The European legal framework on cybercrime: striving for an effective implementation

Calderoni, Francesco

Postprint / Postprint
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law and Social Change*, *54*(5), 339-357. https://doi.org/10.1007/s10611-010-9261-6

The European legal framework on cybercrime: striving for an effective implementation.

ABSTRACT

This article analyzes the European legal framework on cybercrime. Initially, it argues the challenges of cybercrime to traditional criminal justice systems. Subsequently, it focuses on the criminal law framework on cybercrime with a mainly European perspective. The European legal framework provides a three-path solution: the reduction of frictions among national legislations, the introduction of new investigative powers and the facilitation of international cooperation. The article presents and discusses each solution. Further, it argues that the effective implementation of the main legal instruments does not seem to depend on the legal enforceability of these international measures. Contrarily, other, non legal, factors such as national security, politics, the economy and the public opinion appear to stimulate the spontaneous implementation of the European legal framework. In this context, the added value of the EU action is rather low, although the Treaty of Lisbon and the Stockholm Programme may improve this situation in the long term.

INTRODUCTION

This article provides an overall picture of the European legal framework concerned with the repression of cybercrime. This matter has been subject to intervention by a number of international institutions worldwide, such as the United Nations, the G8, the Organization for Economic Co-operation and Development (OECD), the Commonwealth, the Council of Europe (CoE) and the European Union (EU).[1] From a European perspective, two international agreements are of particular relevance both for their (mainly) European focus and their legal effect: the 2001 Council of Europe Convention on Cybercrime (henceforth the CoE Convention) and the 2005 European Union Framework Decision on attacks against information systems (henceforth the FD) (Council of Europe, 2001; European Union, 2005).[2] Cybercrime provokes such high international concern

[1] For detailed information about the initiatives of international institutions and organizations on cybercrime, see International Telecommunication Union, (2008), Schjolberg (2008) and Li (2007).

[2] The Council of Europe is an international organization, established in 1949 and composed now by 47 member states, with the aim of promoting democracy and protecting human rights and the rule of law in Europe. The European Union is an international organization founded in 1993 with the aim of extending the economic cooperation established under the European Economic Community (founded in 1957). It has 27 Member States (MSs). On 1 December 2009 a new treaty, the Treaty of Lisbon, has entered into force. The new treaty has brought significant changes to the EU and in particular to the area of freedom security and justice (AFSJ), the EU sector relevant for the cooperation in criminal matters (see infra section 5). The Treaty of Lisbon has reframed the European treaties into a Treaty on European Union (TEU) and a Treaty on the Functioning of the European Union (TFEU). Until the entry into force of the Treaty of Lisbon, it has

because it has intrinsic characteristics which hamper its repression, and which are briefly described in section 1. In response to these distinctive features of cybercrime, the two above-mentioned legal instruments provide a three-path solution: the reduction of frictions among national legislations (section 2); the introduction of new investigative powers, as summarized in section 3; and the improvement of international cooperation (section 4). This paper presents the main provisions and criticisms relating to each path and concludes by discussing the problems relating to the implementation and effectiveness of the instruments (section 5).

1. CYBERCRIME AND CRIMINAL JUSTICE SYSTEMS

Cybercrime raises several challenges for traditional criminal law and the criminal justice system in general. The first challenge concerns its definition (McQuade III, 2006, 16-17; Marler, 2002, 185; Gordon & Ford, 2006). The fashionable label 'cybercrime' in fact covers different types of offences (Council of Europe, 2005, 87; Smith, Grabosky & Urbas, 2004, 7). This article follows the typologies of the CoE Convention. This conceptual framework has significantly influenced international and national legislation on cybercrime, including the EU policies. Therefore, it is useful in the analysis of the European legal framework on cybercrime. Furthermore, it allows to distinguish between cybercrimes where information systems are targets or instruments for crime (International Telecommunication Union, 2009, 18-19). Accordingly, the first group of cybercrimes comprises offences against the confidentiality, integrity and availability of data and information systems (so called CIA offences) (McQuade III, 2006, 39). An example of these crimes is illegal access to a person's computer in order to collect or delete data. The second group are computer-related offences, where a computer is an instrument, though not an essential one, for the commission of a crime. An example is a credit card fraud perpetrated through a purposely designed internet site. A third group consists of content-related offences, such as child pornography and acts of a racist and xenophobic nature; these behaviours fall within the category of cybercrime when they are committed by means of a computer system. A fourth group concerns the infringement of copyright, as in the unauthorized copying and sale of computer software (Council of Europe, 2005, 87).

A second challenge is that Information and Communication Technology (ICT) is complex and frequently unfamiliar to the traditional criminal justice world. Dealing with crimes involving these devices requires well-trained personnel in the investigation phase, during prosecution, and in courts. Technological and computer knowledge are somewhat alien to law enforcement and legal cultures, and states need to invest in training and education (Smith et al., 2004, 152). Since ICT constitute a rapidly growing and changing sector, operators must constantly retrain so that they are prepared for the new techniques and new *modi operandi* made possible by the advance of ICT (Chaikin, 2006, 12). Again, this flexible and constant approach may be unfamiliar to many criminal justice operators (Lewis, 2006, 1; Downing, 2005, 710).

---

been common to refer to the EU as to a structure with three pillars. These were the European Community (first pillar, regulated by the Treaty establishing the European Community (TEC)), the Common Foreign and Security Policy (second pillar) and the Police and Judicial Co-operation in Criminal Matters, formerly Justice and Home Affairs until the Treaty of Amsterdam, entered into force in 1999 (third pillar) (both regulated by the former Treaty on European Union (TEU)). Since the Treaty of Amsterdam, the objective of the III pillar has been the establishment of an AFSJ through police cooperation, judicial cooperation and approximation of legislation (Articles 2 and 29 of the former TEU).

As a third challenge, many cybercrimes occur in virtual environments like mobile phone channels or the internet. This feature frequently clashes with the main operational criteria of the criminal justice systems, namely sovereignty and the territoriality principle. The virtual nature of many cybercrimes requires countries to establish clear rules on a legal system's jurisdiction over these offences (Brenner & Clarke, 2005, 666; Downing, 2005, 719; Miquelon-Weismann, 2005, 346; Weber, 2003, 426). Furthermore, these crimes frequently occur in different places, which may be under the jurisdictions of different countries. Consequently, there is a strong need for clear norms setting the priorities and competences of each country involved (Smith et al., 2004, 48; Brenner, 2006, 189-193; Csonka, 2004, 6-7).

The fourth challenge is that the world of ICT moves at a pace different from that of physical world. Crimes occur in a fraction of a second and may spread with astonishing speed (Brenner & Clarke, 2005, 666; Csonka, 2004, 13). Additionally, evidence of cybercrime frequently consists of digital information, which is ephemeral by nature and can be altered or deleted. Law enforcement agencies must therefore take rapid action and be able to collect and preserve digital evidence for use in criminal proceedings (Chaikin, 2006; Csonka, 2004, 8-9).

If criminal justice systems are to deal effectively with these problems relating to the repression of cybercrime, they must update their legislation and law enforcement systems where these are unable to cope with investigation and prosecution of the phenomenon. The above mentioned international agreements, the CoE Convention and the FD, seek to resolve these issues.[3] Their combined provisions constitute a three-path approach the reduction of frictions among national criminal laws; the provision of new investigative tools; and the improvement of

[3] Although the two legal instruments share a common goal, they differ in their nature and scope. The CoE Convention is an international treaty. In order for a treaty to become binding, a state must show its intention to be bound by it (becoming a party to the treaty) and the treaty must have entered into force according to the provisions set by the treaty itself (e.g. deadline, minimum number of adhesions). The treaty only binds the nations that have become a Party to it (Kierkegaard, 2007, 20-22). The CoE Convention has been adopted in Budapest on 23 November 2001. Although drafted by the CoE, the Convention is open for accession to non-CoE countries. As to April 2010, 46 states have signed the CoE Convention. The Convention has entered into force for 29 countries, including the United States of America. Five additional countries have been invited to accede (Chile, Costa Rica, Dominican Republic, Mexico, Philippines). Some scholars recognize that the drafting process of the CoE Convention was "unusually open" (Lewis, 2006, 2; Downing, 2005, 711); others show opposite opinions, arguing that "the development of the convention has been secretive and characterised as lacking in public consultation on the cybercrime issues" (Kierkegaard, 2007, 22). Whatever the truth, the Convention has been partially amended in order to address some of the criticisms moved against the first drafts (Lewis, 2006, 3).

The FD is a legal instrument exclusive of the EU action in the III pillar. Its objective is the approximation of national legislations of EU MSs. According to Article 34, "framework decisions shall be binding upon the MSs as to the result to be achieved but shall leave to the national authorities the choice of form and methods". This obliges any EU MS to comply and implement EU Framework Decision within its legal system as an automatic consequence of being an EU MS (Mercado Kierkegaard, 2006, 382-383). FD may thus appear as powerful measures allowing to overcome the length and red tape involved in the process of entry into force of international treaties. However, the possibility to sanction an EU MS for a failure to implement and comply with a framework decision is rather theoretical than actual. This is because, in the framework of the III pillar, the European Commission did not have the power to bring a Member State before the European Court of Justice for failure to fulfil the obligations under a framework decisions, contrarily to what happens in the I pillar. Therefore, this power only rested within the action of other MSs, making this an unlikely and politically inconvenient possibility (Bernardi, 2007, 723). For the innovations of the Treaty of Lisbon on this issue, see infra (section 5).

international cooperation. The following sections summarize the main actions within each of these paths and briefly discuss criticisms and other issues arising from them.

2. REDUCING FRICTIONS: THE HARMONIZATION AND APPROXIMATION OF CYBERCRIME LEGISLATION

One major consequence of the virtual nature of many cybercrimes is that inconsistencies among criminal justice systems may hamper repression of the phenomenon. The perpetrator may be in a different jurisdiction from the victim, and the legal definitions of the criminal behaviour in the two legal systems may not match. Numerous difficulties may arise from this very simple situation. The country in which the perpetrator is present may not consider the conduct to be an offence. It may criminalize it, but as a minor offence punished with less than the minimum sanctions for international cooperation. Even if the penalty requirements for cooperation are present, this may not be possible because the offences do not fulfil the double criminality requirement (Smith et al., 2004, 86; Flanagan, 2005, 108). Especially for cybercrime, an excessively lenient criminal legislation or significant inconsistencies among national regulations may have detrimental effects. Criminals may fully exploit ICT and the virtual environment of the internet and focus their activities on the most tolerant legal systems and on the most vulnerable victims.

One solution in order to solve and prevent these problems is overcoming the frictions among national legislations dealing with cybercrime. The convergence of legislations among European (and other) countries may offer a technical solution to many difficulties related to the current framework of international cooperation (Vermeulen, 2002; Manacorda, 2005).

In this perspective, both the CoE Convention and the FD contain criminalization requirements. Both instruments share a common core constituted by three criminal offences concerning the confidentiality, integrity and availability of computer data and systems. The first is the illegal access (Art. 2 of the CoE Convention and Art. 2 of the FD) consisting of intentionally accessing a computer system without the right to do so. Both agreements allow states to require the infringement of a security measure and exclude minor cases (Chaikin, 2006, 15-16). These options should grant some flexibility to national legal systems. They also take into account the trade-off between over-criminalization (thus seeking to punish all illegal accesses) and the specific selection of criminal illegal accesses (thus stimulating citizens to protect computer data and systems). Critics have argued that this may hinder achievement of the objective of harmonizing national laws (Flanagan, 2005, 110; Mercado Kierkegaard, 2006, 386). Further, scholars suggest that the requirement of the infringement of a security measure is probably the most sensible and efficient approach to the criminalization of illegal access (Brenner & Clarke, 2005, 659; Kerr, 2003, 1599-1600). The possibility of limiting the scope of the criminalization of illegal access provided by the CoE Convention and the FD could hinder international cooperation for those countries that chose to have broader illegal access offences (Flanagan, 2005, 110). However, in the long term these problems may end up by incentivizing countries to restrict illegal access offences, so that they adhere to the most efficient models envisaged by scientific research (Brenner & Clarke, 2005).

The second common offence is system interference (Art. 5 of the CoE Convention and Art. 3 of the FD). This occurs when someone intentionally hinders or interrupts the functioning of a computer by the inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible of computer data. The third common offence is data interference (Art. 4 of the CoE Convention and Art. 4 of the FD).[4] It consists in a broad variety of behaviours (damaging, deletion, deterioration, alteration, suppression) affecting computer data, and which are illicit when committed without right and intentionally (Chaikin, 2006, 16). Both offences must be enacted without right and should be serious (CoE Convention and FD) or at least comprise "cases which are not minor" (FD) (Chaikin, 2006, 17). Critics complained about the lack of definitions of notions such as "intent" and "serious hindering" (Mercado Kierkegaard, 2006, 386-387). The provision of stricter definitions of these deliberately broad concepts would probably have led to stronger reactions as to the identification and national origin of these definitions, giving rise to possible contrasts with different legal cultures.

Notwithstanding a number of criticisms, it seems that the definitions of the three core offences contained in the two international agreements largely correspond. Indeed, harmonization of criminal law should not aim at unification or exact correspondence of national legislation, but rather tackle frictions and inconsistencies among national laws (Calderoni, 2010, 2-4). This is likely to incentivize a European (and international) consensus on the definitions of these offences (Valeri, Somers, Robinson, Graux & Dumortier, 2006, 18-19). Further, it is likely to reduce loopholes and inconsistencies among national legislations.

Besides the above described offences, the CoE Convention covers several others corresponding to other types of cybercrime, such as illegal interception, misuse of devices, computer-related offences (forgery and fraud) and content-related offences (child pornography, infringements of copyright and related rights) (Downing, 2005).[5] The FD instead provides for the criminalization of instigation, aiding and abetting and attempt to commit one of the three offences described above. It requires a minimum penalty of at least between one and three years of maximum imprisonment for illegal system interference and illegal data interference. It provides for aggravating circumstances (at least between two and five years of maximum imprisonment) for offences committed within the framework of a criminal organization or offences "that caused serious damages or has affected essential interests".

The European action against cybercrime is not limited to criminalization. It also introduces new investigative powers for the law enforcement agencies.

[4] According to Article 1 b of the CoE Convention (and Article 1 b of the FD), the term 'computer data' denotes "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

[5] It is necessary to recall the Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. The CoE Convention does not include offences covering these acts. This is because the drafters could not find an agreement on the criminalization of these behaviours (Council of Europe, 2003). Consequently, the drafters opted for an additional Protocol, which was signed on 28 January 2003 and entered into force, after the fifth ratification, on 1 March 2006. To date, 34 countries have signed the protocol, but only 17 have ratified it. The main problem related to the Protocol is its possible conflict with the freedom of expression (U.S. Department of Justice).

3. PROVIDING LAW ENFORCEMENT WITH THE TOOLS: NEW INVESTIGATIVE MEASURES

Articles 14-21 of the CoE Convention require the Parties to introduce new investigative powers. The main consideration in this regard is that the new procedural rules have a broad application. They apply not only to offences envisaged by the first section of the agreement, but also to "other criminal offences committed by means of a computer system" (Article 14, para 2 b), and even to the "collection of evidence in electronic form" for any crime (Article 14 para 2 c). Hence, the measures of this section significantly affect the criminal procedure systems of the Parties. States must adopt laws allowing the activities stated by the CoE Convention, unless their national legislation already complies with it. The scope of application of these measures demonstrates that the need to modernize investigative tools extends beyond the fight against cybercrime. It encompasses all criminal activities, which, just like legal ones, increasingly use and benefit of ICT. There is no need for examples to demonstrate that the seizure and analysis of a suspect's computer or mobile phone may contribute significantly to ascertaining his/her innocence or guilt (Miquelon-Weismann, 2005, 342-343).

The first investigative measure set out by the CoE Convention is the expedited preservation of stored computer data. It enables the authorities to order or obtain the preservation of specific digital information already stored. It allows the freezing for up to ninety days of a defined quantity of data of possible relevance to a criminal investigation in order to prevent its deletion and alteration. This should enable the authorities to obtain the authorizations required by national law before proceeding with seizure, search and other ways to obtain data disclosure (Downing, 2005, 757-758). Furthermore, specific rules provide for the rapid availability of traffic data.[6] Traffic data may be crucial for continuing criminal investigations while waiting for authorizations to disclosure. Article 17, para 1 a, allows to obtain traffic data "regardless of whether one or more service providers were involved". State Parties are thus entitled to regulate the matter specifically, finding the solution that best suits their system (Council of Europe, 2001, 28). Article 17, para 2 b, obliges the person served with a preservation order to disclose to the authorities a "sufficient amount of traffic data" to track the communication so that the perpetrator can be identified.

The second measure is the 'production order'. This may oblige a) a person to submit specified stored information in his/her possession or control and b) a service provider to disclose subscriber information in the provider's possession or control. Subscriber information comprises the type of communication used, technical provisions, period of service (Art. 18, para 3 a), and other information available to the provider on the basis of the contract or agreement with the user (identity, address, contacts, payment information, etc.) (Miquelon-Weismann, 2005, 341-342).

The third measure concerns the search and seizure of stored computer data. It allows the authorities to search a computer or other data storage device. Article 19, para 2, also allows for the automatic extension of the search to data stored in other computers accessible from the one being searched. Additionally, it enables to seize, copy, preserve and remove or make inaccessible the

[6] According to Article 1 d of the CoE Convention, traffic data are "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service".

data. In order to speed up these activities, the authorities can order any person who has knowledge of the system, such as system administrators, to assist with the search.

The fourth and fifth measures concern the real-time collection of computer data. Article 20 deals with traffic data and Article 21 with content data. These norms allow the authorities to intercept and/or order a service provider to assist them, or even to collect traffic data and content data directly. These measures provide for the interception of personal communication, a significant interference with the right to privacy and the right to communicate. They should apply only for serious crimes. Article 21 leaves to domestic law to select such offences. This is a mandatory selection for collection of the content of communications. It is only optional for the collection of traffic data. A Party may limit the collection of traffic data to a range of crimes. This list cannot be more restricted than the list of serious offences allowing interception of content data.

The above described measures provide law enforcement authorities with a valuable ICT toolbox of investigative measures. Article 15 provides guarantees for privacy and freedoms. This provision cites the protection of human rights and liberties and expressly requires that investigative powers respect the proportionality principle (Council of Europe, 2001, 24). Para 2 of Article 15 lists possible safeguards national legislation may provide for, and particularly "judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure". In the letter of the CoE Convention it is evident a preference for a national approach. Domestic legislation shall establish both the conditions for exercising the above-described investigative powers and the safeguards against them. This relativism has been strongly criticized for failing to impose adequate procedural and substantial constraints on law enforcement agencies, thus possibly infringing citizens' rights and freedoms such as privacy rights and the privilege against self-incrimination (Archick, 2006, 4; Marler, 2002, 204-205; Mercado Kierkegaard, 2006, 383-384; Kierkegaard, 2007, 22-23; Miquelon-Weismann, 2005, 337-340). However, several scholars have argued that the CoE Convention respects human rights and freedoms, and that concerns about these issues should not be overemphasized (Marler, 2002, 206-211; Lewis, 2006, 4; Keyser, 2003, 324-325; Li, 2007; Weber, 2003, 445; Archick, 2006, 4; Lemos, 2001). To be sure, human rights and freedoms should be important priorities in drafting new criminal (international) legislation. The Council of Europe and the European Union both have specific instruments and procedures to protect human right and freedoms.[7] The implementation of the new investigative measures by EU and CoE members is not an exception to this. In this perspective, it seems unlikely that the CoE Convention will significantly endanger human rights and freedoms in most European countries. Not surprisingly, scholars from non EU and non CoE countries were the most sceptic about this. Nevertheless, the relativist approach of the Convention appears justified not only because of the relatively high level of protection of human right in Europe. It appears a wise choice for extending the global adoption of the CoE

[7] The 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (also known as European Convention on Human Rights) was the first treaty of the Council of Europe. All new CoE members must ratify the Convention. The Convention sets up a number of basic rights and freedoms and creates the European Court of Human Rights, sitting in Strasbourg, France. The Court judges cases of infringement of the right enshrined in the Convention and is entitled to issue judgements which are binding for the concerned states. Within the European Union, the Charter of Fundamental Rights of the European Union sets up the rights of every EU citizen. The Charter was signed in 2000, but it has legal Since the entry into force of the Treaty of Lisbon, the Charter has the same legal value as the EU Treaties. Consequently, all EU MSs and institutions must respect the Charter. Since the entry into force of the Treaty of Lisbon, the EU is enabled to accede to the European Convention on Human Rights.

Convention. A treaty with stricter requirements as to guarantees would have discouraged its adoption by states, which are likely to be reluctant to introduce safeguards additional or different to the ones already provided by their national legislation. Consequently, stricter requirements probably would have jeopardized the main objective of the CoE Convention: the facilitation of international cooperation.

4. FACILITATING COOPERATION: MINIMUM RULES IN A MORE COMPLEX FRAMEWORK

The CoE Convention also includes several norms intended to facilitate international cooperation and to improve the repression of transnational cybercrime. Notwithstanding criticisms and problems of implementation (discussed below), the part of the CoE Convention on international cooperation is the core of the new treaty. It is widely viewed as the most important element because it enables expeditious actions in a sector where these are necessary, owing to the speed and changeability of cybercrime (Csonka, 2004, 26-27).

Article 22 sets out rules concerning jurisdiction. Paragraph 4 explicitly excludes that these norms may conflict with a Party's jurisdiction on an offence established by its domestic law. Parties shall establish their jurisdiction over the offences defined by the CoE Convention when these occur in their territory. Additionally, they may establish their jurisdiction on offences committed on board a ship or an aircraft registered therein, by one of their nationals if the offence is punishable under criminal law in the territory where it is committed or is committed outside the jurisdiction of any state. Furthermore, Parties must establish their jurisdiction on extraditable offences in cases where they refuse to extradite the suspect on the basis of his or her nationality and the person is present on their territory, thus implementing the principle of *aut dedere aut iudicare* (hand over or try) (Council of Europe, 2001, 41). These provisions have been criticized for failing to address the most critical issue of jurisdiction over cybercrimes, i.e. positive jurisdictional conflicts (when more than one country claims to have jurisdiction over a crime (Brenner, 2006)). Conflicts of this kind are frequent in the case of cybercrimes, since computers and networks activities are rarely subject to physical and spatial restrictions. The CoE Convention only provides for a possibility of consultation among state parties in order to determine "the most appropriate jurisdiction for prosecution" (Article 22 para 5). A merely possible mechanism of this kind is not likely to do much to solve positive conflicts (Miquelon-Weismann, 2005, 347). Furthermore, the focus on prosecution may lead to a prioritizing of law enforcement over the suspect's rights and freedoms (Kierkegaard, 2007, 25). Article 10 para 4 of FD supplements this shortcoming by requiring mandatory consultation among the MSs concerned, centralization of proceedings in one country (as far as possible) and providing three criteria for determination of the jurisdiction: place of commission of the offence, offender's nationality, and place of apprehension of the offender.

In regard to extradition, Article 24 obliges Parties to consider the offences established by the CoE Convention, when punished with at least one year of maximum imprisonment, as extraditable offences under existing or future extradition treaties concluded between or among them. If no agreement exists between Parties, the Convention should be the legal basis for granting extradition. The Parties are required to implement the *aut dedere aut iudicare* principle for the

offences established by the CoE Convention (Council of Europe, 2001, 43), and they must provide the contact addresses of the authorities responsible for making or receiving extradition requests.

Several provisions deal with mutual legal assistance. These concern not only the investigation and prosecution of crimes related to computer systems and data, but also the collection of evidence in digital form. These provisions are thus likely to apply to a wide variety of criminal proceedings dealing with cybercrimes and ordinary crimes (Council of Europe, 2001, 44).

The CoE Convention has a subsidiary function. On the one hand, it provides a framework for mutual assistance when no other agreement exists between the requesting and requested Parties. States must designate a central authority responsible for such requests. National authorities must execute the requests according to procedures specified by the requesting Party.[8] In cases of urgency, the requesting Party can sent requests directly to judicial authorities. The competent authorities are free to directly exchange requests not involving coercive action.

On the other hand, other applicable treaties and national laws should have the priority (Article 27 of the CoE Convention). This allows mutual legal assistance operators to use more familiar instruments, such as, for example, the European Convention on Mutual Assistance in Criminal Matters and its Protocol or the EU Convention on Mutual Assistance in Criminal Matters. This rule is only a general principle and has several exceptions. In particular, Parties shall implement to the full extent the provisions on mutual assistance for the specific investigative actions provided by the CoE Convention (see above, section 2). For these measures, the Convention represents the legal basis for requests of mutual assistance in cases where an agreement is a condition for their fulfilment. Requests for the expedited preservation of stored computer data can be fulfilled without requiring dual criminality (Article 29 paragraph 3), unless a Party so reserves. In case of an expedited preservation, the requested Party must also disclose to the requesting one any service provider involved and the path of the communication. Furthermore, in case of a request of search or seizure of data, Article 31 paragraph 3 requires expedited response when there are grounds to presume that data are particularly vulnerable or other treaties or agreements provide for an expedited procedure.

Mutual legal assistance provisions of the CoE Convention have received criticisms for not establishing adequate guarantees for due process and human rights. In particular, strong criticisms pointed out the lack of dual criminality requirements for granting assistance (Lemos, 2001; Kierkegaard, 2007, 26). In fact, these criticisms seem to be caused by the CoE Convention's above-mentioned relativism as to guarantees and safeguards, and by misunderstandings as to traditional mechanisms of mutual legal assistance. According to Article 25 para 4 of the CoE Convention "mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation". This means that each country will continue to apply its traditional approach to assistance requests made by other Parties. Therefore, dual criminality will apply whenever national laws or other applicable international agreement provide for it. Indeed, in regard to dual criminality, the CoE Convention does not comprise innovations in comparison with other important international mutual assistance treaties, such as the 1959 European Convention on Mutual Assistance in Criminal Matters (Article 5 para 1 a) and the 2001 United Nations

[8] Except when this is incompatible with the law of the requested Party and when refusals are based on political offence or *ordre public* reasons.

Convention on Transnational Organized Crime (Article 18 para 9). The only exception to the possibility to require dual criminality is, as already mentioned, provided by Article 29 para 3 for requests of expedited preservation of computer data for offences established in accordance with Articles 2-11 of the CoE Convention. This provision has been based on the consideration that the requirement of dual criminality may hinder the effective prompt preservation of data and that dual criminality may be assumed for the offences provided by the first part of the Convention (Council of Europe, 2001, no. 285). This option seems wise, also in consideration that further requests of assistance relating to the preserved data may be subsequently subjected to dual criminality checks (Weber, 2003, 434).

Another important tool is the establishment of a network of national contact points for assistance and collection of evidence available on a 24/7 basis. The G8 meeting on 9-10 December 1997 firstly established the network. The 24/7 Network is open to other countries, and the Council of the European Union has recommended MSs to join the network (European Union, 2001). To date, approximately 55 countries have done so. [9] Further, the lists of G8 and CoE national contact points are undergoing a process of consolidation (Polakiewicz, 2010). The CoE Convention places an obligation upon Parties to designate and adequately equip such national contact points. This should increase the number of countries adhering to the 24/7 Network (Csonka, 2004, 27-28). Further, the FD endorses the initiative, binding all EU MSs to establish a national contact point (Article 11 of the FD).

The mechanisms of cooperation described above are likely to represent a minimum threshold. This is a consequence of the above-mentioned subsidiary nature of the CoE Convention, but most of all of the higher level of mutual cooperation established within the framework of EU legislation. In this regard, several measures have been adopted which directly or indirectly concern the repression of cybercrime. They include agreements on mutual assistance in criminal matters, such as the 2000 EU Convention on mutual assistance in criminal matters and its 2001 Protocol. The most innovative instruments in the EU context include measures implementing the principle of mutual recognition in criminal matters. Since the 1999 Tampere European Council, this principle is the cornerstone of judicial cooperation in the EU. Based on this principle, a series of framework decisions has introduced a significantly greater level of cooperation on criminal matters. The best-known of these measures are the European Arrest Warrant, and mutual recognition of freezing orders on property or evidence and of confiscation orders.[10] More recently, new measures have further increased the application mutual recognition.[11] Remarkably, the above-mentioned instruments include computer-related crimes within their range of application. However, as already pointed out in the literature, the famous 32-item list of crimes not requiring

[9] Information provided by e-mail by Albert C. Rees Jr,, Computer Crime & Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, 2 April 2010.

[10] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, (2002/584/JHA), OJ L 190 of 18/7/2002; Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, OJ L 196 of 2/8/2003; Council Framework Decision 2003/577/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders, OJ L 328 of 24/11/2006.

[11] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350 of 30.12.2008, 60–71; Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350 of 30.12.2008, p. 72–92.

the application of the principle of double criminality raises doubts concerning its precision in defining the conducts concerned (Weyembergh, 2005, 1582; Peers, 2004; Manacorda, 2005). Indeed, the reference to "computer-related" crimes is ambiguous, because the notion is broadly criminological rather than denoting specific offences. This is all the more significant if we consider that explicit reference to the provisions of the FD or of the CoE Convention could easily have resolved this issue, since the offences therein established are much more clearly defined. This concern is important for at least one Member State. In relation to the Framework Decision on the European Evidence Warrant (EEW), according to Article 23 para 4, Germany may issue a declaration subordinating the implementation of the EEW to verification of double criminality for a series of crimes, including computer-related ones (Council of the European Union, 2007, 26-39). Accordingly, Germany has declared that it may submit requests of EEWs requiring search and seizures to double criminality, unless the issuing authorities declares that the offence in question matches the CIA offences of the CoE Convention or the offences defined by the FD (European Union, 2008, 92).

The CoE Convention and the EU cooperation framework are important achievements. However, their establishment is only a first step towards effective action against cybercrime. The following step is the implementation of international or European regulations into national legislations.

5. STRIVING FOR EFFECTIVE IMPLEMENTATION: UNCERTAIN PERSPECTIVES

The mechanisms of international law are slow and this may become a serious issue when addressing such a constantly-changing phenomenon (Csonka, 2004, 10-11). Indeed, the approval of international agreements is far from providing *per se* a common framework for the international repression of cybercrime. International law requires that states ratify treaties and implement them into national legislation. The implementation phase is of crucial importance for establishing a common approach to the issue of cybercrime (Miquelon-Weismann, 2005, 353).

With regard to the CoE Convention, its global reach appears difficult. Indeed, in order to prevent safe havens for cybercriminals, the Convention should be adopted by far more countries than the current signatories/Parties (Archick, 2006, 3; Weber, 2003, 443-444; Li, 2007). Remarkably, some of the most important Members of the Council of Europe or signatory Parties in terms of population and GDP have not yet ratified or acceded to the treaty. They include Russia and Turkey (which did not even sign the treaty) as well as Poland, Spain, the United Kingdom, Canada and Japan (which have not yet ratified it). This points out the difficulties in the implementation of the CoE Convention even within the group of countries which are its main targets, at least in theory. Furthermore, in a global perspective, the current level of implementation is even lower. The majority of the world countries with the highest number of internet users have not signed/ratified the Convention.[12] Even if the pace of ratification/accession is rather rapid compared with other international treaties, the current situation exhibits several shortcomings in

[12] Among the first 10 countries per internet users only 3 countries have ratified the Convention (United States, Germany and France). United Kingdom and Japan have only signed the treaty, while China, Brazil, India, Russia and South Korea have not even signed it (for further information, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG).

the implementation of the international framework on cybercrime. Although the Convention is already in force for more than 25 countries, and is potentially open to all states, full implementation of its content at global level – which is its ultimate ambition – still seems a long way off. Notwithstanding its uncertain global reach, the CoE Convention shows a remarkable indirect impact. Scholars recognize that it is a worldwide benchmark for cybercrime legislation, to which the FD itself and other instruments have conformed (Flanagan, 2005, 109).[13] Several institutions and countries outside Europe took inspiration from the Convention in drafting their regulations (International Telecommunication Union, 2008; Gercke, 2009, 416; Picotti and Salvadori, 2008, 4).[14] This element highlights that the mechanisms of implementation and harmonization go well beyond a strictly legal approach. Countries with no legal obligations to implement any international instrument have spontaneously drafted their national legislation in coherence with the provisions of the CoE Convention. If the legal (or "direct") implementation of the CoE Convention appears difficult, its content represents a model for international organizations and countries around the world ("indirect" impact or implementation).

A further issue related to the existence of the Convention is that it has halted or hindered further alternative solutions. Indeed, the possibility of providing the world with better international legal instruments may be impeded if not thwarted by the entry into force of the Convention, owing to the lengthiness of negotiations, the need to reach consensus, and procedures for signature and ratification (Weber, 2003, 443; Li, 2007). In this perspective, the strict adherence of other international instruments to the Coe Convention may have a double effect: on one side, it stimulates the implementation of the international rules; on the other side, it consolidates a core of minimum regulations, preventing further evolutions or developments. In the light of the current situation, it is unlikely that any important international organization (e.g. the United Nations) will ever attempt to depart from the CoE Convention to achieve a better legal framework on cybercrime. More probably, further international action will follow or build upon the basis of the CoE Convention.

With regard to the FD, the deadline for its implementation by the MSs was 27 March 2007. The Council should have assessed the level of implementation of the FD by 16 September 2007. Only on 14 July 2008 did the Commission issue an evaluation report on implementation of the FD (European Commission, 2008). The report stated that by the deadline date for implementation, only Sweden had transmitted an (incomplete) document on its implementation measures. By June 2008, only 23 out of 27 MSs had informed the Commission and 3 of them admitted they were still implementing the FD provisions into national law. Consequently, the Commission performed its evaluation only on 20 MSs out of 27 (European Commission, 2008, 2-3).

The Commission based its report on information and documents provided by EU MSs. This is a serious methodological obstacle to any proper assessment.[15] Indeed, it allows assessment only

[13] See, for example, the Commonwealth's Model Law on Computer and Computer Related Crime which has been expressly drafted to comply with the CoE Convention (Schjolberg, 2008, 13; Li, 2007) and may potentially influence the legislation of more than 50 countries.

[14] In a recent Conference Cooperation against Cybercrime hosted by the CoE in Strasbourg (23-25 March 2010), the Head of Economic Crime Division (Directorate General of Human Rights and Legal Affairs) of the CoE stated that the convention is a guideline, reference standard or model law for more than 100 countries (Seger, 2010).

[15] Although this is not the aim of this paper, criticisms to the harmonization and approximation processes within the III pillar of the EU have been heavy (for further discussion and references, see

of the legislation of the MSs that have provided information to the Commission. Furthermore, it implies an observation bias, since the Commission's analysis appears to be restricted to the documents provided by MSs, which are very likely to play down problems and inconsistencies in their implementation. Notwithstanding these problems, the Commission could not find a provision of the FD that all 20 MSs providing it with information have fully implemented. Compliance rates vary from 12 (in relation to liability of legal persons) to 19 (in relation to illegal data interference) out of 20 respondents. Again, this synthetic information on the implementation of the FD at the EU provides insight into the difficulties of European legal efforts to harmonize criminal legislation. The implementation of a brief though complex measure has required about 50% more time than expected. It is clear that even in a closely connected community such as the EU the actual implementation of the common measures shows significant problems. The fact that the CoE Convention already included most of the common measures further reinforces this impression.

In the light of these considerations, the implementation of the European (and global) legal framework on cybercrime appears a very complex task. The mechanisms of international law and European law (at least under the old institutional framework of the III pillar) appear largely ineffective. The scarce implementation of the CoE Convention and of the FD by the members of the CoE and EU respectively are a striking example. From this it may be obvious to argue in favour of more strict legal tools to evaluate, control and sanction the level of implementation, both at the level of international law and European law. However, these tools have been discussed for years and in several sectors other than cybercrime. The relatively successful indirect implementation of the CoE Convention and its influence outside the boundaries of the signatories Parties argue in favour of a different explanation.

The legal enforceability of international measures is only one factor for their actual implementation. Indeed, there are few cases where a country was forced to implement international measures against its own security interests, or against the will of its government, of its most powerful industries or of a strong public opinion. Security, politics, the economy and international reputation appear as much more determinant factors in this perspective. First, security is a key factor determining the implementation of international measures. The swift adoption of the Framework Decision on the European Arrest Warrant and of the Framework Decision on the fight against terrorism can be considered a reaction to the attacks of 11 September 2001. In this perspective, the international measures on cybercrime are increasingly connected to national security, especially in the protection of national infrastructures. Second, politics may influence the implementation of highly political international measures. The very well known problems in the adoption and implementation of international instruments against terrorism (at least until 2001) clearly reflect this point. The international measures on cybercrime (with the exception of the criminalization of act of racism and xenophobia through computer systems, prescribed by the Additional Protocol to the CoE Convention) appear less sensitive from a political point of view. Third, the national economy may influence the implementation of measures which may significantly affect some markets. The difficulties in the negotiations and ratification of international rules preventing climate change and reducing emissions provide an example of this influence. The international measures on cybercrime impact the business of internet service

(Calderoni, 2008)). Scholars have highlighted the lack of reliable assessment of the level of harmonization and approximation of EU MSs legislation (both before and after the implementation) (Manacorda, 2005, 72; Vermeulen, 2002, 71; van der Wilt, 2002, 84).

providers and other market operators, requesting data and information to be stored. However, the characteristics of these markets may favour the implementation of international standards. Indeed, thanks to ICT, companies can access several national markets with more ease than in other, more traditional, sectors (e.g. automobiles, food, steel). Indeed, ICT provides the possibility to reach markets worldwide. The availability of common rules and standards is important to create a level playing ground and open the way to new markets. Fourth, international reputation may influence the implementation of measures receiving great attention from the public opinion. This is the case for international agreements on, for example, nuclear energy, nuclear weapons, genocide and war crimes. Countries not implementing these measures are stigmatized and their international reputation is affected by this. The international measures on cybercrime do not seem to have a similar impact on the public opinion.

These elements contribute to a better explanation of the dynamics of the implementation of the current European framework on cybercrime. The legal obligations alone do not provide a sufficient explanation of the current level of implementation. Also countries with no legal obligations to implement the international measures are conforming their legislation to it. Security, political, economic and reputational factors are additional relevant variables. As discussed above, the international measures on cybercrime are increasingly linked to national security issues, do not entail excessively delicate political choices and may favour the establishment of a level playing ground for business. These factors may contribute to explain the indirect implementation of the content of the CoE Convention and the FD. For example, developing countries with big internal markets may not implement international standards to protect or favour national companies against foreign competitors (this may contribute to explain the current situation of China, India and Brazil). On the opposite, developed countries may need to show to their public opinion that something is moving in the fight against cybercrime (this may explain the situation of the United States, France and Germany).

In this perspective, the added value of the EU action appears to be low. It does not provide an increased enforceability of the international measures and does not appear to stimulate the MSs from the point of view of national security, politics, the economy or the public opinion. As a result, the FD does not depart significantly from the CoE Convention. As already discussed, this choice may have a double effect: stimulation of implementation, but also consolidation of existing (and possibly insufficient) rules. Concerning the first effect, the analysis of the implementation of FD has showed that EU MSs are not particularly diligent in its implementation. Furthermore, EU MSs are not more virtuous in the implementation of the CoE Convention than non EU countries (16 out of 27 EU MSs against 13 out of 29 non EU MSs have ratified the Convention). This reflects the well know difficulties to reach a common agreement among EU MSs which are at the same time partners in the international and European scene, but competitors in the markets. On one side, they share security and law enforcement objectives. On the other side, they strive to protect and favour their national economy. As a consequence, the second effect is prevailing. The EU has adhered to the CoE Convention standards, renouncing to provide clearer rules, better instruments and guarantees in the field of cybercrime. The main differences relate to the presence of different and faster tools of international cooperation (e.g. mutual recognition instruments, EU agencies and networks such as Europol, Eurojust, European Judicial Network). This rather weak approach is frequent in the EU action in criminal matters and can be encountered in other fields, such as organized crime (Calderoni, 2010, 41-45).

Some new elements may impact on this situation. They are the Treaty of Lisbon and the Stockholm Programme.

The Treaty of Lisbon entails the abolishment of the three pillar structure. The new institutional framework apply to economic policies as well as to the AFSJ. Concerning the latter, the role of many European institutions is strengthened. The Commission has a power of initiative, which is shared with a quarter of the MSs (Article 76 TFEU). The legal instruments (regulations and directives, terminology typical of the former first pillar) are adopted by the Council (deliberating with a qualified majority) and the European Parliament. The role of the European Court of Justice is extended. In particular, the Commission is entitled to bring the MSs before the Court for infringement on the obligations of the Treaties (Articles 258 and 259 TFEU).

These innovations may provide new opportunities for drafting more specific and innovative legal measures in the field of cybercrime. In particular, the Commission may open infringement procedures against MSs not implementing the FD and the EU could adopt a new directive providing more detailed definitions on some unclear points, as demanded by the literature (Picotti and Salvadori, 2008, 12). However, a transitional measure significantly waters down these possibilities for the acts adopted under the former III pillar. Article 10 of the Protocol (no 36) on Transitional Provisions "freezes" the new powers of the Commission and the Court concerning the infringement procedure for five years after the entry into force of the Treaty of Lisbon (unless the legal instruments are amended). The transitional measure reduces the impact of the new institutional framework, but may still allow the Commission to table a new proposal in the field of cybercrime. Even if this appears unlikely, by 1 December 2014 the infringement procedure will be applicable to the implementation of the FD. As discussed above, overestimating the enforceability of the obligations may be risky. However, this element may provide useful in stimulating the implementation by EU MSs. Indeed, the infringement procedure may bring political and public opinion reactions and ultimately shift the balance in favour of the implementation of the international measures on cybercrime.

The Stockholm Programme is the successor of The Hague Programme and provides the guidelines and policies for the development of the AFSJ for the period 2010-2014 (European Union, 2009). The Stockholm Programme deals with cybercrime, stressing the importance of the full implementation of the CoE Convention and promoting better cooperation and understanding in the field of cybercrime. This does not seem to promote radical changes to the above described situation. The Stockholm Programme highlights the importance of "effective implementation, enforcement and evaluation of existing instruments" (European Union, 2009, 6). Accordingly, the Programme provides the implementation of "objective and impartial" mechanisms of evaluation. The Commission should therefore table one or more proposals for the evaluation of the EU policies in the AFSJ. In this perspective, the judicial cooperation in criminal matters, which includes the FD, should be the first sector to be evaluated. Furthermore, the new evaluation should include an "efficient follow-up system" (European Union, 2009, 7). The improvement of the evaluation procedures may represent an important opportunity. Although frequently neglected in the literature, it may produce important advancements in the overall quality of EU legal measures and policies. Indeed, as discussed above, the current evaluation by the Commission is flawed and does not provide effective procedures to solve problematic issues. The possibility to establish effective and independent evaluation of the implementation of EU legal instruments may generate a reverse cascade effect. The Commission may have better arguments to support its infringement

procedures, MSs may pay more attention to the timely implementation of EU measures, the European institutions may be stimulated to draft legal instruments of better quality.

In conclusion the current level of implementation of the European legal framework on cybercrime shows several inconsistencies. These relate more likely to the security, political, economic and reputational factors in the implementation of international measures rather than to their legal enforceability. At present, the EU action does not show a significant added value. This is confirmed by the problems in the implementation of the FD. The Treaty of Lisbon and the Stockholm Programme will bring some changes to this situation, but they are not likely to entail radical changes in the short term. Nevertheless, it is possible that in the long run they will stimulate a better implementation of the legal framework on cybercrime. Given the fast-changing nature of cybercrime, it is legitimate to wonder whether the current European legal framework will still be of any relevance once these changes will eventually become applicable.

6. CONCLUSIONS

Cybercrime poses important challenges to the European criminal justice systems. The above-described three-path approach is a significant endeavour to improve the European (and international) repression of cybercrime. Firstly, it introduces new tools for investigation of these crimes. Secondly, it harmonizes the national definitions of several computer-related offences. Thirdly, it provides a minimum framework for international cooperation on criminal matters. The legal framework provided by the CoE Convention has been generally considered a significant step forward in the international response to cybercrime (Li, 2007; Weber, 2003, 445; Flanagan, 2005, 116; Lewis, 2006, 5; Downing, 2005, 761; Marler, 2002; Schjolberg, 2008, 11). As highlighted above, the European and international legal framework set by the CoE Convention and the FD has not been exempt from criticisms. Some of such criticisms may have been due to a misunderstanding of the general functioning of international cooperation in criminal matters or important concern for human rights and freedoms. However, the effectiveness and actual implementation of these international instruments remain the most critical issues. Indeed, their legal implementation shows some difficulties. However, the indirect implementation of these appears to be more successful. This supports the idea that non legal issues such as national security, politics, the economy and public opinion are more important factors than the legal enforceability in the implementation of these international instruments. Until present, the added value of the EU action in this sector appears relatively low. The Treaty of Lisbon and the Stockholm Programme may improve this situation, but this should not be expected to happen in the short period.

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

REFERENCES CITED

Archick, Kristin. 2006. *Cybercrime: The Council of Europe Convention*. http://www.usembassy.it/pdf/other/RS21208.pdf. Updated September 28, 2006.

Bernardi, Alessandro. 2007. Le rôle du troisième pilier dans l'européanisation du droit pénal: Un bilan synthétique à la veille de la réforme des traitées. *Revue de Science Criminelle et de Droit Pénal Comparé,* 4: 713-37.

Brenner, Susan W. 2006. Cybercrime Jurisdiction. *Crime, Law and Social Change,* 46, no. 4-5: 189-206.

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

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

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

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

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

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

———. 2005. *Organised Crime in Europe: The Threat of Cybercrime.*, Situation Report 2004. Strasbourg: Council of Europe Publishing.

Council of the European Union. 2007. Doc. 9913/07 of 25 May 2007.

Csonka, Peter. 2004. The Council of Europe Convention on cyber-crime: A response to the challenge of the new age? In *Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatico*, ed. Giovanni Ilarda and Gianfranco Marullo, 3-29. Milano: Giuffrè.

Downing, Richard W. 2005. Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, 43, no. 3: 705-62.

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

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

———. 2005. *Council Framework Decision 2005/22/JHA of 24 February 2005 on attacks against information systems*, OJ L 69 of 16.3.2005.

———. 2008. *Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters*, OJ L 350, 30.12.2008.

Flanagan, anne. 2005. The law and computer crime: Reading the Script of Reform. *International Journal of Law and Information Technology*, 13, no. 1: 98-117.

Gercke, Marco. 2009. Europe's legal approaches to cybercrime. *ERA-Forum* 10, no. 3: 409-420.

Gordon, Sarah, and Richard Ford. 2006. On the definition and classification of cybercrime. *Journal in Computer Virology*, 2, no. 1: 13-20.

International Telecommunication Union. 2008. ITU Global Cybersecurity Agenda (GCA) - High-Level Experts Group (HLEG): Global Strategic Report. http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf. 23 february 2009.

———. 2009. Understanding Cybercrime: A Guide for Developing Countries. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Kerr, Orin S. 2003. Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes. *New York University Law Review*, 78, no. 5: 1596-668.

Keyser, Mike. 2003. The Council of Europe Convention on Cybercrime. *Journal of Transnational Law & Policy*, 12, no. 2: 287-326.

Kierkegaard, Sylvia. 2007. Cybercrime convention: Narrowing the cultural and privacy gap? *International Journal of Intercultural Information Management*, 1, no. 1: 17-32.

Lemos, Robert. 2001, June 22. International cybercrime treaty finalized. *CNET News* http://news.cnet.com/2100-1001-268894.html.

Lewis, James A. 2006. The Council of Europe Convention Entered into force January 2004. Http://www.csis.org/media/csis/pubs/060804_coecybercrime.pdf.

Li, Xingan. 2007. International Actions against Cybercrime: Netwroking Legal Systems in the Networked Crime Scene. *Webology*, 46, no. 3.

Manacorda, Stefano. 2005. Le mandat d'arrêt européen et l'harmonisation substantielle: Le rapprochement des incriminations. In *L'intégration pénale indirecte: Interactions entre droit pénal et coopération judiciaire au seins de l'Union européenne*, ed. Geneviève Giudicelli-Delage and Stefano Manacorda. Paris: Société de législation comparée.

Marler, Sara. 2002. The Convention on Cyber-Crime: Should the United States Ratify? *New England Law Review*, 37, no. 1: 183-219.

McQuade III, Samuel C. 2006. *Understanding and Managing Cybercrime*. Boston: Allyn and Bacon.

Mercado Kierkegaard, Sylvia. 2006. Here comes the 'cybernators!'. *Computer Law & Security Report*, 22, no. 5: 381-91.

Miquelon-Weismann, Miriam F. 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? *John Marshall Journal of Computer & Information Law*, 23, no. 2: 329-61.

Peers, Steve. 2004. Mutual recognition and criminal law in the European Union: Has the Council got it wrong? *Common Market Law Review*, 41: 5-36.

Picotti, Lorenzo, and Salvadori, Ivan. 2008. *National Legislation Implementing the Convention on Cybercrime - Comparative analysis and good practices*. Strasbourg: Council of Europe, August 28.

Polakiewicz, Jörg. 2010. Update on Council of Europe standard-setting activities. Paper presented at the Conference *Cooperation against Cybercrime*, March 23-25, in Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Update/Jorg%20Polakiewicz.pdf

Schjolberg, Stein. 2008. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. Http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

Seger, Alexander. 2010. The Budapest Convention on Cybercrime as a global framework: Introduction to panel discussions. Paper presented at the Conference *Cooperation against Cybercrime*, March 23-25, in Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%203/cyber_octopus_WS_3_alexander_CCC_global_frame.pdf.

Smith, Russel G, Peter Grabosky, and Gregory Urbas. 2004. *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

U.S. Department of Justice. 2004. Meeting of G8 Justice and Home Affairs Ministers http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html.

U.S. Department of Justice. Council of Europe Convention on Cybercrime Frequently Asked Questions and Answers. http://www.justice.gov/criminal/cybercrime/COEFAQs.htm#QE1.

Valeri, Lorenzo, Geert Somers, Neil Robinson, Hans Graux, and Jos Dumortier. 2006. *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*. Santa Monica: Rand Corporation.

van der Wilt, Harmen. 2002. Some Critical Reflections on the Process of Harmonisation. In *Harmonisation and harmonising measures in criminal law*, edited by André H. Klip and Harmen G. van der Wilt, 77-86. Amsterdam: Royal Netherlands Academy of Science.

Vermeulen, Gert. 2002. Where do we currently stand with harmonisation in Europe? In *Harmonisation and harmonising measures in criminal law*, edited by André H. Klip and Harmen G. van der Wilt, 65-76. Amsterdam: Royal Netherlands Academy of Science.

Weber, Amalie M. 2003. The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal*, 18, no. 1: 425-46.

Weyembergh, Anne. 2005. Approximation of criminal laws, the Constitutional Treaty and The Hague Programme. *Common Market Law Review*, 42: 1567-97.