Cybercrime in the Perspective of the European Legal Framework

Aldo Shkëmbi
Darjel Sina

"European University of Tirana"
Corresponding author: Cel: +355696699753/ aldo-sh86@hotmail.com

Doi:10.5901/mjss.2013.v4n9p327

Abstract

This paper analyzes the European legal framework on cybercrime. It focuses on the criminal law framework on cybercrime with a mainly European perspective, based in the new modern challenges that have emerged in the form of cyber-crime as criminal groups have taken effectively advantage of technologies. The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries of the European Union, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from cyber- crime, with the introduction of new investigative powers and the facilitation of international cooperation.Cybercrime is a term that is used to refer to a broad range of different activities relating to the misuse of data, computer and information systems, and cyberspace for economic, personal or psychological gain. Policy-makers at the EU and at national levels, academics and law enforcement practitioners have put forward different definitions and systems classifying cybercrime as attacks against information systems, online fraud and scam schemes, identity theft, illicit trading or dissemination of illegal content such as child sexual abuse material. The Union should therefore promote policies and legislation that ensure a very high level of network security and allow faster reactions in the event of cyber disruptions or cyber- attacks.

1. Introduction

This paper provides an overall picture of the European legal framework concerned with the repression of cybercrime. This matter has been subject to intervention by a number of international institutions worldwide, such as the United Nations, the G8, the Organization for Economic Cooperation and Development (OECD), the Commonwealth, the Council of Europe (CoE) and the European Union (EU). From a European perspective, two international agreements are of particular relevance both for their (mainly) European focus and their legal effect: the 2001 Council of Europe Convention on Cybercrime (henceforth the CoE Convention) and the 2005 European Union Framework Decision on attacks against information systems (henceforth the FD) (Council of Europe, 2001; European Union, 2005).

Cybercrime provokes such high international concern because it has intrinsic characteristics which hamper its repression. In response to these distinctive features of cybercrime, the solutions are the reduction of frictions among national legislations, the introduction of new investigative powers, as summarized in section, and the improvement of international cooperation. This paper presents the main provisions and criticisms relating cybercrime and concludes by discussing the problems relating to the implementation and effectiveness of the instruments.

2. Cybercrime and European Legal Framework

Cybercrime may be defined in a narrow sense as any offence targeting computer data and systems or in a very broad sense as any offence involving a computer system. The first one risks being too restrictive as it would exclude phenomena that do exist in the physical world but have gained a different quality and impact through the use of computers, such as child pornography, fraud or intellectual property right violations.

It is important to apply a definition that covers new types of crime as well as old types of crime using computers without being too broad and therefore meaningless. The definition should be sufficiently robust to cover all relevant types of conduct even if technology evolves and phenomena of cybercrime appear to change almost every day. Finally, it should be possible to operationalise it for criminal law purposes in order to meet the rule of law principle that there cannot be a crime without a law.

Only conduct established as a criminal offence can be considered a crime. A definition should furthermore be

widely accepted and not be limited to a specific country and the corresponding domestic legislation.

A concept or "definition" meeting these requirements, that is neither too narrow nor too broad, that is normative and that is widely accepted, is available with the Council of Europe's Budapest Convention on Cybercrime. Under this treaty, cybercrime denotes: Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices.

Offences committed by means of computer systems. This list is limited to those "old" forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale. This concept is capable of capturing cases that consist of a combination of different types of conduct.

Although the Budapest Convention was prepared by the Council of Europe (with currently 47 European member states), Canada, Japan, South Africa and the USA participated in its elaboration and signed it. The USA ratified it and became a full party in 2006. Other non- European countries are in the process of accession to the Convention on Cybercrime (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal). The concept or "definition" of cybercrime as proposed by the Budapest Convention is widely shared and applied in practice. In addition to offences against and by means of computer data and systems, the Budapest Convention addresses a further issue, namely, the question of electronic evidence in relation to any crime involving a computer system. Obviously, even the broadest definition would not consider an offence where computers play an ancillary role to constitute cybercrime.

However, governments – possibly as part of a cybercrime strategy – would have to address the challenge of creating the criminal justice capabilities necessary for the collection, analysis and use of electronic evidence not only in relation to crimes against and by means of computers but in relation to any crime. This broadens the scope: since any offence may involve electronic evidence, not only a few specialized officers need to be trained, but more or less all law enforcement officers, prosecutors and judges.

If criminal justice systems are to deal effectively with the problems relating to the repression of cybercrime, they must update their legislation and law enforcement systems where these are unable to cope with investigation and prosecution of the phenomenon. The 2005 European Union Framework Decision on attacks against information systems (FD) Council of Europe, 2001; European Union, 2005) and the 2001 Council of Europe Convention on Cybercrime (CoE Convention) , seek to resolve these issues.

One major consequence of the virtual nature of many cybercrimes is that inconsistencies among criminal justice systems may hamper repression of the phenomenon. The perpetrator may be in a different jurisdiction from the victim, and the legal definitions of the criminal behavior in the two legal systems may not match. Numerous difficulties may arise from this very simple situation. The country in which the perpetrator is present may not consider the conduct to be an offence. It may criminalize it, but as a minor offence punished with less than the minimum sanctions for international cooperation.

Even if the penalty requirements for cooperation are present, this may not be possible because the offences do not fulfill the double criminality requirement. Especially for cybercrime, an excessively lenient criminal legislation or significant inconsistencies among national regulations may have detrimental effects. Criminals may fully exploit ICT and the virtual environment of the internet and focus their activities on the most tolerant legal systems and on the most vulnerable victims.

One solution in order to solve and prevent these problems is overcoming the frictions among national legislations dealing with cybercrime. The convergence of legislations among European (and other) countries may offer a technical solution to many difficulties related to the current framework of international cooperation.

In this perspective, both the CoE Convention and the FD contain criminalization requirements. Both instruments share a common core constituted by three criminal offences concerning the confidentiality, integrity and availability of computer data and systems. The first is the illegal access (Art. 2 of the CoE Convention and Art. 2 of the FD) consisting of intentionally accessing a computer system without the right to do so. Both agreements allow states to require the infringement of a security measure and exclude minor cases. These options should grant some flexibility to national legal systems. They also take into account the trade-off between over-criminalization (thus seeking to punish all illegal accesses) and the specific selection of criminal illegal accesses (thus stimulating citizens to protect computer data and systems).

Critics have argued that this may hinder achievement of the objective of harmonizing national laws. Further, scholars suggest that the requirement of the infringement of a security measure is probably the most sensible and efficient approach to the criminalization of illegal access. The possibility of limiting the scope of the criminalization of

illegal access provided by the CoE Convention and the FD could hinder international cooperation for those countries that chose to have broader illegal access offences.

However, in the long term these problems may end up by incentivizing countries to restrict illegal access offences, so that they adhere to the most efficient models envisaged by scientific research.

The CoE Convention covers several types of cybercrime, such as illegal interception, misuse of devices, computer-related offences (forgery and fraud) and content-related offences (child pornography, infringements of copyright and related rights).

The FD instead provides for the criminalization of instigation, aiding and abetting and attempt to commit one of the three offences described above. It requires a minimum penalty of at least between one and three years of maximum imprisonment for illegal system interference and illegal data interference. It provides for aggravating circumstances (at least between two and five years of maximum imprisonment) for offences committed within the framework of a criminal organization or offences —that caused serious damages or has affected essential interests. The European action against cybercrime is not limited to criminalization. It also introduces new investigative powers for the law enforcement agencies.

Articles 14-21 of the CoE Convention require the Parties to introduce new investigative powers. The main consideration in this regard is that the new procedural rules have a broad application. They apply not only to offences envisaged by the first section of the agreement, but also to —other criminal offences committed by means of a computer systemll (Article 14, para 2 b), and even to the —collection of evidence in electronic formll for any crime (Article 14 para 2 c). Hence, the measures of this section significantly affect the criminal procedure systems of the Parties. States must adopt laws allowing the activities stated by the CoE Convention, unless their national legislation already complies with it. The scope of application of these measures demonstrates that the need to modernize investigative tools extends beyond the fight against cybercrime.

The first investigative measure set out by the CoE Convention is the expedited preservation of stored computer data. It enables the authorities to order or obtain the preservation of specific digital information already stored. It allows the freezing for up to ninety days of a defined quantity of data of possible relevance to a criminal investigation in order to prevent its deletion and alteration.

The second measure is the ‗production order'. This may oblige a) a person to submit specified stored information in his/her possession or control and b) a service provider to disclose subscriber information in the provider's possession or control. Subscriber information comprises the type of communication used, technical provisions, period of service (Art. 18, para 3 a), and other information available to the provider on the basis of the contract or agreement with the user (identity, address, contacts, payment information, etc.) The third measure concerns the search and seizure of stored computer data. It allows the authorities to search a computer or other data storage device. Article 19, paragraph 2, also allows for the automatic extension of the search to data stored in other computers accessible from the one being searched.

The fourth and fifth measures concern the real-time collection of computer data. Article 20 deals with traffic data and Article 21 with content data. These norms allow the authorities to intercept and/or order a service provider to assist them, or even to collect traffic data and content data directly. These measures provide for the interception of personal communication, a significant interference with the right to privacy and the right to communicate. They should apply only for serious crimes.

Article 21 leaves to domestic law to select such offences. This is a mandatory selection for collection of the content of communications. The above described measures provide law enforcement authorities with a valuable ICT toolbox of investigative measures. Article 15 provides guarantees for privacy and freedoms. This provision cites the protection of human rights and liberties and expressly requires that investigative powers respect the proportionality principle (Council of Europe, 2001).

The CoE Convention also includes several norms intended to facilitate international cooperation and to improve the repression of transnational cybercrime. Notwithstanding criticisms and problems of implementation (discussed below), the part of the CoE Convention on international cooperation is the core of the new treaty. It is widely viewed as the most important element because it enables expeditious actions in a sector where these are necessary, owing to the speed and changeability of cybercrime. Several provisions deal with mutual legal assistance. These concern not only the investigation and prosecution of crimes related to computer systems and data, but also the collection of evidence in digital form. These provisions are thus likely to apply to a wide variety of criminal proceedings dealing with cybercrimes and ordinary crimes (Council of Europe, 2001).

The CoE Convention has a subsidiary function. On the one hand, it provides a framework for mutual assistance when no other agreement exists between the requesting and requested Parties. States must designate a central

authority responsible for such requests. National authorities must execute the requests according to procedures specified by the requesting Party.8 In cases of urgency, the requesting Party can sent requests directly to judicial authorities. The competent authorities are free to directly exchange requests not involving coercive action. On the other hand, other applicable treaties and national laws should have the priority (Article 27 of the CoE Convention). This allows mutual legal assistance operators to use more familiar instruments, such as, for example, the European Convention on Mutual Assistance in Criminal Matters and its Protocol or the EU Convention on Mutual Assistance in Criminal Matters. This rule is only a general principle and has several exceptions. In particular, Parties shall implement to the full extent the provisions on mutual assistance for the specific investigative actions provided by the CoE Convention.

3. Conclusions

Cybercrime poses important challenges to the European criminal justice systems. The above-described approach is a significant endeavor to improve the European (and international) repression of cybercrime. Firstly, it introduces new tools for investigation of these crimes. Secondly, it harmonizes the national definitions of several computer-related offences. Thirdly, it provides a minimum framework for international cooperation on criminal matters. The legal framework provided by the CoE Convention has been generally considered a significant step forward in the international response to cybercrime.

As highlighted above, the European and international legal framework set by the CoE Convention and the FD has not been exempt from criticisms. Some of such criticisms may have been due to a misunderstanding of the general functioning of international cooperation in criminal matters or important concern for human rights and freedoms. However, the effectiveness and actual implementation of these international instruments remain the most critical issues. Indeed, their legal implementation shows some difficulties. However, the indirect implementation of these appears to be more successful. This supports the idea that non legal issues such as national security, politics, the economy and public opinion are more important factors than the legal enforceability in the implementation of these international instruments. Until present, the added value of the EU action in this sector appears relatively low. The Treaty of Lisbon and the Stockholm Programme may improve this situation, but this should not be expected to happen in the short period.

In conclusion, the CoE and the FD constitute an important *corpus* of international law aimed at improving European and international cooperation against cybercrime. Notwithstanding the criticisms, they still appear as important achievements. However, their entry into force is only the first step towards their effective implementation, which is likely to be complex and will probably raise further issues.

References

Brenner, Susan W., and Leo L. Clarke. 2005. Distributed Security: Preventing Cybercrime. John Marshall Journal of Computer & Information Law, 23, no. 4: 659-709.

Calderoni, Francesco. 2008. A Definition that Could not Work: The EU Framework Decision on the Fight against Organised Crime. European Journal of Crime, Criminal Law and Criminal Justice, 16: 265-82.

Calderoni, Francesco. 2010. Organized crime legislation in the European Union. Heidelberg: Springer.

Chaikin, David. 2006. Network investigations of cyber attacks: The limits of digital evidence. Crime, Law and Social Change, 46, no. 4-5: 239-56.

Council of Europe. 2001. Convention on Cybercrime: Explanatory Report. http://conventions.coe.int /Treaty /en/Reports/Html/185.htm.

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems : Explanatory Report. Council of Europe. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.2005.

Organised Crime in Europe: The Threat of Cybercrime., Situation Report 2004. Strasbourg: Council of Europe Publishing. Council of the European Union. 2007. Doc. 9913/07 of 25 May 2007.

European Commission. 2008. Report from the Commission to the Council based on Article 12 of the council Framework Decision of 24 February 2005 on attacks against information systems. COM(2008) 448 final, Brussels, 14.07.2008.

European Union. 2001. Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, OJ C 187 of 3.7.2001.

Agence Nationale de la Sécurité des Systems d'Information [France] (2011): Défense et securité des systems d'information – Stratégie de la France, http://www.ssi.gouv.fr/IMG/pdf/2011-02- 15_ Defense_ et_securite_des_ systemes_d_information_strategie_de_la_France.pdf.

Council of Europe/Global Project on Cybercrime (2009): Cybercrime training for judges and prosecutors: a concept

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_ 4_provisional_8oct09.pdf.
Council of Europe/Octopus Programme (2008): Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, http://www.coe.int/t/dghl/ cooperation/economiccrime /cybercrime /Documents/LEA_ISP/default_en.asp.
European Union (2008): Council conclusions on a concerted work strategy and practical measures against cybercrime, http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf.
Estonian Ministry of Defence (2008): Cyber Security Strategy, http://www.eata.ee/wp-content /uploads /2009/11 /Estonian_ Cyber_Security_Strategy.pdf.