipate various scenarios and individual behaviours.

The current submission is the result of collective work from experts and practitioners across multiple disciplines. In the following section, we provide our recommendations, suggestions, and rationale by conducting an article-by-article analysis of the convention. Our analysis focuses on the section on Preventive Measures (Chapter VI). More specifically:

Proposed modifications to the section on Preventive Measures in the Convention on Cybercrime

Article 90 General provisions on prevention, paragraph 2(b): *"Developing, facilitating and promoting public awareness activities, public information campaigns, public education programmes and curricula and policies aimed at the prevention of [cybercrime] [the use of information and communications technologies for criminal purposes], including media and information literacy programmes targeting in particular vulnerable groups such as children, youth and elderly people. Such information may be disseminated, where appropriate, through the mass media, and relevant programmes and policies shall include measures to promote* *public participation in preventing and combating [cybercrime] [the use of information and communications technologies for criminal purposes];"*

Suggested amendment

We recommend that public awareness should be disseminated not only through the mass media and relevant programs but also through social media platforms since many cybercrimes take place in this environment[1].

Moreover, it is also important to include people with disabilities as a vulnerable group. People with disabilities have diverse needs compared to other vulnerable groups due to the impairments that they experience. People with disabilities can suffer from visual impairment, hearing impairment, physical and motor impairments, and learning difficulties based on existing literature[2], circumstances that may lead to digital exclusion[3] and their relation to the digital technology may be affected. That is the reason why awareness and technology and law design policies should take their needs into account.

Article 90 General provisions on prevention, paragraph 2(c): "*Issuing regular, non-binding advisories on incident prevention and sharing them with the public with a view to preventing cyber-incidents that could lead to criminal activities;"*

Suggested amendment

We propose to expand the term "cyber-incidents, especially in social media platforms…", since a plethora of cyber-incidents, and in particular cyber-violent incidents occur on social media platforms[4].

Article 90 General provisions on prevention, paragraph 2(e): *"Encouraging enterprises within their jurisdiction to employ risk-based approaches to improve their resilience to the offences set out in this Convention and to detect, respond to and recover from such incidents;"*

[1] Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Appl. Comput. Syst.*, *24*(1), 9-17. https://doi.org/10.2478/acss-2019-0002

[2] Haage, A., Bosse, I.K. (2017). Media Use of Persons with Disabilities. In: Antona, M., Stephanidis, C. (eds) Universal Access in Human–Computer Interaction. *Human and Technological Environments*. UAHCI 2017. Lecture Notes in Computer Science, 10279. Springer, Cham. https://doi.org/10.1007/978- 3-319-58700-4_34

[3] Pérez-Escolar, M. & Canet, F. (2022) Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework. *Universal Access in the Information Society.* https://doi.org/10.1007/s10209-022-00867-x

[4] Peterson, J. & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *Aggression and violent behavior*, 34, 193-200. https://doi.org/10.1016/j.avb.2017.01.012

Suggested amendment

We recommend the replacement of paragraph 2(e) of article 90 of the Convention. Encouraging enterprises to improve their resilience to cybercrimes[5] is not sufficient; rather the States should implement measures to ensure that enterprises will secure their systems from malicious activities and cyber-attacks. Furthermore, it is suggested that enterprises should inform the competent authorities when they become aware of such offences.

The recommended paragraph could be as follows: *"Implementing measures to ensure that enterprises within their jurisdiction apply specific and effective rules for the prevention and detection of cybercrime regarding their digital activities and provided services, and promptly inform the competent authorities when they become aware of such incidents, either on their own initiative or following a complaint from the public;"*

Article 90 General provisions on prevention, new paragraph

Suggested additional paragraph

We recommend an additional paragraph between paragraphs 2(h) and 2(i) of article 90 in line with article 93, paragraph 1. The public and private sectors need to collaborate for the effective prevention and detection of cyber-crimes[6]since the offender's identity can be traced and obtained in some cases with the aid of private sector organisations, such as social media platforms, especially when it comes to vulnerable groups.

The new paragraph could be as follows: *"(i) Encouraging the private sector to assist the authorities in prevention and investigation of cybercrime by providing information about the identity and/or activities of users of their services, where there is information regarding their possible involvement, or the possible involvement of members of their families or close associates or persons acting on their behalf, in the commission of offences established in accordance with this Convention, in particular, gender-based violence and hate crimes;"*

[5] Rothrock, R. (2018). *Digital resilience: Is your company ready for the next cyber threat?*. Amacom.

[6] Greiman, V. (2015). Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration. *Journal of Information Warfare*, 14(3), 30–42. https://www.jstor.org/stable/26502729

Article 90 General provisions on prevention, paragraph 4: *"States Parties shall endeavour to gather national and regional prevention experiences to create a multilateral repository, administered by the United Nations Office on Drugs and Crime, enabling the dissemination of good practices in the prevention of [cybercrime] [the use of information and communications technologies for criminal purposes] in diverse contexts. The Office shall facilitate the sharing of best practices with regard to effective and successful preventive measures against [cybercrime] [the use of information and communications technologies for criminal purposes].*"

Suggested amendment

Apart from the establishment of a multilateral repository administered by the United Nations Office on Drugs and Crime, the various States Parties should establish their national repository where they will have the opportunity to collect and store good practices and useful testimonies at the national level. Those good practices can be drawn from both the public and private sectors. In the European context, similar repositories have been established in various sectors of interest by applying certain standards[7].

Even though it is widely accepted that societies should work on preventing cybercrime, there is still a lack of binding and narrowly defined practices that could advance preventive measures. Specifically, computational science is relatively new and therefore, there is not sufficient scientific knowledge in this field.[8] States parties should agree upon the establishment of an agency that is staffed by experts and conduct research on the development of the usage of Machine Learning (ML) and Artificial Intelligence (AI) as preventing measures for cybercrime.[9]

[7] Sīle, L., Guns, R., Ivanović, D., Pölönen, J., & Engels, T. C. (2019). Creating and maintaining a national bibliographic database for research output: *Manual of good practices*. https://repository.uantwerpen.be/docman/irua/35856f/163332.pdf

[8] Tong, E. Y., Zadeh, A., Jones, C., & Morency, L. (2017). Combating Human Trafficking with Multimodal Deep Models. *Meeting of the Association for Computational Linguistics*. https://doi.org/10.18653/v1/p17-1142

[9] Wiriyakun, C., & Kurutach, W. (2021). Feature Selection for Human Trafficking Detection Models. *2021 IEEE/ACIS 20th International Fall Conference on Computer and Information Science (ICIS Fall)*. https://doi.org/10.1109/icisfall51598.2021.9627435

Article 92 Participation of society, paragraph 1(b): "*Ensuring that the public has effective access to information;*"

Suggested amendment

We recommend the addition of the phrase *"especially vulnerable groups"* to paragraph 1(b) of article 92 of the Convention, since vulnerable people, such as the elderly and people with disabilities, encounter more often digital exclusion[10]. Therefore, specific measures should be taken in accordance with their individual needs.

[10] Pérez-Escolar, M. & Canet, F. (2022) Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework. *Universal Access in the Information Society.* https://doi.org/10.1007/s10209-022-00867-x