Evaluation

of the

Proposal for a Directive on attacks against information systems (COM [2010] 517 final)

on the basis of the

Manifesto for a European Criminal Policy

by Prof. Dr. Maria Kaiafa-Gbandi, European Criminal Policy Initiative

With Financial Support from the Criminal Justice Programme of the European Union and the Ragnar Söderbergs Stiftelse

1. On the requirement of a fundamental legal interest worthy of protection

a) What interest does the legal instrument in question aspire to protect?

According to the Commission's proposal, the protected legal interests seem to be **information systems** and **their applications** in the modern information society (Preamble, sec. 2):

"Attacks against **information systems**, in particular as a result of the threat from organised crime, are a growing menace, and there is increasing concern about the potential for terrorist or politically motivated attacks against **information systems which form part of the critical infrastructure of Member States and the Union**. This constitutes a threat to the achievement of **a safer information society** and an area of freedom, security and justice, and therefore requires a response at the level of the European Union".

b) Is the protected interest fundamental in terms of its nature and is it anchored in the primary law of the EU?

Article 83 of the TFEU lists computer crime among the areas of particularly serious crime with a cross border dimension. In this area, the EU retains competence to establish minimum rules concerning the definition of pertinent criminal offences and sanctions for the purpose of the approximation of criminal laws in the Member States, if this proves to be necessary for ensuring a high level of security to the citizens (art. 67 par. 3 TFEU). The reference to computer crime in the Union's primary law itself reveals the importance that the EU attaches to the legal interest protected through the criminalization of attacks against information systems.

On the other hand, the commission's proposal as well as the recent presidency's orientation debate and the Council's general approach (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011 and DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011 respectively) also link information systems to other important legal interests, i.e. critical infrastructures of the Member States or the Union, which are necessary for vital societal functions, such as health, safety, security and economic or social wellbeing of the people (Preamble, sec. 2a).

c) Is the protected interest possible to reconcile with the constitutional traditions of the Member States and the EU Charter on Fundamental Rights?

Information systems are already protected as legal interests in most EU Member States. Consequently, there seems to be no problem with their incorporation as a protected legal interest in national constitutional traditions. It is worth mentioning that the Constitutional Court of the Federal Republic of Germany has pointed out the importance of the right to confidentiality and integrity of information systems as a legal interest [BVerfG, 1 BvR 370/07 (27.2.2008, section 166)]. On the other hand, information systems are recognized and protected as legal interests by the Council of Europe Convention on Cybercrime. So far, this Convention has been signed by all 27 Member States, but it has not been ratified by all of them. The Convention entered into force on 1 July 2004. The EU itself is not a signatory party to the Convention. Given the importance of this instrument, the Commission actively encourages the remaining EU member states to ratify it as soon as possible.

d) In what way is the impact of the proscribed conduct on the protected interest especially harmful to the society?

According to the proposal for a directive and the recent pertinent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 9) as well as the Council's general approach (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, P.4): "There are a certain number of critical infrastructures in the Union, the disruption or destruction of which would have significant cross-border impacts. It emerges from the need to increase the critical infrastructure protection capability in Europe that the fight against the attacks against information systems should be complemented by serious criminal sanctions reflecting the gravity of such attacks. Critical infrastructure may be understood as an asset, system or part thereof located in Member States which is essential for instance for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." (Preamble, sec. 2a). On the other hand, "[T]here is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types" (Preamble, sec. 3).

The question that arises, nonetheless, is whether all the forms of conduct described as punishable in the proposed directive bear the characteristics mentioned above. This is obviously not the case.

e) Does the EU legislator deal with the question of a legal interest worthy of protection, and is there any explicit and detailed justification as to whether a legitimate interest of this kind actually exists?

In the proposal for a directive on attacks against information systems there is no direct justification of the protection of information systems as such. On the contrary, there is a marked tendency of repeatedly referring to organised crime and terrorism (see above Preamble, sec. 2, 2a and 3) in order to explain the need for the criminalisation of the offences proposed in the directive as well as a rather detailed description of the so-called "botnets" and their large scale destructive properties which are, according to the Commission, the reason for the need to criminalize the production, procurement, sale, etc. of tools used for committing attacks against information systems.

"The term 'botnet' indicates a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'. The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack may be in a different location from the offender himself.

Attacks carried out by a botnet are often executed on a large scale. Large-scale attacks are those attacks that can either be carried out with the use of tools affecting significant numbers of information systems (computers), or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc. The damage caused by large-scale attacks has a major impact on the functioning of the target itself, and/or affects its working environment. In this context, a 'big botnet' is understood to have the capacity to cause serious damage. It is difficult to define botnets in terms of size, but the biggest botnets witnessed have been estimated to have between 40,000 and 100,000 connections (i.e. infected computers) per period of 24 hours." (COM 2010, 517 final, p. 3).

The gaps of the current institutional framework

According to the proposal, the existing Framework Decision approximates legislation only to a limited number of offences, but it does not fully address the potential threat posed to society by large scale attacks, nor does it take sufficient account of the gravity of the crimes and sanctions against them (COM 2010, 517 final, p. 4).

However, this position has to be examined in light of the fundamental principles of criminal law as well as those of the Union law (see infra).

2. On the *ultima ratio* principle

a) Are there for the protection of the legitimate interest (according to 1) alternative protection mechanisms –unrelated to the imposition of criminal sanctions- available to the EU?

The proposal itself refers to various alternative measures.

"Other EU initiatives and programmes in force or planned go some way to addressing problems related to cyber attacks or issues, such as network security and the safety of Internet users. They include actions supported by the programme 'Prevention of and Fight against Crime'8, 'Criminal Justice'9 programme, the 'Safer Internet'10 programme and the 'Critical Information Infrastructure Initiative'11. In addition to the Framework Decision, another relevant legal instrument in force is Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography.

At administrative level, the practice of infecting computers, turning them into 'botnets', is already prohibited under EU privacy and data protection rules12. Notably national administrative agencies are already cooperating under the European Contact Network of Spam Authorities. Under those rules, Member States are required to prohibit the interception of communications on public communications networks and publicly available electronic communications services without the consent of the users concerned or legal authorisation. This proposal is compliant with those rules. Member States should pay attention to improving the cooperation between administrative and law enforcement authorities for cases subject to both administrative and criminal sanctions." (COM 2010, 517 final, p.4).

b) Can the European legislator demonstrate the inadequate effectiveness of alternative, non-penal/criminal measures in practice?

No, because the above mentioned alternative measures have not been applied in practice, as some of them are still planned.

c) Does the EU legislator deal with the question of alternative protective measures, and is there an explicit and detailed explanation as to whether resort to criminal law (of member States, where appropriate) is necessary?

The content of the proposal

In an attempt to provide for the achievement of the objective, the proposal refers to four alternative options (COM 2010 517 final, p.5):

- Policy option (1): Status Quo / No new EU action

This option means that the EU will not take any further action to combat this particular type of cybercrime, i.e. attacks against information systems. Ongoing actions are due to be continued, in particular the programmes to strengthen critical information infrastructure protection and improve public-private cooperation against cybercrime (…).

- Policy option (2): Development of a programme to strengthen the efforts to counter attacks against information systems by means of non-legislative measures

Non-legislative measures would, in addition to the programme for critical information infrastructure protection, focus on cross-border law enforcement and public-private cooperation. These soft-law instruments should aim to promote further coordinated action at EU level (…).

- Policy option (3): Targeted update of the rules of the Framework Decision (new Directivereplacing the current Framework Decision)

to address the threat from large-scale attacks against information systems (botnets) and, when committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner, the efficiency of Member States' law enforcement contact points, and the lack of statistical data on cyber attacks (…).

- Policy option (4): Introduction of comprehensive EU legislation against cybercrime

This option would entail new comprehensive EU legislation. In addition to introducing the soft-law measures in policy option 2 and the update in policy option 3, it would also tackle other legal problems related to Internet use. (…)

- Policy option (5): Update of the Council of Europe Convention on Cybercrime

This option would require substantial renegotiation of the current Convention, which is a lengthy process and is at odds with the time frame for action that is proposed in the Impact Assessment. (…)

Preferred policy option: combination of non-legislative measures (option 2) with a targeted update of the Framework Decision (option 3).

Remarks

It is noteworthy that the presentation of the above alternative solutions is identical in all three proposals for a directive that have been presented by the Commission in the field of substantive criminal law after the Lisbon Treaty came into force (trafficking in human beings, sexual exploitation of children and attacks against information systems). This evidences that they are not founded on a significant evaluation, which would help assess the different characteristics and the special requirements of every specific problem.

As already mentioned above, the Commission finds that the proposed directive on attacks against information systems is justified, because such attacks "in particular as a result of the threat from organised crime, are a growing menace, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union" (Preamble sec. 2). Moreover, in the same Preamble (section 12) the Commission recognises that "There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses". This statement makes it patent that the resort to criminal law at this stage –in lack of a complete picture- has been premature, especially given the fact that pertinent criminal law rules are already in existence. Respect for the *ultima ratio* principle in the application of criminal law would require not only a clear picture of the problem but also the exclusion of all other solutions. According to policy option (2), such solutions are to be implemented alongside criminal law measures. Such haste to resort additionally to criminal law is hardly explicable and is definitely not convincing.

Besides, the lack of empirical data also indicates disregard to the principle of subsidiarity. Indeed, absent empirical data it is hardly discernible whether member States could have arrived at the desired result themselves, or whether it was in fact imperative to resort to EU measures.

d) Do the proscribed types of conduct indeed call for criminal sanctions as a last resort?

Starting with the types of conduct already provided for in the framework decision, it is to be noted that the proposed directive expands the ambit of *illegal access to information systems* (article 3), as it no longer recognizes each member State's discretion to confine the proscribed conduct to situations where the offense is committed by infringing a security measure.

The proposed directive goes even further than the Council of Europe Convention, which allowed some margin of discretion to member States under article 2, just like the framework decision. In fact, the Convention not only allows States to exclude offenses not committed by infringing security measures or are unrelated to a computer system that is connected to another computer system, but also permits them to narrow criminal liability through the introduction of subjective elements, such as requiring 'dishonest intent'. In reality, the Council of Europe was attempting to exclude conduct which does not pose any threat whatsoever to information systems, especially when it might reveal

some of their weaknesses. Hence, it left State parties the choice of determining for themselves whether to subscribe to a broad or narrow version of criminalization of cybercrime.

One might counter argue that the same discretion is reserved for Member States under the proposed directive, which requires criminalization in "cases which are not minor". However, this would be an erroneous assumption. Indeed, the same clause is to be found in the existing framework decision (2005/222/JHA) *alongside* a provision permitting Member States to only criminalize conduct infringing a security measure, indicating that these are two distinct limitations. Notwithstanding the inherent ambiguity of the notion of "minor cases", it cannot be argued that every conduct not infringing a security measure is a minor one. Therefore, the possible exclusion of minor cases under the proposed directive cannot be said to fully coincide with the ambit of either the Council of Europe Convention or the existing framework decision.

Besides, allowing States to introduce certain limitations is also in line with the requirement that criminal law be used as a last resort (*ultima ratio* principle), particularly in view of the fact that efficient security measures could protect information systems much more efficiently than unrestrained criminalization. In that sense, one can only applaud the now pending form of the proposal incorporating the outcome of the proceedings of the Council (Justice and Home affairs on the 10th June 2011), which reintroduces the infringement of security measures as a requirement for the affirmation of illegal access to information systems (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 10).

On the other hand, the provisions concerning illegal system interference (article 4) and illegal data interference (article 5) remain unchanged compared to the framework decision. In addition, only minor discrepancies are traceable with the Council of Europe Convention in this respect. As regards *illegal system interference*, the proposed directive calls for its criminalization "at least for cases which are not minor". That same limitation –albeit not contained in so many words under article 5 of the Council of Europe Convention- derives from the proscribed act itself, which alludes to "serious hindering" of a computer system, thereby rendering the exclusion of minor cases redundant. As regards *illegal data interference*, article 5 of the proposed directive is not identical with article 4 of the Council of Europe Convention. The latter explicitly recognizes that State-parties may reserve the right to require that the conduct result in *serious harm*, while the proposed directive again allows only for the exclusion of *minor* cases. In other words, the Council of Europe Convention also allows for the exclusion of offenses of *average* gravity, thus conceding that other measures, such as administrative sanctions, might be enough to address these. Such choice shows respect for the *ultima ratio* principle, entrusting the pertinent decision with each State-party.

With respect to the novel provision concerning *illegal interception of non-public transmissions of computer data by technical means* (appearing for the first time in an E.U. document), the Council of Europe Convention allows States to only criminalize conduct committed with dishonest intent or in relation to a computer system that is connected to another computer system. In contrast, the E.U. has left no such leeway, the only potential limitation emanating from the proposal by the E.U. Presidency, which excludes minor cases.

The provision of the proposed directive which marks an overly expansive tendency in the E.U. context is article 7, requiring Member States to criminalize "the production, sale, procurement for use, import, possession, distribution or otherwise making available of *any device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences*

referred to in articles 3 to 6 or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed". There are two notable differences between this provision and the corresponding article 6 of the Council of Europe Convention.

The first difference is article 6, par. 2 of the Council of Europe Convention, which provides that the provision of paragraph 1 shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to therein is for the purpose of authorized testing or protection of a computer system. One might contend that such exception is superfluous, as the requisite intent of the offense could *per se* preclude conduct carried out for an authorized testing or protection of a computer system. However, given the fact that the proscribed conduct lies distant from any actual harm to computer systems or data, the above clarification can only be regarded as a positive addition. Besides, article 6, par. 1 of the Cybercrime Convention allows State-parties to require by law a minimum number of tools in order for criminal liability to attach to their possession, a circumstance that is absent from the text of the proposed directive.

Secondly, State-parties to the Council of Europe Convention are free to exclude certain types of conduct from criminalization under article 6, par. 1, which alludes to "*the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed*". Again, one discerns a judicious choice by the Council of Europe, which aims at confining criminalization to the distribution of potentially "threatening" means, such as passwords, which can guarantee access to an information system –or parts thereof- by *their very nature*. None among these limitations, which serve to exclude the use of devices for legitimate purposes from the ambit of criminalization, have been adopted by the E.U. As a result, criminalization largely depends on subjective criteria, which are hard to establish. It is no wonder, then, that consensus has been hard to achieve concerning article 7 of the proposed directive, on account of discrepancies evolving around this matter. The only viable for a compromise derived from the Presidency's proposal, which has been accepted by the Council's outcome of the proceedings on the 10th of June 2011. This proposal suggests not to penalize any longer the conduct of mere possession of such tools and confines criminalization to computer programs that have been designed or adapted primarily for attacks against information systems and computer passwords or access codes, while leaving Member States a mere option with respect to proscribing preparatory acts by means of other devices (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 6, 17 and DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 11).

Adding to the picture, two more elements of the proposed E.U. directive point to the broadness of its ambit: first of all, Member States are required to criminalize even aiding and abetting to the offense proscribed under article 7 (article 8, par. 1). Although this requirement is also present in the Council of Europe Convention (article 11), its effect is mitigated by the discretion granted to State-parties; secondly, Member States are required to criminalize attempt without exceptions (article 8, par. 2), in stark contrast to both the framework decision (exempting attempted illegal access to information systems under article 5, par. 3) and the Cybercrime Convention, recognizing the right of each State-party to not apply, in whole or in part, paragraph 2 concerning attempt (article 11, par. 2 and 3). On the other hand, the exclusion of the offense of article 7 from the ambit of attempt is a positive step (one also taken by the Council of Europe Convention). An additional restriction of the scope of attempt is provided under the Presidency's proposal, which has been accepted by the Council's

outcome of the proceedings (10th June 2011) and confines attempt to the offenses of illegal system and data interference, respectively (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 18).

Last but not least, it is noteworthy that every offense proscribed under the proposed directive is only punishable when committed "without right", an element also found in the framework decision and the Council of Europe Convention. Although the Council of Europe Convention leaves the definition of this notion –hence the decision regarding the broadness of criminalization- to State-parties, article 2(d) of the proposed directive defines it as meaning "access […] not authorized by the owner, other right holder of the system or of part of it, or not permitted under national legislation". From a purely rule-of-law standpoint, such definition appears problematic, as it effectively allows the owner –especially in the case of a contract- to even unduly restrict the free flow of information, which is absolutely essential in a democratic society, thus affecting the limits of the proscribed conduct.

The repression of attacks against information systems as described above shows disregard of the *ultima ratio* and the proportionality principles, as well as lacks coherence even when examined in a strict European context. Adding to this picture, article 13 of the proposed directive (in contrast to article 22, par. 1(d) of the Council of Europe Convention) requires Member States to establish their jurisdiction where the offense has been committed by one of their nationals or a person with habitual residence in the territory of the Member State concerned, even absent double criminality. It thus becomes evident that the E.U. requires its Member States to apply their criminal law extraterritorially, even when the act in question does not constitute a criminal offense where committed. Such jurisdictional overstretching, coupled with the expansion of the limits of criminalization under the proposed directive, create serious concerns even with respect to European citizens. Indeed, when it comes to acts committed in a third country, extending jurisdiction without requiring double criminality would effectively mean that the E.U. is imposing its own views as to the protection of information systems (on the mere grounds of the offender's nationality), even though the prerequisites to the exercise of universal jurisdiction appear to be missing. Ensuing reaction has resulted in reaching a compromise on this point, which is why the E.U. Presidency's proposal and the outcome of the Council's proceedings reintroduce double criminality as a prerequisite to establishing jurisdiction over acts committed in other countries by citizens of member States (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 20-21 and DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 14).

3. On the principle of guilt

a) Does the punishment provided for the instrument relate in a proper way to the actual responsibility of the individual?

See infra

b) Do these sanctions correspond to individual guilt in terms of their type and gravity?

Under the proposed directive, Member States shall specifically ensure that every offense mentioned above (i.e. even the preparatory acts proscribed in article 7) punishable by criminal penalties of a maximum term of imprisonment of at least two years (article 9, par. 2). Aside from undermining the

principle of proportionality, such provision signifies that the E.U. leans towards inflexible sentences, as it distances itself from the framework decision providing maximum terms of imprisonment in a more flexible fashion (e.g. a maximum term of at least 1 to 3 years under article 6, par. 2 of the framework decision). The principle of culpability and proportionality are clearly better served by the abolished provision, in terms of both meting out penalties for each offense and delimiting each particular sentence. The wider the margin of discretion, the easier it becomes for Member States to align each sentence to the corresponding gravity of the offense it attaches to. Adding to the picture, the proposed directive introduces for the first time an inflexible minimum sentence for illegal access to information systems. Overall, it becomes evident that the trend is now to establish more stringent penalties, while reducing the margin of discretion of Member States in delimiting them.

The same reasoning has been applied under article 10 of the proposed directive. The said provision expands the enumeration of aggravating circumstances so as to include commission by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (par. 3), as well as through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage (par. 2), in addition to commission within the framework of a criminal organization (par. 1), which is also provided under the framework decision. Moreover, the proposed directive requires a stricter sentence in the event of the above aggravating circumstances (maximum term of at least 5 years as opposed to 2 to 5 years under article 10, par. 1 of the framework decision) to be imposed in the event of commission of any offense, including preparatory acts proscribed under article 7.

c) Does the legislator explicitly deal with the question whether these sanctions are appropriate having regard to the guilt of the individual?

The proposal has not explicitly dealt with the question whether the above mentioned sanctions are appropriate having regard to the guilt of the individual. This is why, as expected, the above provisions have spawned an adverse reaction, leading the E.U. Presidency to request *Ministers to provide guidance* so as to avoid a stalemate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p.4-5). Two proposals are currently put forward by the Presidency and the Council's outcome of the proceedings: (a) the exemption of preparatory acts from the minimum imprisonment term required; and (b) the restructuring of aggravating circumstances, as well as their confinement to the offenses of illegal system and data interference (articles 4 and 5). The proposed aggravating circumstances include currently: (i) commission of illegal interference through the use of a tool designed or adapted to launch attacks which affected a significant number of information systems (calling for a maximum term of imprisonment of at least three years); and (ii) commission of illegal interference in the framework of a criminal organization or resulting in serious damage or launched against a critical infrastructure information system (calling for a maximum term of imprisonment of at least five years). The misuse of identity data of a third person, when committed in relation to a person other than the perpetrator with the aim of gaining trust of a third party has been deleted (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 18-19 and DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 12). It should be noted that both proposals of the presidency, which have been accepted by the Council, are significant improvements, but still they do not solve all the existing problems with respect to the principles of culpability and proportionality.

4. On the principle of legality

a)If the proposed directive aims at the introduction of a supranational criminal offense:

aa) Do the elements of crimes (objective and subjective) clearly emanate from the text of the proposed directive itself?

(-)

bb) Are the sanctions provided for foreseeable?

(-)

b) If the proposed directive aims at harmonising national criminal law provisions:

aa) To the extent that the obligation to adjust national criminal law does not give any leeway for the implementation (and thus exhaustively defines the criminal offence): Are the objective and subjective prerequisites for criminal liability as well as the sanctions which could be imposed foreseeable (as supra a)?

(-)

bb) Do the national legislators have the possibility to implement each single prescription imposed by the European legislative act in such a concrete manner that this results in a strict and unambiguous provision of national criminal law (please give reasons for the answer using possible examples on how to formulate the implementing law)?

The proposal doesn't fulfill the requirements of the legality principle. In particular:

(1) the proposed directive does not even attempt to delimit the notion of 'interception', thus creating ambiguity. Likewise, the Council of Europe Convention contains no definition of 'interception' either. That being noted, it should be emphasized that the institutional framework introduced under the Lisbon Treaty authorizes the E.U. to establish minimum rules concerning the definition of offenses, which inherently calls for strict and unambiguous provisions, permitting an accurate transposition into domestic law. Besides, a mere look at the explanatory report to the Convention on Cybercrime suffices to demonstrate the need for a comprehensive definition, as the Council of Europe interprets it so as to include, among other things, the monitoring or surveillance of the *content* of communications.

(2) The same is true of the device (or even computer program), which is *primarily* designed or created to commit an offence proscribed under articles 3-6 (see art. 7). Inasmuch as these devices can be put to various uses, it is practically impossible to discern whether they primarily serve the proscribed purpose. Such vagueness can only be cured by replacing this element with the requirement that the device be exclusively designed to commit these offences. Indeed, when it comes to preparatory acts, the threshold of clarity is much more elevated. Besides, the proscribed types of conduct should be confined to those which are suitable to express the element of aiming at the commission of the offences contained in articles 3 to 6.

(3) As regards the aggravating circumstances provided under article 10, par. 3, it is unclear what sort of *harm* to the rightful identity owner might justify the doubling of the minimum limit of the maximum sentence. Could some kind of *moral harm* justify such aggravation of the sentence? In case this provision wouldn't have been deleted from the Presidency's proposal and the Council's outcome of the proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 11), it would have been necessary for the European legislator to make clear the specific notion of harm, so that it would be possible to evaluate the pertinent rules in light of the principle of proportionality.

(4) the proposed directive does not delimit the notion of "minor cases", which can be excluded from criminal offences by the Member States. On the one hand, this leaves Member States some room to make their own decisions, which is welcome as such; on the other hand, however, it must be made clear that it leaves national legislatures with no information about what the content of minor cases should be according to the EU. Thus, the minimum rule of the pertinent criminal offences concerning attacks against information systems can differ from one Member State to another. In other words, minimum European rules for certain criminal conduct are not only determined by the objective and the subjective elements described in a directive calling Member States to punish the certain conduct (see in this direction the understanding of the Commission, COM 2010, 517 final, p. 7-8), but are also determined based on the margin left for the introduction of possible exceptions thereto. The EU should therefore show, at least in terms of an indicative enumeration, what are minor cases in the field of attacks against information systems. This has been done in the recent presidency's orientation debate, which has been accepted by the Council's outcome of the proceedings (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 10 and DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 5 respectively), but it has been incorporated only in the preamble of the proposed directive (Nr. 6a "The case may be considered minor, for example, when the damage and/or the risk it carries to public or private interests, such as the integrity of a computer system or computer data, or a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary"),being insufficient in terms of its binding force. One should therefore integrate the pertinent explanation of minor cases in article 2 of the proposed directive, which contains the definitions.

As far as *penalties* are concerned, it has been argued above that the provisions of the proposed directive lean towards inflexible sentences (i.e. the criminal conducts are punishable by criminal penalties of a maximum term of imprisonment of at least two years, art. 9 par. 2), as they distance themselves from those of the framework decision providing maximum terms of imprisonment in a more flexible fashion (e.g. a maximum term of at least 1 to 3 years, art. 6 par. 2 of the FD). Such a choice makes the provision of the penalties absolutely certain, but at the same time it fails to fully serve the principles of guilt, proportionality and coherence (the latter meant as the coherence of the national legal orders).

c) Does the proposed directive introduce retroactive rules, or does it compel member States to introduce such rules?

(-)

d) Is any potential retroactivity justified with reference to the principle of lex mitior?

(-)

e) Have national Parliaments, organizations, and citizens been informed of the proposed directive in a timely and comprehensive manner, and have they been given a reasonable possibility to voice their own opinion?

According to the Commission (COM 2010, 517 final, p. 5):

"A broad range of experts in the field have been consulted in a number of different meetings dealing with various aspects of the fight against cybercrime, including the judicial follow-up (prosecution) of these crimes. They included, in particular, representatives of Member States' Governments and the private sector, specialised judges and prosecutors, international organisations, European agencies and expert bodies. A number of experts and organisations have subsequently sent in submissions and provided information".

As the proposal has proved to be quite problematic (see the recent presidency's orientation debate on it, DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011), it would have been wise for the consultation process to be improved, especially in terms of a broader consultation of experts in the field of European criminal law.

5. On the principle of subsidiarity

a) Why is it not enough with criminal law measures at Member State level?

See infra, under c.

b) Why is the objective of each measure –whether in terms of ist scope or ist impact- better served on a European level?

See infra, under c.

c) Does the EU legislator deal with the question of subsidiarity and is there an explicit and detailed evaluation of the fulfilment of this requirement in Union acts – taking into account all the alternatives and weighing all circumstances?

The subsidiarity principle is rather extensively addressed in the proposal:

"The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reasons: Cybercrime and, more specifically, attacks against information systems have a considerable cross-border dimension, which is most obvious in large scale attacks, as the connecting

elements of an attack are often situated in different locations and in different countries. This requires EU action, in particular to keep abreast of the current trend towards large scale attacks in Europe and in the world. Action at EU level and an update of the Framework Decision 2005/222/JHA have also been called for in the Council Conclusions of November 200816, as the objective of effectively protecting citizens from cybercrimes cannot be sufficiently achieved by Member States alone.

Action by the European Union will better achieve the objectives of the proposal for the following reasons: The proposal will further approximate the substantive criminal law of Member States and the rules on procedure, which will have a positive impact on the fight against these crimes. Firstly, it is a way of preventing offenders from moving to Member States in which legislation against cyber attacks is more lenient. Secondly, shared definitions make it possible to exchange information and collect and compare relevant data. Thirdly, the effectiveness of prevention measures across the EU and international cooperation are also enhanced.

The proposal therefore complies with the subsidiarity principle" (COM 2010, 517 final, p. 8).

Observance of this principle appears rather unproblematic because of the typical cross border dimension, which characterizes the attacks against information systems, as they are usually carried out through the internet, thus being unrestrained by national borders. Still, as mentioned above, the lack of empirical data has been made clear in the proposed directive (section 13 of the preamble), demonstrating the significant deficiencies of a substantial control mechanism for the preservation of the subsidiarity principle.

d) Have national Parliaments expressed their views as to the preservation of the subsidiarity principle and, if so, what was their opinion? Has the EU legislator explicitly considered these arguments?

The existing documents do not give relevant information.

6. On the coherence of domestic criminal justice systems

a) Do the criminal law provisions of the proposed directive undermine the coherence of the criminal justice system of one or more member States?

The above mentioned inflexible choice made by the proposal in relation to the maximum term of imprisonment proscribed in relation to the different offences for the national legislators may well lead to inconsistency of the national penal systems as described already.

b) In terms of systematicity and substantive content, is the proposed directive in line with other EU legislative acts related to criminal law?

The Commission refers to the consistency of its proposal with other policies and objectives of the Union as follows: "The objectives are consistent with EU policies on combating organised crime,

increasing the resilience of computer networks, protecting critical information infrastructure and data protection. The objectives are also consistent with the Safer Internet Programme which was set up to promote safer use of the Internet and new online technologies, and to combat illegal content." Such statements, however, are so general that one cannot possibly trace any substantial effort to justify the observance of the above principle therein.

c) Does the EU legislator deal with the question of horizontal and vertical coherence, and is there an explicit and detailed explanation as to whether the proposed directive does not undermine the coherence of domestic criminal justice systems or at least whether any such undermining is inevitable – particularly in view of the obligation to respect the national identity of each member State?

What is remarkable in the proposal is the discrepancy between the justification of the subsidiarity principle and that of the proportionality principle, which is tightly connected with the fulfilment of coherence as well. The Commission notes pertinently: "This Directive confines itself to the minimum required in order to achieve those objectives at European level and does not go beyond what is necessary for that purpose, taking into account the need for accuracy of criminal legislation" (COM 2010, 517 final, p. 8).

In the field of criminal law, the EU should observe the principle of proportionality, which is closely linked to the principle of coherence, in two aspects: on the one hand, proportionality in terms of distinguishing between penalties for offences emanating from harmonized or harmonizing criminal acts attacking different legal interests (e.g. the penalties threatened against trafficking in human beings ought to be different than those opposable to offences against property) (vertical proportionality of European criminal law, aimed at preserving the latter's coherence); on the other hand, proportionality of specific penalties weighed against the harmfulness of the conduct which is to be harmonised as a criminal act and its aggravating circumstances (*stricto sensu* proportionality between the act and its punishment). In the context of the proposal for a directive concerning attacks against information systems, the Commission has failed in both these aspects. Thus, at least the initial proposal of the directive appears deficient in terms of both the principle of proportionality and the principle of coherence. Some improvement can be noted, though not in terms of justifying the concrete decisions taken, especially as related to the differentiation of the levels of punishment between the different aggravating circumstances in the recent outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011).

OVERALL EVALUATION

☐ The legislative act **fully complies with** the requirements of the Manifesto on European Criminal Policy.

☐ The legislative act **satisfies essentially** the requirements of the Manifesto on European Criminal Policy. Alterations or improvements are required only on certain points (see recommendations).

☐ The legislative act meets **only partially** the requirements of the Manifesto on European Criminal Policy. Significant alterations or improvements are required (see recommendations).

☒ The legislative act **does not substantially meet** the requirements of the Manifesto on European Criminal Policy. Extensive and structural alterations are required (see recommendations)**.**

☐ The legislative act **does not meet at all** the requirements of the Manifesto on European Criminal Policy. The proposal/enactment of such a legal instrument must be wholly reexamined (see recommendations).

The above analysis of the rules concerning the criminalization of attacks against information systems as adopted by the Council of Europe and the E.U.'s proposal, respectively, allows us to draw a conclusion relying on the following elements:

In its effort to amend its regulatory framework concerning criminal repression of attacks against information systems, the E.U.'s proposal did not pay enough heed to the *ultima ratio* principle. Such principle, which directly emanates from the principle of proportionality, is well-founded in E.U. law and would protect against inhibiting technological innovation or blocking the free flow of information. Taking into account the numerous possibilities for restricting criminalization as mandated under the Council of Europe Convention, one would indeed expect the E.U. to strive for more balanced solutions in repressing cybercrime, especially after the Lisbon Treaty, which enables it to bind its Member States–on grounds of majority vote- to minimum rules concerning the definition of offenses and criminal sanctions, i.e. impose its own dictates as to the distinction between those acts that deserve punishment and those that do not.

A close look at the preamble to the proposal for a directive reveals the actual reasons behind the choices made. Prominent among the grounds for adopting the directive is the need to fight organized crime and terrorism, and sec. 2 of the preamble notes the increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. Interestingly, however, the preamble also underlines (sec. 12) the need to collect data on offenses under the directive, *in order to gain a more complete picture of the problem at a Union level*. It becomes evident that hasty resort to repressive means – and indeed in the broadest terms possible- absent *a complete picture of the problem* deprives the proposal of any legitimizing basis. It seems as though the declared goal of eliminating significant gaps and differences in member States' laws in the area of attacks against information systems in order to facilitate the fight against organized crime and terrorism, as well as achieve effective police and judicial cooperation in this area (preamble, sec. 13) has once more drawn the E.U. to policies that are not necessarily compatible with rule-of-law principles governing criminal law on a European level. Besides, the repression of attacks against information systems carried out in the context of organized

crime or terrorism would require nothing more than *special provisions* designed to address these acts, as opposed to a blanket extension of criminal law rules.

On the other hand, the proposal for a directive –especially in its initial form- neither ensures respect for fundamental rights recognized under the Charter of Fundamental Rights of the European Union nor observes Union law principles, despite the preamble's reassurance to the contrary (sec. 16). Indeed, the definitions contained in the proposal do not conform to the *lex certa* requirement, which is also applicable on a European level. Two pertinent examples would be the ambiguous notion of 'interception', as well as the indeterminacy surrounding 'minor cases', which are to be excluded from criminalization. The principle of proportionality on its part is also undermined: how can proportionality be respected when the maximum sentence is doubled on the grounds of participation in a criminal organization, despite the fact that the latter is punishable *per se*? How can proportionality possibly be served, when Member States are left with virtually no margin of discretion in determining applicable sentences, thus being deprived of any competence to introduce variations based on the harm caused to different legal interests within the particular context of their own legal order?

Last but not least, there is a valid concern about broadly criminalizing preparatory acts, such as the production of tools employed to commit pertinent offenses. The problem is that the proposed directive (just like the Council of Europe Convention) also proscribes tools that are not by their very nature designed for the sole purpose of attacking information systems. Coupled with the distance between these acts (i.e. the production of such tools) and the actual attack, it becomes evident that criminalization of this conduct is not associated with a tangible threat to information systems, thus risking punishment over one's mere intent. The fact that the E.U. (unlike the Council of Europe) does not leave room for limitations in this field, makes things even worse. This is why extensive and structural alterations of the proposed directive are required.

RECOMMENDATIONS FOR THE AMENDMENT OF SPECIFIC PROVISIONS OF THE PROPOSED DIRECTIVE:

1. It is recommended that **article 2** of the proposed directive be amended so as to: a) include a definition enumerating –at least in an indicative fashion- **minor cases** alluded to under paragraph 6(a) of the preamble, which is about to be complemented based on the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011) ("The case may be considered minor, for example, (…) when the damage and/or the risk it carries to public or private interests, such as the integrity of a computer system or computer data, or a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary"); b) adequately delimit the proscribed **technical means** by which illegal interception (article 6) is carried out, taking into account the pertinent section of the explanatory report to the Council of Europe Convention on Cybercrime (sec. 53: «Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes»); c) specify that the element "without right", when connoting "not authorized by the owner or other right holder of the system", is only fulfilled "inasmuch as the withholding of such authorization does not constitute an abuse of right». All three amendments aim at ensuring respect for the principle of legality on a European level.

2. It is recommended that **article 3** of the proposed directive be amended according to the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 26) and the respective outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 10), so as to require "the infringement of a security measure" as an element of "illegal access to information systems". This would ensure respect for the *ultima ratio* principle (see).

3. It is recommended that **article 6** of the proposed directive adequately delimit the contours of "illegal interception", so as to satisfy the principle of legality. Such a delimitation could take place based on the explanatory report to the Council of Europe Cybercrime Convention (par. 53), according to which: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording".

4. It is recommended that **article 7** of the proposed directive be eliminated, as it proscribes conduct that lies quite distant from any perceived harm –or even threat of harm- to information systems, thereby criminalizing mere intent (which is itself hardly discernible in the proscribed acts). Should article 7 be retained, it is recommended that its ambit be drastically limited based on four amendments: a) confining the proscribed acts to tools or devices designed for the sole purpose of attacking information systems (or even certain types thereof, such as computer programs); b) excluding mere possession from the ambit of criminalization according to the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 6, 17) and the respective outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 11); c) introducing an exception in minor cases according to the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 3) and the respective outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 11); and d) explicitly excluding cases in which the proscribed acts are carried out with the purpose of controlling or protecting information systems (see article 6 par. 2 of the Council of Europe Convention on Cybercrime: «This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system»).

5. It is recommended that **article 9, par. 2** of the proposed directive exempt the acts proscribed under article 7, so that preparatory acts are not threatened with the same penalty as the offensive conduct itself, following the recent presidency's proposal (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 18) and the respective outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 11). In addition, member States should be allowed some discretion in delimiting the lowest maximum limit of the punishment to be imposed (e.g. 1-3 years), as is the case with the existing framework decision. Both these amendments aim at ensuring respect for the principle of proportionality, as well as for the coherence of domestic criminal justice systems.

6. It is recommended that **article 10** of the proposed directive (concerning aggravating circumstances and recently incorporated in Art. 9 par. 3-4) be amended so as to: a) not contain an

aggravating circumstance in the event of commission within the context of a criminal organization, as participation in a criminal organization as such constitutes a criminal offense in the Member States (subsequent a pertinent framework decision as well as a joint action dating back to 1998), thereby addressing the same circumstance by means of multiple counts; b) as opposed to the aggravating circumstance consisting in commission "through the use of a tool designed to launch attacks affecting a significant number of information systems or attacks causing considerable damage", include an aggravating circumstance whose application shall require "the above mentioned tools to have affected a significant number of information systems or to have caused a serious damage" according to the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 19) and the outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 12). Aggravating circumstances might also include the attack against information systems which are part of critical infrastructures; c) not contain the aggravating circumstance of commission "by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner" (see also the recent presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 19, and the outcome of the Council's proceedings, DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 12), to the extent the latter can be addressed by means of the exact penalty that will be imposed and by means of charging the perpetrator with a possible offence against the rightful identity owner; d) distinguish between various aggravating circumstances in terms of the penalty to be imposed according to the Presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 18-19) and the outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 12), given that the different aggravating circumstances do not reflect conduct of the same gravity); e) allow some discretion to the Member States in delimiting the maximum limit of the punishment to be imposed (as opposed to providing for a fixed lowest maximum term of imprisonment). These amendments are necessary to ensure respect for the principle of guilt and the principle of proportionality, as well as for the coherence of domestic criminal justice systems.

7. Last but not least, it is recommended that **article 13** of the proposed directive link the exercise of extraterritorial jurisdiction to the requirement of double criminality following the presidency's orientation debate (DROIPEN 27, TELECOM 43, CODEC 609, 8.4.2011, p. 20-21) and the outcome of the Council's proceedings (DROIPEN 62, TELECOM 95, CODEC 1025, 15.6.2011, p. 14).