05

CYBERCRIME

DR. TATIANA TROPINA, SENIOR RESEARCHER AT THE MAX PLANCK INSTITUTE FOR FOREIGN AND INTERNATIONAL CRIMINAL LAW

INTRODUCTION

The aim of this module on cybercrime is to build awareness among civil society participants about the different approaches used to address the problem of cybercrime in a multistakeholder environment. The module will aim to explain the phenomenon of various forms of cybercrime and draw the distinction between cybercrime and national security issues in the context of cybersecurity. Furthermore, it will provide an overview of technical, legal, and organisational challenges related to fighting crime in digital networks. Finally, the training will provide an analysis of the current ways to address the multifaceted problem of cybercrime at the national and international level from different perspectives: legal frameworks (substantive criminal law and procedural law), jurisdiction, public-private collaboration, awareness raising, and capacity building.

THE WHAT – WHAT IS THE TOPIC ABOUT?

There is no commonly held definition of cybercrime. It can be referred to, in the narrow sense, only as acts against computers and information networks. However, this definition excludes many illegal activities that involve, but do not target computers and information-communication networks, such as creation, access to, and distribution of child abuse images, grooming, or identity-related crime. Yet when cybercrime is defined as any crime that involves computers or computer systems, the term becomes unnecessarily broad. Many criminal acts might possibly include the use of computers and networks; however, these activities do not constitute the substantial element of the crime, such as, for example, the use of email by drug dealers for communication.

Such important international legal instruments as the Council of Europe Cybercrime Convention, the League of Arab States Convention, and the African Union Convention on Cybersecurity do not provide a definition of cybercrime, but rather outline the acts that constitute what they call “cybercrime.” Most of them refer to crimes against confidentiality, integrity, and availability of computer data and systems; computer-related crimes such as computer fraud and forgery, illegal content; and child abuse crimes. Thus, the definition of cybercrime mostly depends on the underlying purpose behind the use of this term.

Furthermore, from the perspective of criminal justice, the term “cybercrime” should operate on a number of levels. The definition of criminal conduct should

be very specific concerning certain individual unlawful acts that entail criminal responsibility to follow the principle of legal certainty. However, for the purpose of criminal justice, the term has to be sufficiently broad to ensure that investigative powers and international cooperation mechanisms can be applied with effective safeguards and protection of privacy and human rights to the continued migration of offline crime to cyberspace. This will guarantee that digital evidence can be collected in a transparent and accountable manner within the strict legal frameworks and presented in courts.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The issue of fighting cybercrime raises several major challenges for human rights protection. First of all, there is a specific concern for the manner in which the state achieves its criminal justice goals. The law of criminal procedure and the process of cybercrime investigation should come under particular scrutiny from an international human rights perspective, because investigative measures can be simultaneously seamless and very intrusive. Furthermore, human rights standards can potentially be endangered by bulk data collection for the purpose of crime prevention. Last but not least, content-related crimes can be of particular concern. Measures taken against these crimes can restrict freedom of expression and can possibly be turned into an instrument of oppression.

THE WHO – WHO ARE THE MAIN PLAYERS?

Before the evolution of information and communications technologies, fighting crime was mostly considered to be the domain of national governments. The legal frameworks, which regulate prosecution and investigation of crime, always imply sovereignty issues and require effective mechanisms of enforcement, which are based on hierarchical structures and command-and-control approach. The decentralised architecture of the internet is eroding old paradigms of the division of responsibilities between government, the private sector, and civil society even in less flexible areas such as criminal law and criminal investigation. The problem of cybercrime requires the development of effective solutions at various levels, both national and international, and involves both non-governmental and governmental stakeholders.

Thus, industry intermediaries (not only ISPs) are becoming “critical nodes” for preventing and investigating cybercrime and safeguarding the security of their customers. While national governments have the power to establish and enforce legal and regulatory frameworks, the private sector, which owns and manages the ICT networks and offers the services, better understands the changing and converging nature of the ICT environment and has greater adaptability towards new technologies, more expertise, and resources to produce an adequate response to cybercrime threats. Involvement of the private sector in fighting cybercrime is being developed at the national level in many countries far beyond ad hoc collaboration for investigating particular cases of cybercrime or blocking and removing illegal content. It is taking the form of industry cybercrime codes of conduct, public-private reporting platforms, multi-industry public-private collaboration programmes against cybercrime, national botnet detection and mitigation projects involving internet service providers, to name but a few.

Civil society has always been considered an important stakeholder for raising awareness about cybercrime and helping citizens to understand that each person is a crucial part of a larger 'security chain.' However, one of the most prominent roles of civil society is ensuring transparency, safeguards, and human rights protection concerning cybercrime prevention and investigation. This is because electronic communications enable bulk data collection and the accompanying investigative measures can be simultaneously seamless and very invasive.

Since the trans-border character of cybercrime calls for counteractions that are coordinated on different levels – national, regional, and global –international and regional organisations, both governmental and nongovernmental, are also important stakeholders. They deal with a range of issues from harmonisation of substantive criminal and procedural frameworks, (E.g. The Council of Europe) to operational coordination of cybercrime investigations (E.g. Europol), capacity building, awareness raising, and human rights protection.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The problem of fighting cybercrime reflects the tension between nonflexible legal frameworks – which, like criminal law, were not meant to be flexible by their nature – and the non-hierarchical structure and borderless nature of the information and communications networks that do not fit the traditional top-down command and control models. Until quite recently, the problem of cybercrime was considered mainly a legal issue that focused on updating old legal frameworks, which were not applicable to the crimes committed in cyberspace, and development of procedural measures to address the new technologies and trans-border component of the problem.

However, today cybercrime is not considered solely a legal matter. Though law (especially compatible substantive legal frameworks to avoid safe havens for cybercriminals) is one of the most important components of tackling the illegal use of information networks, criminal law can only react to the problem when a crime has already taken place. Proactive measures, in addition to reactive approaches, include capacity building and collaboration among the public sector, private companies, and civil society to provide training and education, to raise awareness about cybercrime, and to make cyberspace a safer place for businesses and users.

THE WHERE AND WHEN – WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Crime in the digital environment is a fast-changing multifaceted problem; addressing it is always like chasing a moving target. There is no 'one fits all' solution as well as no legal and policy frameworks that can cover every aspect of the problem and solve it in the short term. Understanding the complexity of the ecosystem, a combination of using a top-down approach for criminal law enforcement and a bottom-up approach, along with collaboration between public and private stakeholders, transparency, and accountability, are the necessary components of any strategy to tackle cybercrime.

Since the problem is transborder, there are two levels at which to address it: national and international. In the field of harmonisation of legislation, binding and nonbinding international legal frameworks related to cybercrime were created by the Council of Europe, the European Union, the Commonwealth of Independent

States, intergovernmental African organisations like the African Union, and the League of Arab States. However, the issue of tackling cybercrime has been on the agenda of different international organisations and agencies. The G8 Group of States, Organisetion of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Organisation for Economic Co-operation and Development (OECD), Association of South East Asian Nations (ASEAN), Interpol and Europol, and many other organisations are dealing with cybercrime policy and strategy, the harmonisation of legal frameworks and operational activities, capacity building, and awareness raising. On the national level, there are many forms of addressing the problem of crime in digital networks: adoption of legal frameworks to investigate and prosecute cybercrime, awareness raising campaigns, training and capacity building, prevention, detection, and early disruption. The involvement of the private industry and civil society can be witnessed on both the national and international level concerning all forms of fighting cybercrime. Many countries and international organisations are trying to get industry and civil society organisations engaged in policymaking and lawmaking processes in a top-down manner, via stakeholder consultations to ensure transparency and protection of privacy and human rights. However, the bottom up approaches and voluntary initiatives of private industry actors and civil society activists are also very important components of fighting cybercrime on the national level.

SUGGESTED LITERATURE

- UNODC. *Comprehensive Study on Cybercrime*. 2013. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Rob van den Hoven van Genderen. *Cybercrime investigation and the protection of personal data and privacy. Discussion paper.* 2008. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study5-d-provisional.pdf