Combating Cybercrime – Developments in the European Union

Erik O. Wennerström
Csaba Sandberg

1 Introduction ……..…… 248

2 The Council of Europe *acquis* ……..……... 249
2.1 Introduction ……..… 249
2.2 Implementation of the Cybercrime Convention - a Decade Later ... 252
2.2.1 The additional protocol concerning racism and xenophobia 253
2.2.2 Current state of play of signatories and ratifications …..…. 253
2.2.3 Promotional projects by the Council of Europe ……..….. 254
2.3 Concluding Remarks on the Cybercrime Convention's ……..….. 255

3 The EU Approach ……..…….. 255
3.1 Introduction and background to the EU approach ……... 255
3.2 Combating Traditional Forms of Crime in an On-Line Environment ……..……... 258
3.2.1 Framework decision on combating fraud and counterfeiting of non-cash means of payment ……. 258
3.2.2 The Directive on the Prevention of the Use of Financial Systems for Money Laundering and the Directive on Payment Services in the Internal Market ……..…… 261
3.2.3 Action plans preventing fraud of non-cash means of payment ……..….. 262
3.3 Publication of Illegal Content …….……. 263
3.3.1 The Framework decision on combating the sexual exploitation of children and child pornography ……..….. 264
3.3.2 Framework decision on combating racism and xenophobia 266
3.4 Crimes Unique to Electronic Networks …….…….. 267
3.4.1 Framework decision on attacks against information systems …….……... 267
3.4.2 Other efforts by the European Commission ……..… 270
3.4.3 Offenses related to infringements of intellectual property rights ……..... 272
3.5 Enabling Law Enforcement to Combat Cybercrime ……..….. 272
3.5.1 Directive on traffic data retention ……..….... 273

4 Way Ahead – Challenges for the EU 275
4.1 General Challenges …….…….…… 275
4.2 Legislative and Legal Challenges – Lisbon and the Stockholm Programme …….…….. 277

5 Conclusions ……..……..……..……..…..…..……..……. 281

1 Introduction

More's law states that the number of transistors on an integrated circuit board doubles every two years.[1] This law has held its premises since the early seventies and curiously enough seems to be a rather accurate prediction for the emergence of new computer based threats as well. The past decade has been characterized by an exponential growth in people using devices connected to the Internet, creating a golden opportunity for criminals. While it is nothing new that law-makers are constantly lagging behind new forms of crime, it is historically unparalleled how fast criminals have followed new trends in the border-less, constantly on-line parts of western society that embrace almost all aspects of the physical society.

While politicians and legislators evaluate the efficiency of legislation against on-line fraud, criminals are tricking people into giving them their on-line banking details with more and more sophistication. As governments struggle to establish 24/7 information exchange networks for law enforcement agencies, criminals are using on-line technology to communicate with each other in virtually untraceable ways. States have for the past decade met at conferences to define how traditional international norms on "armed attacks" relate to the Internet, while criminals have incessantly launched large scale attacks, crippling public services in countries. The challenge is staggering.

It would not, however, be fair to state that there has been no development in the legal field regarding cybercrime in the past decade. The Council of Europe's Convention on Cybercrime CETS No.: 185 (referred to as the Cybercrime Convention), which was opened for signature in November 2001 and came into force in July 2004, was the first thorough attempt to harmonize cybercrime legislation internationally. The European Union followed suit but instead of one set of all-encompassing legislation, such as the text of the Cybercrime Convention, the EU approach was characterized by thematically smaller legislative acts, recommendations and action plans. Most available types of instruments in the European Union were used to harmonize legislation across the Member States and to create an EU-wide approach to fighting cybercrime.

The purpose of this article is to provide an overview of the legislative developments in the European Union in the past decade regarding the combating of cybercrime. Since the Council of Europe's Cybercrime Convention has been signed by all Member States and has been the foremost influence on the EU's legislative efforts in this field, the article will commence by a brief outline of the Convention and its implementation. The article will then explore the EU's approach to combating cybercrime, examining legislative acts and other forms of institutional efforts regarding the combating of cybercrime. It will outline not only the legislative text but also exemplify their relevance (and/or shortcomings) with regard to the development in the techniques used by cyber-criminals today. The categorization of the EU's approach to cybercrime, used in the article, follows the European commission's categorization of cybercrime, namely: traditional forms of crime, publication of illegal content and crimes unique to

1 *See* "en.wikipedia.org/wiki/Moore's_law".

electronic networks. The article will conclude with a discussion on the political and legislative challenges facing the EU in the coming decade.

2 The Council of Europe *acquis*

2.1 Introduction

Following long and intense negotiations, the Council of Europe succeeded in establishing a convention on "crimes in cyberspace", marked by the signing of the Convention on Cybercrime on 8 November 2001 by close to 30 states.[2] The Convention establishes common definitions of crimes in the cyber environment, as well as judicial co-operation facilities between the participating states to improve their fight against cybercrime. The Convention on Cybercrime entered into force following its ratification on 18 March 2004 by Lithuania, thereby reaching five ratifications, which was the requirement for the Convention to enter into force.[3]

The first part of the convention requires the Contracting States to ensure the criminalization of substantive offenses described in Articles 2 – 10 complemented by rules on attempt, aiding and abetting, as well as rules on the liability of legal persons. The first category of such provisions, in Articles 2 – 6, cover crimes against the confidentiality, integrity and accessibility of data and systems or *computer-crimes* (i.e. environmentally unique crime types). This part defines illegal access, illegal interception, illegal damaging and alteration of data, system entry as well as illegal use of certain types of equipment. Article 2 describes the crime of illegally accessing a computer system, in whole or in part. ("In whole or part" is a necessary qualification, as a "computer system", in accordance with the definitions set out in Article 1, is *any* equipment used to treat data automatically.) While Article 3 criminalizes illegal or unauthorized interception of non-public transmissions of computer data, it is worth noting that Article 4 covers the deletion, alteration and suppression of data – a crime referred to as data interference – referring i.a. to situations where data is made inaccessible to those authorized to access it. Such situations frequently occur when hackers alter the privileges or authorization levels of computer files. As the article covers alteration of data, most forms of malicious computer viruses will also be covered by it.[4]

Article 5 criminalizes serious system interference, resulting in hindering a system from performing the functions it was designed to perform. In order for

2 All the then 43 Council of Europe Member States participated in the negotiations, together with Canada, Japan, South Africa and the United States. For a fuller description, *See* Wennerström, E., *EU-legislation and Cybercrime – A Decade of European Legal Developments*, in Scandinavian Studies in Law, Vol. 47, Stockholm 2004 (in the following "Wennerström 2004"), pp. 452-456.

3 The negotiations were based on a process leading back to a series of recommendations adopted by the Committee of Ministers of the Council of Europe – Recommendations No. R (85) 10, R (87) 15, R (88) 2, R (89) 9 and R (95) 13 – as well as to Resolutions 1 (97) and 23 (00) adopted by the European Ministers of Justice.

4 *See Convention on Cybercrime* (ETS no. 185), *Explanatory Report*, p. 61.

the interference to be criminal, it must be the result of some form of data manipulation, not mere accident. Unsolicited e-mail advertisement or spam, cannot be seen as such interferences *per se*, but the distribution of spam may ultimately result in a system (or server) being overloaded, leading to its malfunctioning. In that situation, it may be argued that a system interference has taken place (based upon a *culpa eventualis*-evaluation – the perpetrator had no direct criminal intent, but realized the risk of his behavior and ignored the risk) with results identical to that of a deliberate denial-of-service attack, i.e. the intentional overloading of a system in order to make it malfunction.[5] Article 6 criminalizes the misuse of devices, a concept directly imported from the US Federal Criminal Code, Section 1029 "Fraud and related activity in connection with access devices".[6] Paragraph 1 of Article 6 criminalizes the production and dissemination of devices, mainly designed to commit the crimes outlined in Articles 2 – 5. This includes the dissemination of passwords and other tools to gain unauthorized access to computer systems, provided there is criminal intent on the part of the perpetrator. Possession of such devices is likewise criminalized, provided there is intent to commit one of the listed offenses demonstrated.

As regards *computer-related crimes* (i.e. traditional crime types adapted to the IT environment) the convention defines computer-related fraud and forgery in Articles 7 and 8. Although most States already have criminalized the crimes of fraud and forgery as such, these provisions require States to examine their laws to ensure that they apply to IT-situations. Computer-related forgery and fraud are two specific kinds of manipulation of computer systems or data, and the provisions serve to acknowledge the fact that traditional legal provisions are not always suitably adapted or neutral enough to cover new forms of manipulations.

The Convention also covers some *content-related crimes* and requires States to criminalize i.a. distribution, production and possession of child pornography through the use of computer systems, according to Article 9.[7] This provision criminalizes several aspects of child pornography, which in its offline-form already was criminalized in most States.[8] Originally racism and xenophobia was also covered by the Convention's provisions on content-related crimes, but during the finalizing stages of the negotiations it became clear that it would not be possible for some of the negotiating states to agree upon a text that basically criminalized what their constitutional guarantees for freedom of expression were

5 Id. p. 69. *See* also Wennerström, E., *Europeiskt arbete mot IT-brottslighet*, in Europarättslig Tidskrfit, 2001 (in the following "Wennerström 2001"), p. 480.

6 *Cf.* 18USC1029; *See* U.S. Code Online via GPO Access, "www.access.gpo.gov/UScode/title18/parti_chapter47_.html".

7 This article was later the model for its counterpart in EU legislation, *See* below under 3.

8 The aspects covered are a) the production of child pornography for the purpose of distribution through a computer system, b) the 'offering' and making available of child pornography through a computer system, c) the distribution or transmission of child pornography through a computer system, d) the 'procuring for oneself or for another' of child pornography, i.e. actively obtaining it through e.g. downloading, and e) the possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom.

safeguarding. (These provisions were later brought into the Protocol to the Convention; see below.) Finally we also find among the criminal law definitions infringements of copyright and other intellectual property rights, in Article 10, which states are required to criminalize.

States are required to criminalize these acts through the introduction of penal law sanctions that include custodial penalties. Before it is possible to say whether these provisions actually create a finely woven web of substantive criminal law over the ratifying states, it is necessary to see how the ratifying states implement them in their national laws. The states are given room to maneuver in the implementation, as a result of the compromises that lay behind the ultimately adopted text.[9] Article 11 (3) may serve as an example of how much is still at stake, as it makes the obligation to criminalize the attempt to commit the crimes described in Article 2 – 10 optional for the ratifying states. This may lead to ulterior difficulties regarding i.a. the requirements for dual criminality.

The convention contains *rules on criminal procedure* such as coercive measures to facilitate investigations of the crimes described above, through a combination of "old" and "new" procedural measures. One such new measure is the "rapid freezing" of data (including traffic data; see below) i.e. an authority with relevant competence shall have the right to order data concerning a crime or a criminal to be stored with an Internet Service Provider (ISP, i.e. a company providing access to internet, e-mail services etc.) in order for it to be deliverable to the investigating authority upon a subsequent formal request for its release. This measure may remain in place for a maximum of 90 days, according to Articles 16-17. Traditional possibilities for search and seizure in order to obtain stored data are provided for in Article 19. Authorities shall have the possibility to secure seized data and to make it inaccessible for unauthorized persons.[10]

Although stopping short of requirements concerning historical traffic data (this later presented the EU with a legislative challenge that is still being implemented; see below on retention of traffic data) the Convention provides that data shall be presented to the law enforcement authorities at their legally authorized request, in order to identify the operators and the route that particular data has taken in transmission. It shall also be possible for authorities to order an ISP to reveal information on its user/client accounts. The Convention stipulates that it shall be possible for authorities to collect traffic data in real time – again: not going back in time, but from a point in time and forwards – that is related to certain data communications and ISP's may be ordered to assist authorities in relation to such measures. Just like in the offline situation, it shall be possible for authorities to use telecommunications-interception in real time while investigating serious crimes (Articles 20 and 21). These measures may only be taken under special conditions such as authorization by a judge or another independent authority, subject to the rules on human rights and proportionality in the Signatory States.

9 *See* Wennerström 2001 p. 483.

10 *See Convention on Cybercrime* (ETS no. 185), *Explanatory Report*, pp. 200-202.

The Convention's rules on international co-operation aim at making the procedural rules described above enforceable transnationally, by providing possibilities for law enforcement authorities in one country to seize computer-based evidence on behalf of the authorities in another country (Article 31) swiftly and in a less formalized manner in urgent cases (Article 29). The assistance may consist in freezing and seizing certain data in another state that is relevant to an investigation. Central authorities shall be appointed for sending and receiving requests for such assistance, but it shall in urgent cases be possible for authorities to communicate directly with each other. Requests may be refused only under certain circumstances and certain user limitations may come into play as a result of states' rules on data protection. Apart from this, spontaneous and voluntary exchange of information is foreseen.

Pending a formal request for assistance, states shall freeze stored data on request, for at least 60 days. The grounds for refusal are limited. States naturally have the right to access publicly available information without the permission of other states, even if such data is hosted on servers located on another state's territory. On request states shall assist each other with real time collection of targeted traffic data (Article 33) – "targeted" as opposed to "fishing expeditions" where i.a. all traffic data generated at a particular server is monitored indiscriminately – for all crimes falling under the convention, in accordance with the conditions and procedures described in national law. States shall furthermore assist each other with interception of telecommunications as far as is possible with regard to existing treaties and national law, Article 34.

The crimes described in the convention should be able to lead to extradition, according to Article 24, provided that the crimes are punishable with imprisonment of one year or more, with certain exceptions, and that requirements of dual criminality, where applicable, are satisfied. In order to provide support to ongoing investigations, a network of contact points is created, available 24 hours a day, seven days a week, as outlined in Article 35. This network is modeled on the G8-network[11] and in reality means that the G8-network is expanded to all ratifying States of the Council of Europe convention.[12]

2.2 Implementation of the Cybercrime Convention - a Decade Later

It has passed over eight years, almost a decade, since the initial opening for signatures of the Convention (23/11/2001) and it is indeed interesting to reflect

11 The Group of Eight (G8), and formerly the G6 or Group of Six and also the G7 or Group of Seven is a forum, created by France in 1975, for the governments of the six most industrialized countries in the world: France, Germany, Italy, Japan, the United Kingdom, and the United States. In 1976 Canada joined the group (thus creating the G7). In becoming the G8, the group added Russia in 1997. In addition, the European Union is represented within the G8, but cannot hoast a chair. In 1997 a G8 subgroup on High-tech Crime was created. One of its most significant achievements is the creation of the "24/7 Network", which allows law enforcement in the participating countries to reach out "24 hours a day, 7 days a week" to counterparts in other countries for rapid assistance in investigation computer crime and preserving electronic evidence. This network has grown beyond the G8 countries and today encompasses more than 50 countries.

12 *See Convention on Cybercrime* (ETS no. 185), *Explanatory Report*, p. 298.

on what has happened since then. Following the successful conclusions of the negotiations on the Convention, the negotiation teams continued their work on the content-related crime that had been lifted out of the mother Convention: racism and xenophobia. The "*Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*" was adopted by the Council of Europe Committee of Ministers on 7 November 2002. The Protocol was opened for signatures on 28 January 2003 and entered into force is 1 March 2006.

2.2.1 The additional protocol concerning racism and xenophobia

The Protocol requires states to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults. Article 6, Section 1 of the Protocol specifically covers the denial of the Holocaust and other genocides recognized as such by other international courts set up since 1945 by relevant international legal instruments.[13] Section 2 of Article 6 allows Parties to the Protocol at their discretion only to prosecute if the offense is committed with the intent to incite hatred, discrimination or violence; or to make use of a reservation, by allowing a Party not to apply – in whole or in part – Article 6.

2.2.2 Current state of play of signatories and ratifications

The Convention itself entered into force on 1st of July 2004 after it was ratified by five nations including three Council of Europe Member States. To date, forty two out of the forty-seven Member States of the Council of Europe have signed the Convention.[14] The following EU Member States have signed and ratified the Convention: Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Portugal, Romania, Slovakia, and Slovenia. The following EU Member States have only signed the Convention: Austria, Belgium, Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Spain, Sweden, and the United Kingdom.[15] It is interesting to note that more than a third of the 27 EU Member States have not ratified the Convention and that amongst the Nordic and Scandinavian countries, it is only Sweden that has not ratified the Convention, although all countries have signed it.

Only thirty-three Member States of the Council of Europe have signed the Additional Protocol since it opened up for signatures in January 2003. Several EU Member States have not signed the Additional Protocol. Out of the Non-Member States of the Council of Europe only Canada and South Africa have

13 *See* the *Explanatory Report of the Protocol* , which refers to the ECtHR *Lehideux & Isorni* judgment of 23 September 1998.

14 Andorra, Monaco, Russia, San Marino and Turkey are members of the Council of Europe but have not signed the Convention. Out of the Member States who have signed the Convention, 18 have ratified it into national legislation. An additional four of the Non-member States of the Council of Europe (Canada, Japan, South Africa and the United States) have signed the treaty and the United States ratified it 29/9/2006.

15 *See* the Council of Europe Treaty Database, at 24th of April 2010, "conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG".

signed the Protocol. The following EU Member States have signed and ratified the Protocol: Cyprus, Denmark, France, Latvia, Lithuania, Portugal, Romania, and Slovenia. The following EU Member States have only signed the Protocol: Austria, Belgium, Estonia, Finland, Germany, Greece, Luxembourg, Malta, Netherlands, Poland, and Sweden.[16] In contrast to the Cybercrime Convention, there are several EU Member States who have not even signed the Additional Protocol to the Convention – Bulgaria, Czech Republic, Hungary, Ireland, Italy, Slovakia, Spain, and the United Kingdom – and only less then a third of the Member States have ratified the Additional Protocol.

Some explanations regarding why not all EU Member States have signed and/or ratified the Convention or the Additional Protocol can be found in internal EU mechanisms. First of all, reference should be made to the dynamics of EU enlargement. When the Cybercrime Convention was opened up for signatures, the ten Central and Eastern European countries that were candidates for EU membership were still very much in their accession negotiations. The Cybercrime Convention was rapidly included into the *acquis* or legislative package of international and European norms that they had to demonstrate their willingness to incorporate nationally, in order to meet the requirements for EU membership. All of the candidate states signed the conventions, and the degree of ratification is higher among them than among the "older" 15 Member States[17], that were under no such pressure. The same pattern can be observed with regard to the Protocol on Racism and Xenophobia.[18]

The second internal EU factor that to some extent explains the slowing down of the roll-out of the Cybercrime Convention, can be attributed to the negotiations and adoption in February 2005 of the EU *Framework Decision on attacks against information systems* and the EU *Framework Decision on Racism and Xenophobia* of November 2008. Once these instruments were available, there were legislative obligations of a more *contraignant* nature inside the EU that covered the same legislative areas as the two Council of Europe instruments. The added value of ratification of the Council of Europe instruments quickly diminished for EU Member States.

2.2.3 Promotional projects by the Council of Europe

The Council of Europe launched a project in September 2006 in order to promote the implementation of the Convention and its Protocol on Xenophobia and Racism. The project was completed in February of 2009 and during this time, over 100 activities were carried out all over the world with various stake-holders and actors. The activities included, for example, legislative reviews, workshops and global conferences. Although "only" about fifty nations have signed the Convention, there are over 100 countries around the world that either have cybercrime legislation in place, or are in the process of putting such

16 *See* "conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG".

17 *See* "conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG".

18 *See* "conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG ".

legislation in place, thanks to the Convention and the promotion project. The Convention has thus become a global reference with regards to cybercrime legislation. The project has also prepared guidelines for law-enforcement, promoted the training of judges and prosecutors, the establishment of 24/7 points of contact (by February 2009, all parties except the Ukraine had one) and strengthened multi-stakeholder cooperation.[19]

A second phase of the project commenced in March 2009 continuing along the lines of Phase one, namely promoting the broad implementation of the Convention and its Protocol. Conferences, workshops, training for judges and prosecutors, legislative reviews, continuing the strengthening of the 24/7 contact points were carried out on local, regional and global levels. In addition to the mentioned project regular consultations of the signatories of the Convention meet at least once per year as the Cybercrime Convention Committee for consulting on various topics and issues regarding the Convention and the implementation of the convention.[20]

2.3 Concluding Remarks on the Cybercrime Convention's

As is the case with all conventions, their weakness lies in the need for ratification, a process that can be time consuming and uncertain – even positive ratifications can be combined with reservations towards certain parts of the agreed text. This weakness that is even more evident when compared with EU-instruments (Framework Decisions, Council Decisions, and Directives) that enter into force upon their adoption. Nevertheless, the Council of Europe has created an instrument with broad coverage, legally – covering substantive criminal law, procedural law as well as international co-operation – as well as geographically, which is its main advantage. It was also the first of its kind and has through this status exerted extensive influence, well beyond the Member States of the Council of Europe, well before it entered into force. Even before the text of the Convention had been agreed upon in 2001, its influence could be discerned on national, regional and international negotiations and discussions on cybercrime, which demonstrates its unique nature at the time of adoption, and the high technical quality of its provisions.[21]

3 The EU approach

3.1 Introduction and background to the EU approach

Efforts by the European Union to tackle cybercrime date back to the end of the 1990's. In April 1998, the Commission presented the results of a study on computer related crime (the so-called 'COMCRIME' study). In October 1999,

19 *See* Project on Cybercrime Final Report, September 2006 – February 2009, Council of Europe, Strasbourg, 14 May 2009, ECD/567(2009)1.

20 *See* "www.coe.int/t/DGHL/STANDARDSETTING/T-CY/default_en.asp".

21 *See* e.g. references to the Convention in the explanatory memorandum to the Commission's proposal for a Council Framework Decision on attacks against information systems, COM (2002) 173 final, 19.04.2002.

the Tampere Summit of the European Council concluded that high-tech crime should be included in the efforts to agree on common definitions and sanctions. The Commission launched the *eEurope initiative* in December 1999 in order to ensure that Europe can reap the benefits of digital technologies and of the emerging information society. In June 2000, The Feira European Council adopted a comprehensive *eEurope Action Plan* which highlighted the importance of network security and the fight against cybercrime.[22]

The Commission issued a Communication to the Council and the European Parliament in January 2001, on *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (referred to as the Cybercrime Communication)[23] which has framed the EU's approach to tackling cybercrime during the past decade. It contains policy proposals as well as indications on planned legislative proposals from the Commission. The Commission concluded that there was a need for EU-legislation leading to:

- approximation of Member States' penal legislation on child pornography,
- further approximation concerning crimes against system integrity [e.g. hacking], racism and xenophobia and drugs trafficking via the Internet,
- mutual recognition of judicial decisions, covering measures such as search and seizure,
- evaluation of the need for a special initiative on traffic data retention.

The Commission also called for the establishment of an EU forum where all affected stakeholders could exchange experiences, encourage research programs, promote training of relevant staff and for the support of a database on legal developments in Member States in this field.[24]

The extent to which the Cybercrime Communication influenced the EU's approach in dealing with cybercrime is exemplified by the fact that:

- the general competence of EUROJUST includes the following of "computer crime",[25]
- the European Arrest Warrants can be used in situations relating to "computer-related crime",[26]

22 *See* the Commission's Communication COM(2000) 890 final of 26.01.2001 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, p. 2.

23 Idem.

24 *See* COM(2000) 890 final, p.2.

25 *See* Council Decision (2002/187/JHA) of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Article 4 (1b).

- the expression "computer crime" is listed as one of the forms of serious international crime of which Europol is competent to deal with,[27]
- the European Network and Information Security Agency (ENISA) was established in 2004.[28]

Since then, there have been several legislative developments in the EU with regard to harmonizing Member State's legislation covering cybercrime. As stated above, there is no EU version of the Cybercrime Convention that covers *all* aspects of cybercrime. The different provisions of the Cybercrime Convention can be found spread out over different EU instruments. Although there is seldom absolute synchronization and demarcation between the different EU instruments, there are several re-occurring sections that point to the fact that the EU legislative bodies do act in one strategic direction, albeit on different fronts, to overcome the legislative problems around cybercrime. Thus, almost every relevant EU instrument has a section extending liability for the criminal offense of respective legislative act to legal persons (ensuring that criminals can not escape punishment by carrying out offenses through a company). There is also, with few exceptions, provisions dealing with jurisdictional aspects of the crime regulated, ensuring that criminals can not escape prosecution by exploiting the border-less aspects of the Internet.

This section will examine these legislative instruments using the categorization of cybercrime used by the Commission: traditional forms of crime (such as fraud or forgery in an on-line context), publication of illegal content (such as sexual abuse material or incitement to racial hatred in an on-line context) and crimes unique to electronic networks (such as hacking or denial of service attacks).[29]

---

26 *See* Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, Article 2(2).

27 *See* Europol Convention, consolidated version, p. 44, at "www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf". In addition to the regular activities of Europol, the EU Council of Ministers approved in late 2008 a proposal to establish a centre to fight cyber crime within Europol. Its tasks are to serve as an EU-wide platform for collecting information on cyber crime and child pornography. In their conclusion, government representatives called upon the European police authority to focus in particular on combining and analysing data in member states' existing or planned internet crime reporting centres. The ministers envision the second step as an exchange of incoming reports between the national platforms. Futhermore, the police office in The Hague will set up a website to explain typical forms of internet crime to web surfers, list walk-in centres, publish statistics on collected information, and keep the European Council up to date the centre's activities. Following an expansion of its mandate in 2007, Europol already has a mandate fighting cyber crime and, in the framework of the Check the Web project, combing the web in search of terrorist activity.

28 *See* Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

29 *See* the Commission Communication COM(2007) 267 final of 22 May 2007 *Towards a general policy on the fight against cyber crime*, p. 5.

3.2 Combating Traditional Forms of Crime in an On-Line Environment

In a legal context "traditional forms" of cybercrime[30] are usually considered to be fraud and forgery committed with the help of computers and the Internet or directly on the Internet. However, in elaborate criminal situations, it is sometimes difficult to draw the line between computer-related and computer-based criminal activities. Very often both forms are present in a criminal offense and legislation needs to cover all levels and modes of criminal activity in order to be effective. Although the Member States of the EU and the Commission were involved in the early cybercrime legislative attempts it may only have been natural that the EU chose to legislate first in the field of computer-*related* offenses, as this implies an extension of previously existing criminal law mechanisms and provisions to a new area of criminal methodology, rather than the creation of criminal law provisions with little or no resemblance to previous criminal law.

3.2.1 Framework decision on combating fraud and counterfeiting of non-cash means of payment

Although the initial intention may have been to combat credit card fraud, the protective value of the *Framework Decision on combating fraud and counterfeiting of non-cash means of payment*[31] goes a lot further than just criminalizing the skimming of credit cards and photo-copying of travelers cheques. The Council of the European Union adopted the Framework Decision with the objective to ensure that fraud and counterfeiting involving *all* forms of non-cash payments are subject to effective, proportionate and dissuasive sanctions across the EU Member States in order to combat individual criminal acts and organized crime (Preamble 4). The development of the Internet and the extent of online-payment systems and Internet banking that exist today may or may not have been envisaged in 2001, but the Framework Decision does indeed encompass many of the on-line fraud scenarios that occur currently.

The Framework Decision defines payment instruments as corporeal instruments, other than physical money, enabling the holder to transfer money or monetary value. Examples of payment instruments under the definition include i.a. credit cards, travelers' cheques, and bills of exchange. Aimed at preventing abuse carried out by legal persons as well, the Framework Decision defines legal persons as: "any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organizations."[32]

Using credit cards as an example of a payment instrument, Article 2 not only calls for the criminalization of the act of stealing credit cards but also for the act of falsifying credit cards. It, furthermore, criminalizes the selling of, handling of

30 Also known as computer-related offenses as defined in Section 1, Title 2 in the Cybercrime Convention. *See* above, section 2.

31 *See* Council *Framework Decision (2001/413/JHA) on combating fraud and counterfeiting of non-cash means of payment* of 28 May 2001.

32 *See* Council *Framework Decision (2001/413/JHA) on combating fraud and counterfeiting of non-cash means of payment* of 28 May 2001, Article 1.

and the possession of stolen or counterfeited credit cards if intended to be used fraudulently. The Framework Decision also calls on Member States to criminalize any fraudulent use of stolen or counterfeited credit cards thus ensuring that participation in and instigation of the above mentioned conducts are punishable with deprivation of liberty and that they can lead to extradition.[33]

Article 3 of the Framework Decision deals with offenses related to computers. The Article calls for the criminalization of situations where someone, fraudulently and without right, alters computer data or interferes with the functioning of a computer program or system during a money transfer causing loss for someone else while procuring economic benefits for the perpetrator. Article 4 calls for the criminalization of making, selling, receiving and possessing instruments, articles or computer programs that can be used to counterfeit payment instruments or computer programs which have the purpose of carrying out the computer related offenses described in Article 3.

As mentioned, the Framework Decision also aims at extending criminal liability in such situations to legal persons. Thus, legal persons are to be liable for crimes committed, for benefit, by persons in leading positions in the organization. The liabilities include crimes defined in Article 2(b), (c) and (d) and Articles 3 and 4, including:

- counterfeiting of payment instruments
- obtaining and selling of, along with possession of, stolen or counterfeited payment instruments
- fraudulent use of stolen or counterfeited payment instruments
- altering computer data or using computer programs to gain monetary benefits
- making, selling or possessing instruments or computer programs to carry out such crimes.

The Framework Decision calls on Member States to ensure that legal persons are liable in situations where the lack of supervision or control by a person in charge has made possible the carrying out of the named offenses. It also clarifies that such liabilities for the legal person do not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories of such crimes.[34]

Appreciating the cross-border tendencies of non-cash fraud and counterfeiting, the Framework Decision also calls for jurisdictional harmonization (Article 9), harmonization regarding extradition and prosecution

33 *See* Council *Framework Decision (2001/413/JHA) on combating fraud and counterfeiting of non-cash means of payment* of 28 May 2001, Articles 5-6.

34 *See* Council *Framework Decision (2001/413/JHA) on combating fraud and counterfeiting of non-cash means of payment* of 28 May 2001, Article 7. The punishment for legal persons who carry out such actions, besides being effective, proportionate and dissuasive, should, according to Article 8, also include sanctions such as: exclusion from entitlement to public benefits or aid; temporary or permanent disqualification from the practice of commercial activities; placing under judicial supervision; a judicial winding-up order.

(Article 10), and cooperation between Member States in respect of proceedings relating to the offenses provided for in the Framework Decision (Article 11). Finally, Member States are to set designated operational contact points for the exchange of information and other information between Member States for the purpose of applying the Framework Decision (Article 12).

As mentioned above, the Framework Decision goes a long way in tackling on-line transaction based fraud even with today's developments. Although Article 2c prohibits the possession of stolen or counterfeit payment instruments (i.e. credit cards), it only covers payment instruments that are "corporal" i.e. physical. Thus, the illicit possession of stolen information, stored on credit cards, is not explicitly covered by the Framework Decision. However, once that information is used to transfer monetary value illicitly, it falls under Article 3 which prohibits the use of computer data, in particular identification data, without right.[35] Following this line of reasoning, illicitly transferring of money through on-line services which do not require credit card details at all (for example on-line banking but also commercial services such as PayPal) are also covered by Article 3.

The practical application of Article 4 on current forms of fraud committed in "cyberspace" is, however, more questionable. While it definitely includes skimming devices, hardware and software devices used in creating credit cards with stolen information, it is not as successful in dealing with pure on-line situations such as phishing attacks or hi-jacked computers (so called *zombie* computers) used for such attacks. Para. 2 in Article 4 prohibits the fraudulent creation, use, transferring, etc of computer programs that are intended to commit offenses described in Article 3. As it has been established above Article 2 only covers situations where physical payment instruments are involved and although Article 3 covers situations where computer data or identification data is used without right, in a money transfer situation, it does not cover situations when such data is being stolen or the act of acquiring it. Since Article 3 only covers situations where money is actually being transferred, Article 4 para. 2 only prohibits software that interferes with such transmission in real time. Thus, Article 4 para. 2 would in essence only cover software used for "man-in-the-middle" attacks where a perpetrator eavesdrops on active Internet connections between, for instance, an on-line bank and its customer and changes the data sent back and forth so that the bank transfers money to another account than intended by the customer. Although such malicious software does exist in real life[36], it is a lot more common for malicious applications used during phishing attacks to gather the customers' login information first, transfer this to a perpetrator who then commits the actual fraud, or sells the details to a third party who commits the fraud. Such malicious applications (which do not do real-time editing of data) are, however, not covered by Article 4 and so creating, using or possessing the kinds of malicious applications used in a the vast majority of fraudulent situations are not prohibited by the Framework Decision. As mentioned above,

35 The rationale for this is that one could easily argue that the information stored on the chip or magnetic stripe on a credit card is a form of, or at least contains, identification data (data that identifies the owner and their account details).

36 *See* e.g. “en.wikipedia.org/wiki/Man_in_the_Browser”.

however, the moment the login details collected by these malicious applications are used, then they do fall under what is covered by Article 3.

It is important to remember the point made earlier in this section, that it is often difficult to make a clear distinction between the traditional forms of crime carried out on a computer and the computer-specific forms of crime. Thus, it is important that cybercrime legislation covers all steps and aspects of the offenses carried out. In this context the Framework Decision covers the actual fraudulent behavior of criminals while other regulations, such as the *Framework Decision on attacks against information systems*[37], cover the more technical aspects such as the gathering of login-information illicitly.

3.2.2 The Directive on the Prevention of the Use of Financial Systems for Money Laundering and the Directive on Payment Services in the Internal Market

In order to have a holistic approach to combating fraud regarding non-cash payments the efforts of the EU were not restricted to the third pillar of the European Union. The various legislative bodies of the EU were also active in the first pillar (the European Community) through the creation of Directives and Action Plans. Although legislation established through the first pillar can not, as a rule, specifically require Member States to introduce provisions of criminal law – this function has traditionally been reserved for EU legislation in the third pillar or the area of freedom, security and justice – the EC did, nonetheless, contribute an important part to the overall EU approach to tackling cybercrime.

In this context, it is especially important to mention two initiatives, the *Directive of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*[38] and the *Directive of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market*[39].

The money laundering-Directive is applicable to the financial sector, lawyers, notaries, accountants, real estate agents, casinos, trust and company service providers. The Directive introduces detailed obligations for these entities in relation to customer due diligence by requiring them to identify and verify the identity of their customer and of their beneficial owner, and to monitor their business relationship with the customer (Article 8). The Directive also calls for the reporting of suspicions of money laundering or terrorist financing to public authorities (such as the national financial intelligence unit) (Article 22). Those subject to the Directive also need to take supporting measures, such as ensuring the establishment of appropriate internal preventive policies and procedures and proper training of their personnel (Article 34). The implementation of the Directive should thus lead to a better management of fraud risks involved in, for example, non-face to face situations (e.g. when monitoring customers'

37 *See* Council Framework Decision (2005/222/JHA) on attacks against information systems, of 24 February 2005.

38 *See* Directive 2005/60/EC.

39 *See* Directive 2007/64/EC.

transactions). As organized crime syndicates often use hi-tech methods of carrying out financial crimes the Directive's "know-your-customer" approach and the due diligence enforced on the mentioned subjects, make it an important piece of the puzzle when it comes to combating such crimes.[40]

A practical example of where the Directive would be relevant is in combating child pornography on the internet. Previously, membership to such sites could easily be obtained through credit card transactions. With the Directive in place the bank issuing the account to the "organization" that collects the payments should know what the account will be used for before it is opened and what it is used for once it has been opened. Furthermore, if the bank knows that an account is used for illegal activities it should be able to identify other accounts depositing money into said account and report these to the proper authorities. Unfortunately, when it comes to the trafficking of credit card transactions over the Internet, the money trail is difficult to follow, making it at least as hard for investigators to trace the revenues.[41]

The *Directive on payment services and the internal market* aims to ensure that payments within the EU, in particular credit transfers and card payments, become as easy, efficient, and secure as domestic payments within Member States. Parts of the Directive are, however, aimed at addressing payment fraud. Article 42, for instance, requires service providers to inform service users with i.a. information about the payment instruments and on the use of the payment service used (Article 42(2)) along with information about the payment instruments' safeguards and corrective measures (Article 42(5)). Article 55(2) states, furthermore, that payment service providers may reserve the right to block the payment instrument for objectively justified reasons related to the security of the payment instrument while Article 57(1a) obliges payment service providers to make sure that the personalized security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument. Additionally Articles 60 and 61 define the liability relationships between the payment service provider and user regarding unauthorized transactions. Finally, Article 79 ensures the availability of personal data for processing by payment systems and payment service providers for fraud prevention purposes.

3.2.3 Action plans preventing fraud of non-cash means of payment

It is also important to mention the European Commission's specific work on fraud prevention of non-cash means of payment. To this end, the Commission

40 *See Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan*, Commission Staff Working Document SEC(2008) 511, p. 8, and *High-Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment 2007*, Europol High Tech Crime Centre, Public Version, August 2007, p. 18.

41 *See High-Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment 2007*, Europol High Tech Crime Centre, Public Version, August 2007, p. 18.

launched an Action Plan for 2001-2003[42] and one for 2004-2007[43]. These action plans contain the general approach to tackling the problem and are the instruments through which policy is coordinated among several different policy areas, such as internal market policies and justice and home affairs, and between different types of instruments, from voluntary exchanges of experiences in seminar format to legislative acts requiring Member States to change national law. During the first Action Plan (2001-2003) the Commission organized various conferences on the topic, provided an information exchange platform for various stakeholders, established the *EU Fraud Prevention Expert Group (FPEG)*[44] and participated in G8 meetings dealing with payment fraud.[45] Building on these activities, the Commission proceeded between 2004-2007, together with the FPEG and other bodies, to provide a platform for stakeholders for cooperation and for information exchange. The Commission also supported Europol's efforts to provide specialized training to national law enforcement authorities and facilitated the possible implementation of a single phone number for notification of lost credit cards. The roll-out of the Joint Investigations Teams under the aegis of Europol and Eurojust is a process that also took place during this period.[46]

3.3 Publication of Illegal Content

Content-related offenses or the publication of illegal content, as it is known in the EU's legislative frameworks, usually refer to sexual abuse or incitement to racial hatred in an on-line context.[47] The EU's efforts in stopping sexual abuse of children and child pornography reaches back to the nineties and encompasses, i.a., the *Joint Action concerning action to combat trafficking in human beings and sexual exploitation of children*[48] of 1997 which was replaced by the *Framework Decision on Sexual Exploitation of Children and Child Pornography*[49] in 2003. Similarly, the work on combating racism and

42 *See* Commission Communication COM(2001) 11 final of 2 February 2001 *Preventing fraud and counterfeiting of non-cash means of payment.*

43 *See* Commission Communication COM(2004) 679 final of 20 October 2004 *A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment*.

44 For more information on FPEG, *See* "www.ec.europa.eu/internal_market/fpeg/index_en.htm".

45 *See Report on the implementation of the EU Fraud Prevention Action Plan on non-cash means of payment*, Commission Staff Working Document SEC(2004) 1264.

46 *See Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan*, Commission Staff Working Document SEC(2008) 511.

47 *See supra* on the *Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, CETS No.: 189.

48 *See* Joint Action (97/154/JHA) of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children.

49 *See* Council Framework Decision (2004/68/JHA) of 22 December 2003 on combating the sexual exploitation of children and child pornography.

xenophobia also stretches back into the same period with the *Joint Action concerning action to combat racism and xenophobia*[50] from 1996 which resulted in, and a decade later was replaced by, the *Framework decision on combating racism and xenophobia*[51] in 2008.

3.3.1 The Framework decision on combating the sexual exploitation of children and child pornography

The purpose of the *Framework Decision on combating the sexual exploitation of children and child pornography* is to approximate laws and regulations of the Member States to combat the sexual exploitation of children and child pornography. It defines children as any persons below the age of 18 years and child pornography as visual material that depicts or represents a real child involved or engaged in sexually explicit conduct (including the exhibition of pubic area), a real person appearing to be a child involved in sexual conduct, or realistic fictional images of children engaged in sexually explicit conduct (Article 1).

The Framework Decision calls on Member States to criminalize offenses concerning the sexual exploitation of children (Article 2) and offenses concerning child pornography (Article 3). The Framework Directive calls for the criminalization of child pornography, when committed intentionally and without right, irrespective of the medium used to undertake the act (i.e. computer system or not). As such, production, distribution, dissemination or transmission, supplying or making available or acquisition or possession of child pornography is encompassed by Article 3 of the framework. Member States are given the option to create exceptions in their national implementations in the circumstances where a real person appearing to be a child was in fact 18 years of age or older at the time of the depiction. Exceptions can also be used in the case of production and possession, where images of children having reached the age of sexual consent are produced and possessed with their consent and solely for their own private use. Even where the existence of consent has been established, it shall not be considered valid, if for example superior age, maturity, position, status, experience or the victim's dependency on the perpetrator has been abused in achieving the consent. Finally, Member States are given the option for exceptions where it is established that a fictional pornographic material is produced and possessed by the producer solely for his or her own private use, as long as no child or person appearing to be a child was used for the purpose of its production, and provided that the act involves no risk for the dissemination of the material.

Article 4 calls the criminalization of instigation, aiding, abetting and attempt of the above mentioned crimes. The penalties for offenses in the Framework Decision should be criminal penalties of between one and three years of imprisonment and in case of aggravating circumstances the penalty range should

50 *See* Joint Action (96/443/JHA) of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia.

51 *See* Council Framework Decision (2008/913/JHA) of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

be between five and ten years of imprisonment.[52] The Framework Decision also calls on Member States to ensure liability for legal persons (Articles 6 and 7). Article 9 focuses on the protection of and assistance to victims providing that investigations into the prosecution of offenses covered by the Framework Decision shall not be dependent on the report or accusation of the victim (at least when the crime is committed on a Member State's territory). The article also states that victims of sexual exploitation shall be treated as vulnerable victims and that Member States shall take all measures possible to ensure appropriate assistance for the victims' families (Article 5).

The jurisdictional regulations are, as in all situations regarding cybercrime, very important. The Framework Decision establishes that each Member State should have jurisdiction over offenses committed in whole or partly on its territory (Article 8(1)(a)) or by one of its nationals (Article 8(1)(b)). They shall also have jurisdiction over child pornography crimes (and if relevant for instigation, aiding, abetting or attempt of such crimes) if the offense is committed by means of a computer system accessed from their territory (the computer does, however, not have to be physically located on the Member State's territory) (Article 8(5)).

As mentioned above, the Framework Directive calls for criminalization of acts related to child pornography regardless if it is committed on a computer system or not. There is a requirement for intentional conduct. As such, persons who have their computers hijacked and used as a distribution point of child pornography are not covered by the area criminalized by this Framework Decision. It is, however, unclear to what extent the act of viewing child pornographic content on a computer is included or not. While Article 3(1)(d) criminalizes the acquisition or possession of child pornography it is unclear whether viewing of such content through streamed media, which is only a temporary measure where none of the content is stored on the perpetrator's computer, would be included by the definition. Naturally, every Member State's implementation of this regulation varies to some extent, and unfortunately, there are no clues regarding this issue in the report by the Commission regarding the Member States implementation of this Framework Decision either.[53]

52 An aggravating circumstance is, for example coercing a child into prostitution or participating in pornographic performances or profiting from such acts. Other aggravating circumstances include situations where the victim is a child below the age of sexual consent, the offender has deliberately or by recklessness endangered the life of the child, the offenses involve serious violence or caused serious harm to the child or the offenses are committed within the framework of a criminal organization. Member States are also supposed to take necessary measures to ensure that a natural person, who has been convicted of one of the offenses above, may, if appropriate, be temporarily or permanently prevented from exercising professional activities related to the supervision of children.

53 *See* Commission Communication COM(2007) 716 final of 16 November 2007, Report from the Commission Based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography.

3.3.2 Framework decision on combating racism and xenophobia

The adoption of the *Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law*[54] has been the subject of lengthy and difficult negotiations from 2001 when the Commission first presented a proposal. It wasn't until June 2005 that the Justice and Home Affairs Council could reach a draft compromise text and the Council reached a general approach in April 2007.[55] The Framework Decision finally entered into force 28 November 2008.

The Framework Decision aims to combat racism and xenophobia through a common minimum set of criminal law penalties at a European level but is limited to combating particularly serious forms of racism and xenophobia (Preamble 6). It is also, limited in the sense that it does not give the Member State's the authority to modify the fundamental rights and fundamental legal principles, including freedom of expression and association enshrined in Article 6 of the Treaty on European Union (Article 7).

Racist and xenophobic acts are considered to be, when committed intentionally, publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin (Article 1). The article also includes the commission of materials for public dissemination or distribution or publicly condoning denying or grossly trivializing war crimes directed against a group of people where the conduct is likely to incite to violence or hatred of the said group. Member States are given the option to only punish conduct which is carried out in a manner likely to disturb public order or that is threatening, abusive or insulting (Article 1(3)) and acts of denying or grossly trivializing war crimes only if such war crimes have been established as such by a court (Article 1(4)).

The Framework Decision calls for the criminalization of instigation, aiding and abetting (Article 2) of named offenses and sets criminal penalties to a maximum of at least between 1 and 3 years of imprisonment (Article 3(2)). Member States are also required to ensure that racist and xenophobic motivation in other forms of crimes (i.e. all forms of crime except for the ones stated in Article 1 and 2) are considered as aggravating circumstances or, alternatively, that such motivation may be taken into consideration when courts determine penalties (Article 4). Article 5 and 6 extend the liability of offenses described in the Framework Decision to legal persons as well.

The Framework Decision's jurisdictional regulations are also important from a cybercrime perspective. Article 9(1)(a) and (1)(b) establishes national jurisdiction for offenses committed on a Member State's territory or by its national. Article 9(2a) extends national jurisdiction to cases where the offense is committed through an information system and the offender commits the conduct while physically present in the state's territory (the material does not have to be hosted on the state's territory). The same holds true if the offense involves

54 Ref. no. 2008/913/JHA.

55 For a description of this agreement, *See* e.g. "www.europarl.europa.eu/oeil/resume.jsp?id =216962&eventId=1004469&backToCaller=NO&language=en".

material hosted on an information system on the state's territory irrespective of the perpetrator's physical location when the crime is committed.

This Framework Decision regulates actions whereby someone publicly and verbally acts against a group of people. Arguably, there is nothing more public than the Internet. However, information available on the Internet can be aimed at a limited group of people, in which case the requirement of publicity may not be fulfilled. This can be achieved either by technical means, i.e. by passwords protecting access to the place where the information is made available, or simply by intent, i.e. the person publishing the information intending only for a special group of people to access it. It is, of course, the Member States' national legislation which steers to what extent publications on the Internet are to be considered public, as this is not regulated through the Framework Decision.

3.4 Crimes Unique to Electronic Networks

The category of crimes unique to electronic networks is what probably first springs to mind when the term cybercrime is used. It includes actions such as hacking, man-in-the-middle attacks, denial of service attacks, phishing, viruses, trojans, worms and all other forms of malicious activity that flourishes through the Internet. While the previously mentioned EU instruments dealing with cybercrime are based on, or are at least inspired by, the Cybercrime Convention, a close inspection of the *Framework Decision on attacks against information systems*[56] reveals that it contains sections directly taken from the Cybercrime Convention. In some aspects, however, the two pieces of regulation are different. In addition to presenting the Framework Decision, the section below will explore the incongruence between the definitions used in the Framework Decision and the Convention concerning information and computer systems, in order to exemplify real life consequences of such legislative discrepancies.

3.4.1 Framework decision on attacks against information systems

In 2002, the Commission proposed a *Framework Decision on attacks against information systems*,[57] in order to improve co-operation between judicial and other competent authorities through approximating rules on criminal law in the European Member States in the area of attacks against information systems. The Framework Decision was adopted in February 2005 requiring Member states to comply with its provision by 16 March 2007.[58]

The Framework Decision deals with certain areas covered by the Cybercrime Convention, but is not as extensive in scope as the Convention. The definitions used in the adopted version of the Framework Decision are for instance less extensive in comparison to the proposed Framework Decision of 2002. Several of the terms defined in Article 1 in the proposal did not make it to the final version adopted in 2005. The definition of "electronic communications network" was, for example, not included in the final version of the Framework Decision

56 *See* Council Framework Decision (2005/222/JHA) of 24 February 2005 on attacks against information systems.

57 *See* Commission Communication COM(2002) 173 final of 19 April 2002.

58 *See* Council Framework Decision (2005/222/JHA) of 24 February 2005.

because including it under the definition of "information system" was deemed by many Member States as too extensive.[59]

Article 1 of the final version of the Framework Decision defines technical terms, such as "computer data", which is duplicated verbatim from the Convention. Instead of "computer system", which is the term used in the Cybercrime Convention, the Framework Decision uses "information system". Both terms cover individual or connected computing devices which through software process computer data. The definition of information systems (Framework Decision) includes non-executable computer data stored on a device that is needed for the devices to function (Article 1(c)) while the definition of computer system (Cybercrime Convention) does not include any non-executable computer data.[60] The provisions on illegal access to information systems in Article 2 of the Framework Decision equal Article 2 of the Convention and are defined as the intentional access, without right, to the whole or any part of a computer/information system. Paragraph 2 of the Article in the Framework Decision provides Member States with the option to limit criminal activity to intrusion through a security device. This optional qualifying element can also be found in the Convention. Other elements of the Convention such as the intent of obtaining computer data or other dishonest intent are not, however, present in the Framework Decision.

As such, both the Cybercrime Convention and the Framework Decision cover access, without right, to any device or the software on a device. However, since neither the Convention's nor the Framework Decision's definition of computer/information system includes non-executable computer data the question arises whether a perpetrator commits a crime when accessing such data (such as documents, pictures, movies that can not be considered to be executable software). Point 46 of the Explanatory Report to the Cybercrime Convention expands the definition of computer system and clearly states that accessing computer systems also occurs when content-related data is accessed without right. Thus in the context of the Cybercrime Convention illegal access to computer systems includes accessing, without right, whole or part of a device that can run executable code or accessing any software or any content related data on such a device. In direct contrast to the Cybercrime Convention, however, illegal access, as defined by the Framework Decision, only encompasses non-executable computer data that is required by the system to operate.[61] As such, accessing stored data that can not be executed and which is not used by the system for its functioning (such as documents, pictures, music or video files), without right, can not be considered illegal access through the Framework Decision.

This distinction has actual consequences in real life situations. One example for consideration is a public e-mail service provider where anyone can create a user account and send e-mails from that account. If a perpetrator does not have an account with this service, he/she would be committing a crime if he/she tried

59 *See* Swedish Government Bill (Prop. 2006/07:66) p. 23.

60 *See* Explanatory Report to the Convention on Cybercrime (ETS No. 185) point 23.

61 *See* Swedish Government Bill (Prop. 2006/07:66) p. 23.

to "hack" the system to gain access to other users' e-mails or login information. This is because the perpetrator would be trying to access the system without right, through the e-mailing application or the system software itself (which, in both situations, are considered to be executable applications). So far, both the Cybercrime Convention and the Framework Decision are in agreement.

But the situation becomes radically different if the perpetrator has a valid e-mail account with the service provider and also knows, or guesses, another user's login details. When the perpetrator logs in to the other user's account (without consent) he/she simply accesses static data which is stored on the system and which is neither executable nor necessary for the system to operate. Although the perpetrator does so without consent from the other user, he/she does not actually access any part of the system without right since he/she does have the right to enter the part of the system where e-mails can be read. However, the data accessed this way can not be executed and falls, therefore outside the scope of an information system as defined by the Framework Decision. Using the definition made by the Swedish legislature, this scenario could therefore not be described as illegally accessing an information system. It is important to remember that Member States have introduced their own definitions of illegal access to information systems and so situations which may not be covered by the wording of the Framework Directive Decision may indeed be covered by national legislation.[62] Over time, this room for interpretation may lead to challenges in Member State cooperation, in its turn leading to a need for stricter approximation on this specific provision.

Although illegal access to static computer data may not be covered by the Framework Decision, any illegal data interference (deletion, damaging, deterioration, alteration, suppression or rendering inaccessible) is covered through Article 4. This article prohibits anyone from modifying any data stored on an information device without right. In the above scenario if the perpetrator would have changed or deleted any e-mail in the other user's e-mail account, then he/she would have committed illegal data interference.

Article 3 ensures the criminalization of serious hindering or interruption of the functioning of an information system. This regulation has become very important in recent years as the use of bot-nets has grown dramatically. As the incidents related to Estonia in 2007 have shown,[63] shutting down information systems by overloading them through various means is just as efficient as hacking them (and usually requires a lot less resources or skills).

Article 5 of the Framework Decision penalizes the dependent forms of crime, instigation, aiding, etc. Article 6 deals with the penal aspects of the Framework Decision requiring that the penalties of offenses referred to in Articles 2, 3, 4, and 5 are effective, proportional and dissuasive and that illegal system and data interference (Articles 3 and 4 respectively) are punishable by at least one year of imprisonment. Article 7 expands the prison sentence to between two and five

62 Chapter 4 §9c of the Swedish Penal Code, defining the crime of data intrusion, most definitely encompasses the mentioned scenario, in spite of the mentioned reasoning.

63 *See* e.g. "en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia".

years for illegal system and data interference and for illegal data access if such access infringed on security measures (Article 2(2)).

Article 8 ensures that the actions of legal persons (more precisely, persons who are in leading positions of legal entities) also fall under the jurisdiction of the Framework Decision. The Framework Decision makes the leaders of legal persons responsible not only for direct actions which result in the offenses described in the Framework Decision but also for the above listed dependent forms of crime and also indirect actions where the lack of supervision or control by such persons lead to offenses described in the Framework Decision. As penalties for legal persons, the Framework Decision lists criminal or non-criminal fines and gives the Member States the option of also implementing penalties of exclusion from entitlement to public benefits or aid, of temporary or permanent disqualification from the practice of commercial activities, of placing legal persons under judicial supervision or of judicial winding-up orders (Article 9).

Article 10 deals with Member States' jurisdiction. A Member State has jurisdiction over crimes committed in whole or in part on its territory or by one of its citizens. Crimes committed on a Member States territory include situations when the offender committed the offense while physically present on the State's territory or when the offense was carried out against an information system located on the State's territory. Provisions for conflicting jurisdictions and the traditional *aut dedere aut judicare*-provision one normally finds in EU-instruments are also covered in Article 10.

Member States shall use the existing 24/7 networks of operational points for the exchange of information concerning the investigation of the crimes concerned, according to Article 11. The article refers to "operational points" which is a way of linking the networks together along the same lines as the Convention does through Article 35, i.e. the G8-inspired 24/7-network.

3.4.2 Other efforts by the European Commission

In addition to the criminal legislative efforts undertaken by the EU through the *Framework Decision on attacks against information systems*, the European Commission has been assisting in the fight against spam and malware as well. It has, i.a., launched awareness raising-campaigns, including the *Safer Internet plus program*, which promotes safer use of the Internet and new online technologies and is intended particularly for children. It hosted an OECD workshop on spam in 2004 and contributed to the OECD's *Anti-spam toolkit*. The Commission has also assisted the fight against spam and malware through cooperation initiatives and cross-border cooperation. The *Contact Network of Spam Authorities (CNSA)*, a network that meets regularly, exchanges best practices and cooperates on enforcement across borders in the fight against spam. It is also conducting initiatives with the United States, China, and in Japan on this matter. The Commission launched several research projects (with a total financing of €13,5 million) under the *6th RTD Framework Program*[64] to help

64 *See* Commission Communication COM(2006) 688 final of 15 November 2006 on Fighting spam, spyware and malicious software, pp. 4-6. RTD refers to research, technological development and demonstration activities in the European Union.

stakeholders fight spam and malware. These projects include a range of different technical approaches for fighting spam, phishing and malware. Finally, The Commission has supported industry actors in their ongoing struggle. Amongst others, it co-funds the *Spotspam initiative*,[65] which is a partnership between private and public bodies aiming to build a database to facilitate the cross border investigation and enforcement of spam cases.[66]

In the Communication on fighting spam, spyware and malicious software from November 2006, the Commission calls on Member States, the industry and the EU to take action in a unified manner against spam and malware. The Commission proposes that Member States lay down clear lines of responsibility for the agencies involved in tackling spam; that they ensure effective coordination between their national authorities; that they involve market players; that they ensure adequate resources for law enforcement efforts; and that they subscribe to international cooperation procedures and act on requests for cross border assistance. The Commission also invites the industry to ensure that the standard of information for the purchase of software applications is in accordance with data protection regulations; to contractually prohibit illegal use of software in advertisements; and e-mail service providers to apply filtering policies. Finally, the Commission asserts that it will continue with its awareness-raising and stakeholder cooperation-efforts; it will continue to develop agreements with third countries; attempt to introduce new legislation to strengthen the rules in the area of privacy and security in the communications sector; it will involve ENISA expertise in security matters; and that it will support research and development in the 7th Framework Program.[67]

The Commission has also been active in spreading knowledge about the need for cyber security. It has achieved this through, amongst others, the Communication on a strategy for a secure information society.[68] The maturing knowledge about information security risks are clearly expressed by the insights expressed in the Communication. In this Communication, the Commission identifies not only the well known and documented security threats (such as spam, malicious code and botnets), but also emerging ones (such as threats arising from more and more communication devices being inter-connected and connected to the Internet through high speed connections). Such solutions offer significant opportunities but also significant security and privacy risks.[69]

Just like in the Communication on fighting spam, spyware and malicious software, the Commission makes certain suggestions in the Communication on a strategy for a secure information society as well. As a first suggestion the

65 *See* "www.spotspam.net".

66 *See* Commission Communication COM(2006) 688 final of 15 November 2006 on Fighting spam, spyware and malicious software, pp. 4-6.

67 *See* Commission Communication COM(2006) 688 final of 15 November 2006 on Fighting spam, spyware and malicious software, pp. 6-11.

68 *See* Commission Communication COM(2006) 251 final of 31 May 2006 A strategy for a Secure Information Society.

69 *See* Commission Communication COM(2006) 251 final of 31 May 2006 A strategy for a Secure Information Society, pp. 4-5.

communication expresses that diversity, openness and interoperability are integral components of security and should be promoted. The Commission then expresses that there is a need to improve the knowledge of the problem before it can be fully tackled and that a change in the mindset of organizations regarding security needs to be achieved whereby security should be looked upon as a virtue and opportunity and not as liability and cost.[70]

In order to achieve a secure Information Society, the Commission expresses the need for a widespread culture of security through a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. To achieve this, the Commission carried out various policy initiatives, amongst others the addressing of new and emerging threats complementing the Commission's Green Paper on the European Programme for Critical Infrastructure Protection.[71]

3.4.3 Offenses related to infringements of intellectual property rights

Chapter II, Section 1, Title 4 of the Cybercrime Convention deals with offenses related to infringements of copyright and related rights. The Commission's definition and categorization of cybercrime, as defined in the *Communication Towards a general policy on the fight against cyber crime*[72], does *not* include intellectual property rights infringements as a part of cybercrime. A closer description of the EU instruments relating to this topic fall outside the scope of this article. That does, however, not mean that there have not been any developments in this field in the EU. Arguably the most influential, and most controversial, developments in this field were the adoption of the *Directive on the enforcement of intellectual property rights*[73] which entered into force in April 2004.

3.5 Enabling Law Enforcement to Combat Cybercrime

As outlined above, the EU instruments of the past decade do to a large extent mirror the essence of the Cybercrime Convention, albeit in the more supranational way that is possible through EU legislation. The Cybercrime Convention does, however, only deal with the legislative aspects of criminality that provide the definitions that prosecutors need to bring a case in front of a judge and for the judge to be able to make a ruling. All this means nothing, however, if the law enforcement agencies are not given the means of collecting evidence upon which a case can be built.

Since the Internet has to a large extent become an alternative means of communication, replacing regular communications mechanisms such as

70 *See* Commission Communication COM(2006) 251 final of 31 May 2006 A strategy for a Secure Information Society, p. 5.

71 *See* Commission Communication COM(2006) 251 final of 31 May 2006 A strategy for a Secure Information Society, p. 7, and Commission Green Paper on the European Programme for Critical Infrastructure Protection, COM (2005) 576 final of 17.11.2005.

72 *See* Commission Communication COM(2007) 267 final of 22 May 2007 Towards a general policy on the fight against cyber crime, p. 5.

73 *See* Directive (2004/48/EC) of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

telephones or mobile phones, it is only natural that criminals use the Internet to communicate with each other. Thus, law enforcement agencies need not only the technical tools to access and monitor communication carried out over the Internet, but also need the legal authority and procedural guidelines on when and how such monitoring can be carried out.

3.5.1 Directive on traffic data retention

The *Directive on privacy and electronic communication*[74], adopted in July 2002, allows Member States to restrict the rights of citizens to their privacy and oblige communications providers to store data that can intrude on citizens' privacy for the purpose i.a. of national defense and criminal prosecution (Article 15(1)). Considering the border-less characteristic of cybercrime, the fact that there may be a need for a more harmonized approach to this problem was already identified in the Cybercrime Communication in which the Commission called for examining whether there was a need for retention of traffic data.[75] The storage of traffic data was then harmonized in March 2006 through the *Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*.[76]

The Directive aims to harmonize Member State's provisions concerning the obligations of communication service providers to retain traffic and location data, generated by natural persons and legal entities that are needed for investigations and prosecution of serious crime (Article 1). It is important to note that the Directive only encompasses traffic and location data. It explicitly states that it does not apply to the content of such communications (Article 1(2) and Article 5(2)). Although the purpose of the Directive is for collected data to be available for law enforcement in cases of serious crime, it does not hinder Member States from adopting national legislative measures that provide national authorities with access to this data in other instances as well, as long as these measures fully respect fundamental human rights (Preamble 25).

The data to be retained is data necessary to trace and identify the source of a communication, the destination of a communication, the date and duration of a communication, the type of communication, the user's communication equipment and the location of the communication equipment if a mobile device was used (Article 5). The Directive includes communication taking place on fixed network telephony devices, mobile telephony devices, Internet access, Internet e-mail and Internet Telephony.

---

74 *See* Directive (2002/58/EC) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

75 *See* Commission Communication COM(2007) 267 final of May 22 2007 Towards a general policy on the fight against cyber crime, p. 5.

76 *See* Directive (2006/24/EC) of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The table below summarizes the various data that service providers need to retain about each communication made through their services.

Categories of Retained Data	**Fixed and Mobile Telephones**	**Internet access, E-mail and Internet Telephony**
Source of a Communication	The calling telephone number. The name and address of the subscriber.	Allocated user ID. User ID and telephone number to communication that uses public phone networks.
Destination of a Communication	Numbers dialed and any routing information. Name and address of subscriber.	*Internet Telephony:* user ID or telephone number of intended recipient. *E-mail and Internet Telephony:* Name and address of subscriber and user ID of intended recipient.
Date, Time and Duration of a Communication	Date and time of the start and end of the communication.	*Internet access:* user ID and IP address along with date and time for log-in and log-off based on a time zone. *E-mail and Internet Telephony:* date and time of log-in and log-off of the service based on a certain time zone.
Type of Communication	The telephone service used	The internet service used
User's Communication Equipment	*Fixed telephony:* The calling and called telephone numbers. *Mobile telephony*: The calling and called phone numbers. IMSI and IMEI of the calling and called parties. In case of pre-paid anonymous services, the date and time of the initial activation of the call and the Cell ID from which the call was activated.	The telephone number in case of dial-up accesses. The end point (e.i. DSL) of the originator of the communication.
Location of Mobile Communication Equipment	Cell ID at the start of the communication. Data identifying the geographic location of cells by reference to their Cell ID during the period for which the communications data are retained.	

The data collected in such manner needs to be retained by the service provider for no less than six months and no more than two years from the date of the communication (Article 6). The Directive calls for the secure storing of, the limited access to and, after the expiration of the retention time, the deletion of the collected data (Article 7). Besides being stored securely, the collected data must be stored so that it can be transmitted to competent authorities, upon request, without delay (Article 8). The Directive also calls for Member States to set up or designate public authorities to oversee the application of the provisions

of the Directive (Article 9) and to provide statistics to the Commission on a yearly basis (Article 10).

4 Way Ahead – Challenges for the EU

4.1 General Challenges

As the mobilization of political support behind the legal developments of the EU, and other actors, appear to be triggered by external stimuli (organized crime, terrorism, e-business, etc.) it is reasonable to ask from where the next such impetus will come and in what form, as well as whether it will be sufficient to mobilize the support necessary for the challenges ahead. This is part of the political challenge of regulating through criminal law the undesired utilization of ICT. While the efforts of the EU thematically can be seen as movement in different phases – protection of vulnerable groups (children, consumers), protection of individuals in general, protection of individuals and the political structures of Member States, and protection of the integrity of the physical infrastructure of Member States – the EU now finds itself at a crossroad.

In a recent phase, having exhausted the legislative room – at least under the pre-Lisbon treaties – of combating criminal threats to individuals and states through criminal law, the EU turned to the protection of the infrastructure of its Member States. The EU measures for Critical Infrastructure Protection (CIP)[77] are still in a sense embryonic; the only legislative act is a directive EU COM(2006) 786 which defines European Critical Infrastructure as designated critical infrastructures that, in case of fault, incident or attack, could impact both the country where it is hosted and at least one other EU Member State. The Directive establishes a procedure for the identification and designation of Critical Infrastructure (CI), and a common approach to the assessment of the needs to improve the protection of such infrastructure. Parallel to this directive, the European Commission manages the *European Programme for Critical Infrastructure Protection (EPCIP)*, providing support to Member States in enhancing the protection of relevant infrastructure. Such measures, designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, include the *Critical Infrastructure Warning Information Network (CIWIN)*, the use of expert groups at and the identification and analysis of interdependencies, and support for Member States concerning National Critical Infrastructures (NCI). The measures also encompass the accompanying financial measures and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP-related measures having a potential for EU transferability. The Directive as well as EPCIP identifies ICT among the different ECI sectors, falling within their respective mandates. The creation of the European Network and Information Security Agency (ENISA) for communication security, should also be seen as part of this effort.

77 Inspired, no doubt, by the American Presidential directive PDD-63 of May 1998, setting up a national program of “Critical Infrastructure Protection”.

The EU efforts were initiated by the Commission, through its first policy document, 'Critical infrastructure protection in the fight against terrorism' from 2004.[78] In it, the Commission offers this relatively wide description of European Critical Infrastructure (ECI): "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services."

A Green Paper on Critical Infrastructure, published on 17 November 2005[79], followed, where the Commission addressed issues such as what threats are relevant, the definition of what EU critical infrastructure is and what national critical infrastructure is, as well as the role of owners and operators of infrastructure. In the course of 2005 the Commission created a Critical Infrastructure Warning Information Network (CIWIN), which brings together member-state CIP specialists to assist the Commission in drawing up a programmes to facilitate exchange of information on shared threats and vulnerabilities and appropriate counter-measures and strategies.[80] On 12 December 2006, the European Commission adopted a Communication to improve the protection of European Critical Infrastructure (ECI) from terrorism, in which a Directive was proposed.[81] The justification at the time was overwhelmingly from the threat of terrorism, with references to the atrocities of 11 September 2001 in New York, the Madrid train bombing in 2004 and the London Underground attacks in July 2005, that all indicated terrorists' willingness to target infrastructures such as transport, energy and communication.

A challenge that was recognized at early stages of the EU CIP-process, similar to that of the early days the Council of Europe Cybercrime Convention, was the need to engage countries outside the EU in the process, in order to make any effort viable. When an EU task force was established in 2005 to explore what its Member States are doing to combat cyber-threats against critical infrastructure, the scope of its cooperation mandate was extended to include USA, Canada, Australia and Russia.[82]

---

78 *See* Commission Communication COM(2004) 702 final of 20 November 2004 on Critical Infrastructure Protection in the fight against terrorism.

79 *See* Green Paper COM(2005) 576 final of 17 November 2005 on A European Programme For Critical Infrastructure Protection.

80 The United States has a similar system known as Critical infrastructure Warning Information Network (CWIN), operational since 2003.

81 *See* Commission Communication COM(2006) 786 final of 12 December 2006 on a European Programme for Critical Infrastructure Protection.

82 This project is known as *the EU's Critical Information Infrastructure Research Coordination CI2RCO project.*

A challenge that emerges – especially after the Estonia incident in 2007 – as a missing link between these initiatives on critical infrastructure, and the efforts against cybercrime, concerns is the interface between criminal law and international law, namely the situation when attacks on a function or a system in a country is perpetrated not by individual hackers, nor by organized crime networks orchestrating BOT-attacks, but by foreign state actors consciously attempting to harm functions in another country. The technical challenge lies in the fact that initially, such an attack may have all the appearances of any other, non-state initiated intrusion, and it is only after a successful investigation into the origins of the attack that investigators will discover that the originator was in fact an agent of a state.[83]

4.2 Legislative and Legal Challenges – Lisbon and the Stockholm Programme

Apart from addressing new political challenges through legislation, a main preoccupation for the EU over the next years, is likely to be the "Lisbonization" of the area that has already been covered by legislative acts. This is a pattern we recognize from the aftermath of the entry into force of the Amsterdam Treaty in 1999; there were acts adopted for purposes of approximation of criminal law under the Maastricht Treaty, but with the limited effect that justice and home affairs acts had under that treaty, the additional strength acquired under Amsterdam was rapidly used to replace such acts with stronger instruments, although all such acts suffered from having to be adopted by unanimity under Amsterdam, thereby reducing their thrust down to the lowest common denominator. (This has been described above, i.a. with regard to the EU instruments on child pornography, where a Framework Decision (the more forceful Amsterdam instrument) replaced the Joint Action covering the same area, from the Maastricht era.) Under the Lisbon Treaty, most justice and home affairs will be adopted through the normal EU legislative procedure, i.e. through qualified majority voting, and with a stronger role for the Court in ensuring their effective implementation. The Stockholm Action Plan (see below) provides an outline over what some of these legislative reinforcements will be, but we are likely to see more.

The Stockholm Programme is in truth two different instruments: a political commitment by the Council, as well as an action plan that operationalizes this commitment. It is the latter instrument that gives a clear picture of the legislative thrust in justice and home affairs, or freedom, security and justice, as the more euphemistic heading refers to it. The Stockholm Programme Action Plan was proposed by the Commission and outlines most activity under this five year-plan. Areas of relevance for cybercrime are found under several different

83 Reference should be made here to i.a. the case from the International Court of Justice (ICJ), *The Republic of Nicaragua v. The United States of America*, of 1986. The ICJ held that the U.S. had violated international law i.a. by supporting Contra guerrillas in their rebellion against the Nicaraguan government. Although the support to the Contras was indirect, the Court nevertheless found in its verdict that the United States was "in breach of its obligations under customary international law not to use force against another State", "not to intervene in its affairs", and "not to violate its sovereignty". Applied to situations where a state engages "contractors" to carry out cyber-attacks, the case has certain relevance.

headings, with indications of responsible EU entity (Commission, Member States) as well as the year in which the activity will be launched.[84]

The most central area of activity for ICT relevance is naturally *"Cyber-crime and Network and Information Security"*. Under this heading we find

- measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as the one on modernized Network and Information Security Agency (ENISA) as well as other measures allowing faster reactions in the event of cyber attacks Council/Commission/European Parliament, 2010-2012),
- a legislative proposal on attacks against information systems (Commission, 2010),
- the creation of a cybercrime alert platform at European level (Europol/Commission, 2010-2012),
- the development of a European model agreement on public private partnerships in the fight against cybercrime and for cyber security (Commission, 2011),
- measures, including legislative proposals, to establish rules on jurisdiction on cyberspace at European and International levels (Commission, 2013), as well as
- the ratification of the 2001 Council of Europe Cyber-crime Convention (Member States, no time given).

Of direct interest is also *"Economic crime and corruption"*. With actions such as a legislative proposal on criminal measures aimed at ensuring the enforcement of intellectual property rights (replacing proposal COM (2006) 168 final) (Commission, 2011), and a European strategy on identity management, including legislative proposals on criminalization of identity theft and on electronic identity (eID) and secure authentication systems (Commission, 2012), the Commission takes a leading role in ensuring that the EU keeps criminal legislation up to date with emerging trends in economic crime through the misuse of ICT.

Under *"Protecting citizen's rights in the information society"* the following measures should be noted:

- a Communication on a new legal framework for the protection of personal data after the entry into force of the Lisbon Treaty (Commission, 2010),

84 *See* Commission Communication COM(2010) 171 final of 20.4.2010 Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme.

- a new comprehensive legal framework for data protection (Commission, 2010), and
- a Communication on Privacy and trust in Digital Europe: ensuring citizens' confidence in new services (Commission, 2010).

The planned efforts under *More effective crime prevention – Statistics* contain more activities of ICT relevance than perhaps first meet the eye. The first EU Security Survey (Commission, 2013) will be created as a sort of in-depth Eurobarometer[85] in the area of crime fighting. As a prelude for this survey, a serious effort will be made to align crime statistics formats and, to some extent, reporting mechanisms, which is outlined in the action Collection of comparable statistics on selected crime areas: money laundering, cybercrime, corruption, trafficking in human beings (Commission, Ongoing).

More targeted measures are foreseen under *Protection against serious and organized crime - Sexual exploitation of children and child pornography***,** such as the proposal for a Directive on combating sexual abuse, sexual exploitation of children and child pornography (Commission, 2010), the promotion of partnerships with the financial sector in order to disrupt the money transfers related to websites with child abuse content (Commission, Ongoing), and promote relevant measures under the Safer Internet Programme 2009-2013 (Commission, Ongoing).

The area of *Terrorism* maintains its importance for the EU, as is demonstrated by the following actions: a communication on stocktaking of counter-terrorism measures (Commission, 2010), a recommendation to authorize the negotiation of a long term agreement between the European Union and the United States of America on the processing and transfer of financial messaging data for the purpose of the fight against terrorism (Commission, 2010), public-private sector dialogue on illegal online activities related to terrorism and other crimes (Commission, 2010), a report on non-legislative measures to combat the use of the Internet for terrorist purposes (Commission, 2011), improvement of the fight against illicit use of dual use goods (Commission, ongoing).

The growing importance of Critical Infrastructure Protection is demonstrated under *Comprehensive and effective EU Disaster Management: reinforcing the EU's capacities to prevent, prepare for and respond to all kinds of disasters,* where we find the following actions:

- evaluation of the pilot-phase of the Critical Infrastructure Warning Information Network (CIWIN) system in preparation of the decision on further progress (Commission, 2010),
- a proposal on the implementation of the solidarity clause (Commission, 2010-2011),
- a communication on the reinforcement of the EU's Disaster Response Capacity (Commission, 2010), reinforcing the Monitoring and

85 *See* "ec.europa.eu/public_opinion/index_en.htm".

Information Centre's (MIC) analytical and coordination capacity (Commission, 2010 onwards),

- a report on the implementation of Directive 2008/114 on Identification of European Critical Infrastructure, followed by a review of the Directive including considering the extension of the scope (Commission, 2011/2012).

A number of initiatives planned in several different designated areas, are ”upgrades” of instruments created by the Treaty of Amsterdam for fighting crime or simply the evaluation of such instruments, with an implicit ”threat” to re-legislate. This is the case with:

- the implementation of the Framework Decision 2008/913/JHA on racism and xenophobia (Member States/Commission, 2010/Ongoing),
- a Communication on the fight against racism, xenophobia and discrimination (Commission, 2011),
- a report on the implementation of the Framework Decision 2008/913/JHA on racism and Xenophobia, (Commission, 2013),
- a report on the implementation of the Framework Decision 2002/584/JHA on the European Arrest Warrant, and appropriate follow-up (Commission, 2010/2014),
- a legislative proposal on a comprehensive regime on obtaining evidence in criminal matters based on the principle of mutual recognition and covering all types of evidence (Commission, 2011),
- a legislative proposal to introduce common standards for gathering evidence in criminal matters in order to ensure its admissibility (Commission, 2011), and
- a proposal for a Regulation providing Eurojust with powers to initiate investigations, making Eurojust's internal structure more efficient and involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities (Commission, 2012).

The heading *Internal Security Strategy* contains only one action of relevance, namely the Communication on the Internal Security Strategy (Commission, 2010) but this is likely to be an instrument – albeit not a legislative instrument, at first – of broad implications, as is the actions we find under *Upgrading the tools for the job - Managing the flow of information* which include:

- a Communication on the overview on information collection and exchange (Commission, 2010),
- a legislative proposal on a common EU approach to the use of passenger name record data for law enforcement purposes (Commission, 2010),

- a Communication on the transfer of Passenger Name Record (PNR) data to third countries (Commission, 2010),
- a proposal for authorizing the negotiation of agreements on Passenger Name Record data between the European Union and relevant third countries (Commission, Ongoing/2011-2014),
- an evaluation report of the application of the Data Retention Directive 2006/24/EC, if necessary followed by a proposal for revision (Commission, 2010/2012),
- a report on the implementation of the Framework Decision 2006/960/JHA (Swedish initiative) on the exchange of information between the law enforcement authorities (Commission, 2011),
- a report on the implementation of the Decision 2008/615/JHA (Prüm Decision) on the interconnection of DNA, fingerprints and vehicle information databases (Commission, 2012), Communication on the European Information Exchange Model, followed by an Action Plan (Commission, 2012/2013),
- a Communication on enhancing the traceability of users of pre-paid communication services for law enforcement purposes (Commission, 2012), and
- a Green paper on commercial information relevant to law enforcement and information exchange models (Commission, 2012).

5 Conclusions

Since the conclusion of the negotiations leading to the Cybercrime Convention, the EU has not only caught up with the Council of Europe's extensive convention, but also surpassed it in scope and in strength, utilizing the stronger framework for both legislation and for cooperation that the EU provides. This strength increases under the Lisbon Treaty. A schematic comparison between the efforts of the two main institutionalized European legislative and cooperative processes, reflects this. Reference is made here also to an instrument which is not cybercrime specific, in order to complete the picture of the arsenal of relevant EU instruments. The MLA Convention or the EU Convention on Mutual Assistance in Criminal Matters of 2000, aims to encourage and modernize cooperation between judicial, police and customs authorities within the Union as well as with Norway and Iceland by supplementing provisions in existing legal instruments and facilitating their application. The State receiving a request must in principle comply with the formalities and procedures indicated by the requesting State.[86]

86 See Council Act of 19 May 2000 (2000/C 197/01) establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union.

Crime-type or measure	**Council of Europe Cybercrime Convention**	**EU instruments**
Criminal law		
Computer-crimes	Art. 2 – 6	Framework Decision (FD) on Attacks against information systems
Computer-related crimes	Art. 7-8	FD on fraud and counterfeiting of non-cash means of payment
Content-related crimes	Art. 9 on child pornography	FD on the sexual exploitation of children and child pornography
	Protocol on racism and xenophobia	FD on combating racism & xenophobia
Crimes against intellectual property rights	Art. 10	–
Criminal procedural law		
Ex post traffic data retention	Art. 16-17	MLA Convention of 2000, Art. 17-20, and Directive on traffic data retention
Real-time traffic data retention	Art. 20-21	MLA Convention of 2000, Art. 17-20
Ex ante traffic data retention	–	Directive on traffic data retention
Cooperation, mutual assistance		
Measures for rapid assistance	Art. 16-17, 19, 25-26, 33, etc.	MLA Convention 2000, Art. 6-7, etc.
Dual criminality	Art. 25	Restrictions on application of the principle in MLA Convention 2000, Art. 3, and other EU instruments.
Institutions for cooperation	24/7-network, Art. 35	24/7-network EUROPOL, EUROJUST, ENISA
Assymetric, state-organized or state-sponsored attacks on information infrastructure	–	Directive on European Critical Infrastructure

European initiatives, in the Council of Europe and the European Union, have succeeded in bringing the substantive criminal laws of the States therein closer together, so that sanctions are at the disposal of all European courts, or will hopefully be soon. Measures have also been taken to ensure more effective judicial and police cooperation between the European states. Most Council of Europe and EU actions were initially organized crime-driven, later measures factor in terrorism and even more recently threats to states more than to individuals. An area that the EU has yet to approach concerns the interface between criminal law and international law, that is activated by transnational attacks by states or state agents on another state's electronic infrastructure.

As it has been shown above, the EU's approach to creating legislation in the field of cybercrime has not followed the text of the Cyber crime Convention entirely. Thus the EU Member States face the challenge of two sets of regulations that they have to implement into national law, which do not overlap at all points. The challenge of harmonizing legislation between the Member States of the European Union is not specific to cyber crime legislation. Even for a more "kinetic" type of crime such as road-traffic violations, and the ensuing disqualification of offenders, the EU has been struggling for well over a decade to establish an effective pan-European system.[87] Due to the borderless nature of cybercrime, as well as the exponential growth of usage of IT-services, it is essential that the definitions used by national legislation among Member States are compatible so that cybercrime can be fought in an efficient and timely manner.

The time it takes Member States to implement harmonized EU legislation is a challenge in itself and is exemplified by the transposition of the *Framework Directive on attacks against information system*s into national law. Article 12(2) of the Framework Decision obliges Member States to transmit, to the Council Secretariat and the Commission, information on how the provisions of the Framework Decisions have been transposed into national law. This was to be done, two years after the entry into force of the Framework Decision, that is 16 March 2007. To quote the Commission: "By that date, only one State (Sweden) had transmitted a national text to the Commission and even that was incomplete". More than a year later, the Commission was still missing replies from Malta, Poland, Slovakia, and Spain, while Ireland, Greece and the UK had replied that they had not implemented the Framework Decision's provisions. In other words, three years after the entry into force of the Framework Decision, one fourth of the EU Member States had not implemented the Framework Decision or provided enough information to decide whether or how it had been implemented. The Commission's report on the implementation of the Framework Decision highlights a misunderstanding regarding the phrase "cases whish are not minor" which is an optional clause in several articles and which was used by several Member States. It does, however, conclude by stating that "Significant progress has been made in practically all the 20 Member States

87 *See* "europea.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l33065_en.htm2".

assessed in this report, where the level of implementation has been found to be relatively good".[88]

With the ever changing modus operandi of cyber-criminals the harmonizational challenges of the EU and its Member States will surely remain a reality in the coming decade. With the more robust legislation mechanisms under the Lisbon Treaty, however, there is reason to be optimistic that the EU will be in a better position than ever to face the challenge.

88 *See* COM(2008) 448 final 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 pp. 2-10.