the related legal terminology may raise problems. While providing for the criminalization of attacks that constitute a crime, the legislator has not delimited adequately the notions,[26] which relate to attacks, thus creating some ambiguity.[27]

Taking into consideration that legislators aimed at introducing technology neutral rules to ensure their sustainability, we should also keep in mind that flexibility and adaptability of law[28] should not be achieved at the expense of clarity and legal certainty. Clear and precisely defined, objective substantiation of a crime constitutes one of the basic principles of criminal law. Moreover, as prevention, enforcement and prosecution of cybercrime are largely dependent on the common understanding between technical and non-technical stakeholders, such as the prosecutors, lawyers, and the judges providing consistency in understanding, language and taxonomies is of crucial importance.

Furthermore, it is noteworthy that the relevant legal framework ignores the concept of threat, although threat[29] is one of the more crucial concepts for ensuring security.[30] Actually, this choice is consistent with the fact that both the Cybercrime Convention and the Directive 2013/40/EU regulate by their nature the criminalization of conduct and they do not address threats, which seem to be more a matter of cybersecurity policy. Moreover, threats may be accidental (e.g., fire, power failure, operator error), environmental (e.g., flood, lightning) or deliberate (e.g., hacking, malicious software, eavesdropping), while the term "attacks" indicate a deliberate malicious action; this corresponds to the choice of the EU legislator to impose criminal liability only if the offence has been committed with criminal intent, regardless whether the objective criteria of the offences laid down in the Directive are met.

§1.03 SECURITY OF INFORMATION SYSTEMS

The concept of attacks against information systems has to be understood in connection with the notion of security. Security, in a nutshell, is the absence of danger.[31] "*Security*

26. For example the Council of Europe Convention contains no definition of interception while the Directive 2013/40/EU contains a quite general and vague reference in Recital No. 9.
27. Kaiafa-Gbanti, *Criminalizing Attacks against Information Systems in the EU – The Anticipated Impact of the European Legal Instruments on the Greek Legal Order*, 20 Eur. J. Crime Crim. L. & Crim. Just., 59 (2012).
28. We should also keep in mind that notwithstanding the intentions of legislators to create technology neutral rules the provisions usually mirror the state of the art of the time that legislation is adopted or in any case the perceptions of legislators thereof. It is worthy to mention the focus of the Directive 2013/40/EU on "botnets."
29. Defined as potential cause of an unwanted incident, which may result in harm to a system or organization (ISO 27000-2014, 2.83). Threat is also defined as a circumstance that has the potential to cause loss or harm.
30. Indicative of the importance of threat as a concept is the fact that the European Union Agency for Network and Information Security (ENISA) is almost exclusively referring to "threats" in its documents. However, we must take into consideration that in some cases these terms are also used in an interchangeable way.
31. European Commission, Ethical and Regulatory Challenges to Science and Research Policy at the Global Level, Directorate-General for Research and Innovation, Brussels, 2012, 14.

is the condition (perceived or confirmed) of an individual, a community, an organization, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, [and] disasters (natural and man-made)."[32]

The need for information and communication systems security essentially arises exactly from the growing dependence on information technology to support an ever-increasing range of activities. Attacks against information systems are not a technical issue, as the damages caused correspond to interference with rights and interests, harms and damages to persons, private organizations and government. Even without explicit references, both the Budapest Convention and the Directive 2013/40/EU aim at protecting security of information, security of information (and communication) technology and, last but not least, fundamental rights and freedoms such as communications secrecy, privacy and personality.

Information security has to be distinguished from Information and Communication Technologies (hereafter ICT) security. ISO/IEC defines security in a functional way: "Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO/IEC 17799).[33] In a more specific context, ISO/IEC states that security consists in preservation of the so-called CIA triad or the classic C-I-A triplet: (a) *confidentiality*,[34] which is actually the aspect that people or at least lawyers most closely associate with the concept of security and refers to the prevention of unauthorized information disclosure, (b) *integrity, which* relates to the prevention of unauthorized modification of information[35] and (c) *availability*,[36] which corresponds to the need for data and systems to be accessible and usable (by authorized parties) whenever and wherever they are required.

ICT security is defined by ISO/IEC as all aspects relating to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation,[37] accountability, authenticity,[38] and reliability[39] of information resources (ISO/IEC 13335-1,

32. A.J. Sieber, *Presentation on CEN BT/WG 161 – Standards for Security and Protection of the Citizens*, in Security Research Conference, (Ankara 2008).
33. ISO/IEC 17799 ISO/IEC 17799 on Code of Practice for Information Security Management, 2005.
34. According to ISO 27000-2014 (2.12) confidentiality means the property that information is not made available or disclosed to unauthorized individuals, entities, or *processes*.
35. According to ISO 27000-2014 (2.40) integrity means the property of accuracy and completeness (2.40). In a formal security mode integrity refers to the protection against unauthorized modification or destruction of information. J. Graham, R. Howard, R. Olson, Cybersecurity Essentials, CRC 2011, 5.
36. According to ISO 27000-2014 (2.9) availability means the property of being accessible and usable upon demand by an authorized entity.
37. According to ISO 27000-2014 (2.54) non-repudiation means ability to prove the occurrence of a claimed event or action and its originating entities.
38. According to ISO 27000-2014 (2.8) authenticity means the property that an entity is what it is claims to be.
39. According to ISO 27000-2014 (2.62) reliability means the property of consistent intended behavior and results.

2004).[40] Each of these components is critical to overall security. As they interact to each other the failure of any one component may result in potential system compromise.[41]

§1.04 CYBERSECURITY

In the last years policy emphasis and the respective terminology is shifted to the notion of cybersecurity. In Europe, the increased number of cyber attacks and the sophistication of the methods used, as well as the growing scale of the damage, has shifted cybersecurity in the top of the agenda.[42]

The term cybersecurity has been used in theory often interchangeably with the term information security. However, cybersecurity is conceived in a broader way as a notion encompassing protection of information, information systems and infrastructure from those threats that are associated with using ICT systems in a globally connected environment.[43] In the European Union's documentation and legislative approach, cybersecurity is conceived in an more general and vague way which combines institutional and organizational aspects: the European Commission states that cybersecurity "*... commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.*"[44]

Cybersecurity and cyber attacks are strictly related not only to computer systems but also to computer networks. Cyber attacks include actions that may undermine the functions of a computer system or a computer network, i.e., they may alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.[45] A cybersecurity incident may also lead to breaches in the confidentiality, integrity or availability of information.

The goal of the EU cybersecurity strategy, the Draft NIS-Directive being a central element thereof, is to protect European citizens, administration, infrastructure and economies from cyber disruptions. A range of legislative, organizational and security measures are to be taken by Member States to create a cohesive approach with regard to cybersecurity measures, and minimize discrepancies within and between Member

40. See R. von Solms & J. van Niekerk, *From Information Security to Cyber Security*, Computers and Security 3, 897 e102 (2013).
41. J. Graham et al., *Cybersecurity Essentials*, 3–6.
42. European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions (2013).
43. U. Helmbrecht, *ENISA at the Service of the EU's Cyber Security, SEDE speech*, European Parliament Brussels, (Mar. 16, 2015).
44. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee Of The Regions, Join (2013), (Feb. 7, 2013).
45. See the comprehensive definition adopted by U.S. National Research Council in the Report Nat'l Research Council, Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 1 (William A. Owens et al.), 2009.

States. Directive 2013/40/EU is a decisive step towards creating a cyberspace and cybersecurity policy for Europe. Cyber security touches on multiple aspects of security: individual, national, international or even global security and stresses across the fields of internal market, justice and home affairs, and foreign policy to the extent that it angles to cyberspace issues.

Directive 2013/40/EU aims to harmonize the criminalization of specific types of conduct (such as illegal access to information systems or illegal system and data interference) and does not address the prevention of Network and Information Security (NIS) risks and incidents, the response to NIS incidents and the mitigation of their impact. The Directive's ultimate goal is to address large scale events and to contribute to the creation of a safer information society and of an area of freedom, security and justice.[46]

§1.05 CYBERCRIME AND CYBERWAR

Large-scale momentums and malicious cyber attacks may disable infrastructures and cause their malfunction in ways and to an extent that they impose severe sufferings on citizens or even physically harm them. Such attacks may threat security and safety of persons and organizations and produce economic damages through the interruption of information and/or communications systems or loss of confidence in markets. At the same time, the growing number of cyber events reported on a regular basis has transformed "Cyberspace" into a battlefield, bringing to light "Cyber warfare" as "the fifth domain or warfare" after land, sea, air and space.[47] Attacks causing far-reached damages on public infrastructures or having national-security implications test the categories and limits of existing legal framework and expand the boundaries of cyber crime *lato sensu* to include also cyberwar.[48]

However, there is no commonly accepted definition for cyber warfare. As a result, States and organizations perceive the notion of cyber warfare differently, depending on their priorities and specific interests. Despite the fact that there has been considerable progress at the European and International level towards the development of National Cyber Security Strategies and the adoption of an effective comprehensive legal framework of prevention measures against cyber attacks, it is doubtful if such strategies and rules can deal adequately and effectively with cyber war. More specifically, it has not been clarified in which cases cyber attacks could be treated as an "armed attack", making it possible for a state to respond by exercising its legitimate right of self-defense under Article 51 of the UN Charter.

Actually, there is currently no institutional framework for the evaluation of the "use of force" concept in cyberspace. However, experts have proposed evaluation

46. K. Pipyros et al., *Cyberoperations and International Humanitarian Law: Obstacles in Applying International Law Rules in Cyber Warfare*, Information and Computer Security (to be published).
47. W. Lynn, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, vol. 89, No. 5, available at: www.foreignaffairs.com/ articles/66552/william-j-lynn-iii/defending-a-new-domain (2010).
48. NATO Cooperative Cyber Defence Centre of Excellence, *Ten Rules for Cyber Security*, (Talinn 2011).

well-known, but, on the other hand, it is impossible for a specific individual to prove that one of his private communications has been subject to this mass surveillance mechanism. It has been argued that on this point a modification of the ECHR's jurisprudence would be profitable.[90] It could take the form of an acceptance of an *in abstracto* personal prejudice or of an *actio populis* claim.

The UK case is based on a claim of breach of Articles 8 and 10 of the ECHR. While the implication of Article 8 (protection of privacy) is obvious enough, the reference to Article 10 is justified by the alleged chilling effect on freedom of speech of the knowledge or even suspicion that all electronic communications are followed by information agencies. The UK court, in a secret judicial process, then had two issues to address: whether there are publicly known rules for the interception of communications, whose content is sufficiently indicated, and whether these rules are subject to proper oversight. The Court answered positively to both questions in February 2015.[91]

Since the fundamental principle of secrecy of correspondence has encountered a lot of difficulties in its efficient enforcement, the main lesson from the NSA scandal seems to be that a technological answer could be the best solution. The generalization of cryptography or even the recognition at a legal level of a right to encrypt private messages as a new subdomain of the right to data self-determination would, indeed, slow down the activities of information agencies. Of course, this also means that the various national anti-terrorist regulations will not be as effective. In any case, a public debate is already raging about the need to continue on the road of strict antiterrorism measures, or whether it is time to finally leave behind the trauma of the 9/11 attacks.

[E] Relationship of Cyber-Attack Offences with Other Offences

[1] Consecutive and Concurrent Sentences

As it has already been noticed, the very precise definition of the offences of cyber attacks may create an overlap between the offences. Not only these offences are interrelated but also it is necessary to ascertain also their relationship with other offences which are applicable, depending on the circumstances. It is, therefore, important to determine where cyber attacks could be punished – alternatively or cumulatively – under the legal framework of generally applicable crimes.

In some cases, the illegal acts of access or interference to information systems can only be a means for the perpetration of a more serious offence. For instance, the hacking of an "intelligent" car can lead to a lethal accident. Illegal acts of interference to data can be seen also as a form of illegal misappropriation of an intangible good. Illegal access to online client databases means most of the time that the legal framework of personal data protection is also violated.

90. Sloot, Bart van der, *Privacy in the Post-NSA Era: Time for a Fundamental Revision?*, 5(1) JIPITEC 1 (May 2, 2014).
91. *Liberty (The National Council of Civil Liberties) & Others v. The Secretary of State for Foreign and Commonwealth Affairs & Others*, [2015] UKIPTrib 13_77-H.

In case where the general interest protected by the offences is exactly the same, the general legal principle *"specialia generalibus derogant"* shall be applied. This means that the more specific offence, as *lex specialis*, should prevail upon the most general one. However, in case whereas the various applicable offences refer to a different philosophy, the question of the cumulative application of those offences is legitimately posed according to the ECHR case law.[92] In criminal law theory, this issue is resolved by the application of the theories of accumulation of offences. First of all, it should be noted that the plurality of offence does not raise by itself any difficulty: in case of culpability, the defendant is liable separately for each one of the offences. The issue is to ascertain the sanction. Is it possible for the sentences to run concurrently? Should the privations of freedom cumulate? With or without limit? Unfortunately, the corpus juris, namely the EU acquis related to Criminal law, does not solve the issue, which is left to national legal systems. In practice very different systems apply, even if informally most European systems tend to adopt a "totality principle" which requires the court to consider the overall sentence in relation of the totality of the offending.[93]

Furthermore, it has to be highlighted that the principle *"non bis in idem"* is well established in EU criminal law.[94] The EU Charter of Fundamental Rights enshrines this principle in Article 50 ("Right not to be tried or punished twice in criminal proceedings for the same criminal offence") and the same principle is mentioned on Article 4 of Protocol No. 7 to the ECHR. The rule forbids the accumulation of two penalties of the same kind. This means practically that independently of the chosen offence, the same cyber attacks cannot be prosecuted twice. The rule prohibiting concurrent application of sentences refers to the accumulation of two penalties of the same kind, that is to say, to criminal-law penalties. But also, it is clear that, in accordance with Article 50, the *"non bis in idem"* rule applies not only within the jurisdiction of one State but also between the jurisdictions of several Member States.[95] In other words, in case of a European-scale cyber attack, even if rules exist in order to avoid jurisdictional conflicts (see section § 2.05), a possibility of accumulation of prosecution cannot totally be avoided. In this case, the principle *non bis in idem* will have the effect to prevent a second prosecution in another country for the same attack.

[2] The Concurrent Application of "Computer Related" Offences with Cyber Attacks Offences

It should be added that the Budapest Convention inserts under the title "Computer related offences" two very specific offenses, the offences of "Computer-related

92. ECHR, *Oliveira c/ Suisse*, Jul. 30, 1998, §22.
93. Andrew Ashworth, *Sentencing and Criminal Justice* 170 (Cambridge University Press 2010).
94. For instance, see decision of the Court of First Instance of Apr. 20, 1999, Joined Cases T-305/94 *Limburgse Vinyl Maatschappij NV and others v. Commission* [1999] ECR II-931.
95. Explanations relating to the charter of fundamental rights, 2007/C 303/02.

forgery"[96] and of "Computer-related fraud",[97] which are very closely interrelated with the cyber attacks offences.[98] Indeed, the Budapest Convention's Explanatory Report characterizes them as "two specific kinds of manipulation of computer systems or computer data."[99] The Convention stipulates that those offenses should be punished as criminal offences. Both offences are inspired by the Convention's general cybercrime principles: only intentional acts without right are criminalized.

The computer-related forgery has a narrow field of application, since it applies to forgery of computer data for legal purposes only. It is a matter of interpretation whether this offence applies to the specific kind of cyber-attack which is related with certificate falsification. Most platforms of online application distribution nowadays impose a system of software certification in order to create a form of developer's liability and therefore prevent the dissemination of malware. Similarly, the mechanism of certificates is used for HTTPS-based web sites, usually for e-commerce purposes. The certificate here authenticates the website and ensures the user that it has not been hacked. Even in the case where the data have not a legal purpose, the eventual alteration of these certificates would qualify as a data alteration in the scope of the related offence.

In any case, the offence of computer-related forgery still possesses a wide importance when applies in respect of digital signatures. This field of law has just been completely revised by the European legislator. The Regulation 910/2014[100] on electronic identification and trust services for electronic transactions in the internal market creates a new general legal framework related to digital identification, distinguishing between the legal regime of electronic signatures,[101] electronic seals,[102] electronic time stamps,[103] electronic registered delivery services[104] and website authentication[105]

96. Article 7 of the Budapest Convention: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches."
97. Article 8 of the Budapest Convention: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
    (a) any input, alteration, deletion or suppression of computer data,
    (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".
98. Venancio, Pedro Dias, *Similarity and Competition between Cybercrimes Related to Computer Data in the Council of Europe's Convention on Cybercrime*, 7 Masaryk UJL & Tech. 97 (2013).
99. Budapest Convention's explanatory report, *ibid.*, 80.
100. The Regulation 910/2014 of the European Parliament and of the Council of Jul. 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
101. Chapter III, section 4.
102. Chapter III, section 5.
103. Chapter III, section 6.
104. Chapter III, section 7.
105. Chapter III, section 8.

(section 8). Each time these electronic identifications are used for legal purposes (public, such as relationship with public services, or private, such as contractual purpose), the intentional alteration of their authenticity leads to the application of the computer-related offence. The Regulation adds that in case of security breach which questions "the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission."[106] Furthermore, in parallel of the question of criminal liability, the Regulation imposes civil liability "for damage caused intentionally or negligently to any natural or legal person"[107] of the various implicated actors of the identifying process (the State, the party issuing the electronic identification means and the party operating the authentication procedure) according to the obligation's failure.

The offence of "computer-related fraud" has also to be interpreted very narrowly. It would not apply to the general activities of phishing which are alarmingly developing on the Internet. Indeed, whereas the hacker uses a fraudulent means, such as a false email (for instance the famous "Nigerian scam"), or even a fake website mirroring the appearance of a genuine website (which raises also issues of copyright law infringement), Internet is used only as a means of communication and the legal response can be found accordingly to the rules applying to the general offence of fraud or even to extortion (in case of romance scam). The condition of "economic benefit for oneself or for another person" is certainly met in these cases. However, the cumulative condition of alteration of computer data or interference with the functioning of a computer system is not met.

By consequence, the offence of "computer-related fraud" should be seen as a specific application of the offences of cyber attack, when the fraudulent intent of economic benefit is established. This could apply to direct attacks against systems of electronic money distribution or even of cryptocurrencies' systems.

§2.03 PRIVATE LAW ASPECTS OF THE REGULATION OF CYBER ATTACKS

[A] Civil Liability for Cyber Attacks

Neither the Budapest Convention nor the European legislation touch upon civil law issues related to cyber attacks. Civil liability poses issues both in respect of the liability of the perpetrator of the cyber attack and in respect of the intermediaries' liability. The specific issue of the intermediaries' liability plays a substantial role in general in Internet regulation and, therefore, it is discussed in detail in the Chapter 3 of this book.[108] However, the direct civil liability of the perpetrator of a cyber attack has not

106. Article 10 of the Regulation 910/2014.
107. Article 11 of the Regulation 910/2014.
108. See Chapter 3(B)(1).

been clearly defined yet by the legislator. In general, the legal framework of civil liability has not been harmonized in the European Union yet. However, a common Roman law heritage, centuries of discussions and the concerted efforts of scholars in the past twenty-five years (such as the European Principles of Tort law PETL,[109] which were published in 2005[110]) led to some practical results. The civil law arsenal in this matter includes on the one hand, injunctive relief and disclosure orders to Internet Service Providers (ISPs) against perpetrators. On the other hand, the person who has been harmed by the cyber attack is also entitled to civil claims in order to recover the loss caused by the cyber attack. Therefore, the private aspect of cyber attacks can be dealt mostly by applying the standard reasoning of civil law, "though to novel factual settings."[111]

As it has already been mentioned above, cyber attack offences require intention. From a private law perspective, this means the application of a fault-based liability regime. Indeed, as stated in the PETL, "a person is liable on the basis of fault for intentional or negligent violation of the required standard of conduct."[112] From a continental law approach, this should be enough to ensure that the liability of the person behind a cyber attack is established. From a common law approach, an additional difficulty appears. The intention should exclude the application of the tort of negligence. However, the criminal aspect of a cyber attack could be used as a direct legal basis for an action for compensation under the "breach of statutory duty" tort. The criteria for the application of this tort are certainly related to the intention of the legislator. In other words, the judge has to ask himself if, by promulgating a general interdiction, the legislator also presumes that the perpetrator should be civilly liable. Even if, in general, the existence of criminal sanctions works as a presumption that the legislator did not wish to impose a civil sanction, in the case of cybercrime, a reasonable approach would be to recognize that the intention of the law is to cover also the loss inflicted by a cyber attack. Therefore, even if in principle, the existence of criminal sanctions works as a presumption of the legislator's intention not to accept civil sanctions, civil law actions shall not be excluded.

Both in common law and civil law jurisdictions, causation has to be established. In other words, a casual relationship between the cyber attack and the loss has to be proven. As stated in the PETL, "An activity or conduct (hereafter: activity) is a cause of the victim's damage if, in the absence of the activity, the damage would not have occurred",[113] while the liability is limited to the extent of the foreseeability of the damage.[114] The application of these general principles depends on the specific type of the cyber attack. For example, in case of computer-related fraud, the causation

109. European Principles of Tort law PETL, http://www.egtl.org/.
110. European Group on Tort Law, *Principles of European Tort Law, Text and Commentary*, XII, 282 (Springer 2005).
111. A. Koch, Bernhard, *Cyber Torts: Something Virtually New?*, 5.2 J. Eur. Tort Law 133–164 (2014).
112. Article 4:101.
113. Article 3:101.
114. Article 3:201.

between the fraud and the loss is evident. Similarly, in case of a direct intrusion to a system, the intentional intrusion is the cause of the data breach.

However, in case of a virus or of a DDoS attack, the perpetrator could be tempted to use the rules of causality in his benefit in order to avoid liability. Viruses, malware, DDoS attacks most of the time imply the act of a third person, which is often the innocent "medium" for the transmission and the perpetration of the attack. In this context, could the perpetrator use the defense of "*nova actus interveniens*" ("breaking the chain")? Furthermore, in case of a virus or a malware, the perpetrator has often no control on the dissemination of the tool and no idea of the real extent of the damage that it will be caused. Could this signify that the total damage is not foreseeable? Also, the DDoS attack exploits the vulnerability of connected devices in order to create a zombie network. The force of the DDoS attack depends on the size of the network. Could, therefore, the tortfeasor validly claim that his liability has to be limited by application of the rules of third party's liability for negligence? For all those complex questions, the reckless attitude of the tortfeasor should serve as a justification for a flexible application of the rules of causation by the judge.

Finally, in certain circumstances, the issue of civil liability as regards cyber attacks would be resolved differently. The European Commission has proposed a Trade Secrets Directive[115] protecting information which is secret, which has a commercial value because it is secret and has been subject to reasonable steps to keep such information secret. Therefore, the perpetrator of an act of an unlawful acquisition which is defined mainly as unauthorized access, theft, bribery, deception, breach or inducement to breach confidentiality, is primary liable for this action. The Trade Secrets Directive, if adopted, would also create a regime of secondary liability which is currently absent in most countries. More precisely, the third party who obtains access to the protected information with knowledge of their unlawful acquisition is also civilly liable. In conclusion, the proposed legal framework of trade secrets institutes a quasi-intellectual property right[116] on trade secret, which is deemed to play a substantial role in the framework of civil law conflicts related to cyber attacks.

[B] The Calculation of Damages

One particularity of the civil aspect of cyber attacks is that in most cases the court has to deal with issues of solidary and several liability. In this context, underground networks which are responsible for DDoS attacks, malware programming and other cyber attacks should be seen as multiple tortfeasors. In the same time, viruses, malware, massive Internet frauds and general online communication surveillance

115. Proposal for a Directive of the Parliament and the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM/2013/0813 final – 2013/0402 (COD).
116. J. Heitto, *The Trade Secret Directive Proposal and the Narrow Path to Improving Trade Secret Protection in Europe*, 16(5) Computer L. Rev. Intl. 140–144 (2015).

> *liability exemptions set out in the e-Commerce Directive, as the technical capabilities of online intermediaries develop and the commercial uses of the content they present become ever more sophisticated.*[18]

A deeper involvement of ISPs in cybercrime prevention faces significant obstacles, such as the burden of technical costs and thorny legal questions. The exact role and competencies of ISPs in the fight against cybercrime is an intricate issue, since possible interventions of Internet intermediaries shall be scrutinized from a human rights perspective, while the regime of their liability is also at stake. Indeed, as it is stated in the United Nations Office on Drugs and Crime, Study on Cybercrime:

> *that service providers should have some role in cybercrime prevention is, at the same time, both 'obvious', but yet nuanced and complex – engaging issues such as service provider liability and responsibility for internet content.*[19]

In the same vein, the report of the US Institute for Homeland Security Solutions states that:

> *Customer contracts often specifically prevent an ISP from filtering traffic, and international connections multiply the potential legal complexities. ISPs also worry that providing more security would implicitly increase their liability (i.e., if an ISP states that they provide security and a customer is negatively affected by a security breach, the ISP could be held fully or partially liable).*[20]

The question of the liability of ISPs is not exclusively raised in respect of their duties to their customers, but also in a criminal law spectrum vis-à-vis the State, such as for aiding and abetting criminal activities, as it has been demonstrated in the US by the settlement agreement of Google with the United States Department of Justice, where Google admitted to its knowledge of, and participation in, unlawful advertising, because by permitting online Canadian pharmacies to place advertisements through AdWords, it facilitated the unlawful importation of controlled pharmaceuticals into the United States.[21] Similarly, when a bulletin board is used to publish passwords to allow unauthorized access into a computer system, the operator may be liable for aiding, abetting, counseling or procuring commission of an offence, or for incitement to commit an offence if he has actually advertised that passwords are available on the bulletin board to a community of people who are likely to carry out computer hacking.[22]

Nonetheless, holding ISPs criminally responsible is subject to the classic obstacles for establishing criminal liability for corporate crimes in general, where the

18. Commission Staff Working document, *A Digital Single Market Strategy for Europe, – Analysis and Evidence*, Brussels, 6.5.2015, SWD 100 final, 55–56 (2015). Available online at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf.
19. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft (February 2013).
20. Brent Rowe et al., *The Role of Internet Service Providers in Cyber Security* (Institute for Homeland Security Solutions June 2011).
21. For the text of the non-prosecution agreement, see: http://googlemonitor.com/wp-content/uploads/2011/05/Google%20Agreement.pdf.
22. Graham Smith, *Internet Law and Regulation* 118 (Sweet & Maxwell 2007).

question of proof of the ISPs *mens rea* might be decisive. Indeed, ISPs will often not be aware of illicit contents posted by their subscribers, while the latter can modify this content without any intervention of the ISPs and they are not required to inform them for these acts.[23] Therefore, even if the E-Commerce Directive's ISPs safe harbor concerns the civil liability of online intermediaries and not the criminal one, the safe harbor could not apply anyway; since the criminal liability (for instance for conspiracy or aiding and abetting) implies the intent of the ISPs, it encompasses by definition their actual knowledge of the civil or criminal activity of the user. Consequently, the ISPs cannot find protection against liability.

Also, while the idea of making ISPs more responsible or even legally accountable for cybersecurity purposes might be attractive, defining the legal foundations, the conditions and the scope of such a regime is certainly a complex issue, since important legal policy choices finally have to be made, such as, for example, whether an ISP's possible civil liability should be based in negligence or strict liability.[24] And yet, if such legal mechanisms are introduced in a national basis, the ubiquitous nature of Internet communications might significantly undermine the effectiveness of such legal regimes. So, even if Europe or the U.S. establish an ideal ISP liability regime, where any cyber attack originating from a European or an American ISP can be traced, European or American Internet users would yet remain vulnerable to cyber attacks committed from computers in countries without the same, strong level of Internet regulation.[25]

[B] The Big Challenge: Balancing ISP Subscribers' Rights with Law Enforcement Objectives

Besides, ISPs appear to have two potentially conflicting roles: on the one hand, a role as the trusted stewards of their clients' personal data and private communications and, on the other hand, their emerging role as a party in possession of data which might assist in law enforcement.[26] Indeed, since gathering electronic evidence in cybercrimes is often linked to obtaining computer data from ISPs, the role of ISPs in the storage and retention of various types of data (traffic data, subscriber data, content) is substantial.

The European Convention on Cybercrime establishes specific procedural rules for the obtaining of such data by the ISPs. Indeed, ISPs in signatory countries would be required to respond to and comply with legal processes from other signatory countries

23. Xavier Amadei, *Standards of Liability of Internet Service Providers: A Comparative Analysis of France and the United States with a Specific Focus on Copyright, Defamation and Illicit Content*, 35 Cornell Int'l L.J. 189, at 207 (2002).
24. See on this issue: Assaf Hamdani, *Who is Liable for Cyber Wrongs*, 87 Cornell L. Rev. 901 (2002). Available online at: http://scholarship.law.cornell.edu/clr/vol87/iss4/1.
25. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, Chicago John M. Olin Law & Economics Working Paper No. 217 (2D SERIES), (July 2004). Available at SSRN: http://ssrn.com/abstract=573502 or http://dx.doi.org/10.2139/ssrn.573502.
26. Ian Kerr & Daphne Gilbert, *The Role of ISP in the Investigation of Cybercrime*, in *Information Ethics in the Electronic Age: Current Issues in Africa and the World* 165 (Tom Mendina & Johannes J. Britz (ed.), McFarland & Company Inc 2004).

with respect to the provisions of the Cybercrime Convention, regardless of the laws of the country in which they reside.[27]

It is also important to distinguish whether the collection is about data which are already stored by the ISPs or it is real time collection of traffic or content data. While the procedural safeguards of privacy and of secrecy of communications vary depending on the type of data which are processed by ISPs, the intervention of ISPs in the fight against cybercrime marks a shift in the role of these private actors, who are now attributed certain state assigned competencies and obligations in the law enforcement process.[28]

According to Article 15 of the Cybercrime Convention, the Parties should provide some safeguards in their domestic law, in order to balance the requirements of law enforcement and the protection of human rights. Nonetheless, the Convention does not specify these conditions and safeguards, but provides for including some general criteria referring back to obligations which have been undertaken by the Parties under human rights law instruments.[29]

In this context, it shall be reminded that the European Court of Human Rights (ECtHR) has undertaken significant efforts to define the safeguards and standards governing electronic investigations and electronic surveillance. The gravity of the interference of the investigation, its purpose and its proportionality are emphasized as crucial factors to be taken into account and certain fundamental principles deriving from the Court's case law are highlighted. More precisely:

> *a) a sufficient legal basis for investigation instruments is necessary b) the legal basis must be clear with regard to the subject c) the competences of the law enforcement agencies need to be foreseeable and d) surveillance of communications can be justified only in case of serious crimes.*[30]

In *Weber Saravia v. Germany*, the Court held that:

> *since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent*

27. Sylvia Mercado Kierkegaard, *Cracking Down on Cybercrime Global Response*, Communications of the IIMA, 59, 5(1) (2005), at: http://www.iima.org/ CIIMA/CIIMA%205.1%2059%20Kirkegaard-7.pdf.
28. Ian Kerr and Daphne Gilbert, *ibid.*, 171.
29. Lorenzo Picotti & Ivan Salvadori, *National Legislation Implementing the Convention on Cybercrime –Comparative Analysis and Good Practices* 46 (Mar. 12, 2008). Available online at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567%20study2-d-version8%20provisional%20_12%20march%2008_en.pdf.
30. Cormac Callanan & Marco Gerke, *Cooperation between Law Enforcement and Internet Service Providers against Cybercrime: Towards Common Guidelines*, Council of Europe, Project on Cybercrime, 16–17 (Mar. 17, 2008). Available online at: http://www.coe.int/ t/dghl/cooperation/economiccrime/cybercrime/cy_activity_interface2008/567%20prov-d-wg%20STUDY%20FINAL%20%282%29.pdf.

> *authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference*[31].

The possible threat of secret surveillance systems for democracy has been identified by the Court in the *Klass and others v. Germany*, where it was stressed that:

> *"the Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*[32]*"* and that, *"the Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."*[33]

The privacy implications of the perspective of a more dynamic role of ISPs in cybercrime enforcement have also been demonstrated by the controversies of the interpretation of Article 32(b) of the Cybercrime Convention. This section deals with the determination of the conditions upon which a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance. According to this provision, a Party may access or receive, without the authorization of another Party, stored computer data located in another Party through a computer system in its territory, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer.

Thus, the provision of Article 32(b) addresses the situation where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system.[34] While it has been ambiguous whether ISPs could also be considered as persons who have lawful authority to disclose the data,[35] the Council of Europe clarified the meaning of that term. After emphasizing that the respect of the rights of individuals and the interests of third parties are to be taken into account when applying the measure, the Committee determined that service providers are highly unlikely to be able to consent validly and voluntarily to disclosure of their users' data under that provision, since normally,

31. ECtHR, *Weber and Saravia against Germany*, Application No. 54934/00, Jun. 29, 2006, para. 94.
32. ECtHR, *Klass and others v. Germany*, Application No. 5029/71, Sep. 6, 1978, para. 49.
33. ECtHR, *Klass and others v. Germany*, *ibid.*, para. 50.
34. Convention on Cybercrime, Explanatory Report. Available online at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.
35. Groupe interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes*, Rapport sur la cybercriminalité, at 50 (February 2014). Available online at: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

service providers will only be holders of such data, they will not control or own the data, and they will, therefore, not be in a position to give a valid consent.[36]

Similarly, Article 29 Working Party underlined that companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process. In this context:

> *they can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is require.*[37]

[C] Cybercrime Prevention via Internet Filtering: Precedents and Controversies

Additionally, ISPs could contribute to cybercrime prevention through active "filtering" of Internet communications or content with a view to preventing cybercrime acts in the first place.[38] By relying on intermediaries to block illicit Internet content, the administrative and technical burden of filtering on government can be reduced, whilst providing a new form of crime prevention.[39] At the same time, this policy raises important issues of accountability, due to the lack of public or governmental oversight in the implementation of such methods of control.[40]

While the ISP's role in the filtering and blocking of sites has mainly emerged in respect of cyber-enabled crimes, the use of such law enforcement techniques on *stricto sensu* cybercrimes is at stake. Definitely, Internet serves as a platform where it is possible to acquire all the necessary resources to conduct a cyber attack without having particular skills. Cybercriminal business models function on a combination of sales of various malicious products and services, with an offer of an efficient "customer care" to support customers in their initiatives, and social networks platforms to manage the community of clients and communicate with them rapidly.[41]

36. Cybercrime Convention Committee (T-CY), n. 3, Transborder access to data, Strasbourg, 7 (Nov. 5, 2013). Available online at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf.
37. *Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime* (Brussels, Dec. 5, 2013). Available online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.
38. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft (February 2013). Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
39. M. McIntyre, *Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems*, in *Research Handbook on Governance of the Internet* (Edward Elgar 2012).
40. Joss Wright & Yana Breindl, *Internet Filtering Trends in Liberal Democracies: French and German Regulatory Debates*, 2(2) Internet Policy. Rev. Available online at: http://policyreview.info/articles/analysis/Internet-filtering-trends-liberal-democracies-french-and-german-regulatory-debates.
41. Pierluigi Paganini, *Cybercrime and the Underground Market* (Jan. 15, 2013), at: http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/.

The most representative example of the implementation of filtering for cybercrime prevention purposes can be found in the respect of child pornography, while such filtering and surveillance schemes are also often found in national antiterrorist legislations. Nonetheless, as it will be demonstrated, even in those cases, where the defense of public interest goals appears to be of particular weight, the implementation of Internet filtering by ISPs has proved to be a thorny question in practice.

Using filters as a preventive measure for restricting access to illegal or harmful Internet content has proved to be controversial, even though the purposes served by such measures are not contested themselves. An illustrative example is the implementation of filters preventing access to websites containing child pornography and child abuse content.

In the European level, Article 25 of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[42] provides that:

> 1. *Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavor to obtain the removal of such pages hosted outside of their territory.*
> 2. *Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.*

It is noteworthy that the Directive does not set out as a prerequisite the prior authorization of blocking by the judiciary.[43] Recitals 46 and 47 of the Directive are of particular importance on how these measures can be implemented by Member States. According to Recital (46):

> *Child pornography, which constitutes child sexual abuse images, is a specific type of content which cannot be construed as the expression of an opinion. To combat it, it is necessary to reduce the circulation of child sexual abuse material by making it more difficult for offenders to upload such content onto the publicly accessible web. Action is therefore necessary to remove the content and apprehend those guilty of making, distributing or downloading child sexual abuse images. With a view to supporting the Union's efforts to combat child pornography, Member States should use their best endeavors to cooperate with third countries in seeking to secure the removal of such content from servers within their territory.*

Recital (47) is more explicit and it precisely provides that:

> *However, despite such efforts, the removal of child pornography content at its source is often not possible when the original materials are not located within the Union, either because the State where the servers are hosted is not willing to cooperate or because obtaining removal of the material from the State concerned proves to be particularly long. Mechanisms may also be put in place to block access from the*

42. OJ L 335, 17.12.2011.
43. Sarah Summers et al., *supra* n. 11, 189.

rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 7

Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;
(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8

Incitement, aiding and abetting and attempt

1. Member States shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.
2. Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence.

Article 9

Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor.
3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose.
4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:
   (a) they are committed within the framework of a criminal organization, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;
   (b) they cause serious damage; or
   (c) they are committed against a critical infrastructure information system.
5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

Article 10

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following:
   (a) a power of representation of the legal person;
   (b) an authority to take decisions on behalf of the legal person;
   (c) an authority to exercise control within the legal person.
2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.