# Criminalizing attacks against information systems in the EU – The anticipated impact of the European legal instruments on the Greek legal order

M. Kaiafa-Gbandi
Professor of Criminal Law – A.U.TH.

## 1. Introduction

Admittedly, information technology has radically and irrevocably changed modern societies. In technologically advanced countries, information systems have infiltrated virtually every sector of social life to such an extent as to redefine both State and individual activities. Government, national defense, communications, transportation, health systems, education, and entertainment are but a few among many fields administered by the so-called "information society".[1] Personal computers on their part have affected the everyday lives of all citizens, as evidenced for instance in the widespread use of e-mail and the dissemination of information on the worldwide web.

The unprecedented economic and social changes brought about by these developments have rendered information systems –as well as the data circulated therein- fundamental interests worthy of protection. This only makes sense, given the implications of the potential abuse of an information system: a mere click of the mouse can cause massive power outages, cancel out copious scientific efforts, and even bring about nuclear holocaust through the breach of information systems running nuclear reactors. Without a doubt, this dark side of information systems might be the single most important challenge information society has to face.[2]

It soon became clear that the applications of information technology had to be accompanied by pertinent regulation.[3] As far back as the '80s, a number of legal orders recognized information systems as fundamental interests worthy of protection, and adopted criminal law rules to proscribe their breach.[4]

The rapid growth of the worldwide web has made it palpable that the impact of criminal conduct against information systems is unrestrained by national or geographic boundaries, hence ringing an alarm for the international community.[5] Considering that malicious viruses can be unleashed from anywhere in the world, no viable solution can be achieved in the absence of international cooperation. This is especially true of a supranational organization like the E.U., which aspires to establish a common area of freedom, security and justice (articles 67 and 82 *et seq*. TFEU) also by addressing serious crime with a cross-border dimension (article 83, par. 1 TFEU),[6] including cybercrime. Besides, the approximation of domestic criminal law in this field is the first step towards achieving harmonized approaches in the field of procedural law, as well as facilitating judicial cooperation.

It becomes evident that, when it comes to the criminal law protection of information systems, European and international initiatives become central, as they largely determine the position of national legislatures.

## 2. The European and international institutional framework concerning attacks against information systems

### 2.1. A comparative survey of a complex framework

The Council of Europe Convention on Cybercrime is probably the most important instrument on the international plane.[7] The said convention requires State-parties to proscribe not only *stricto sensu* computer crimes[8] –i.e. those posing a direct threat to information systems and digital data- but also other types of crime perpetrated by means of a computer (such as computer fraud), including content-related crime (such as child pornography). Despite its flaws,[9] the Convention on Cybercrime has thus emerged as the most comprehensive instrument in the international fight against cybercrime,[10] owing in part to its provisions on procedure and judicial cooperation.

Although the E.U. itself is not a signatory party to the Convention, all of its member States have signed it, while most of them have already ratified it. In fact, the European Commission "actively encourages" the remaining member States to ratify the Convention as soon as possible,[11] despite the adoption of a framework-decision on attacks against information systems in 2005,[12] which is about to be replaced by a pertinent directive, owing to the novel institutional framework introduced by the Lisbon Treaty.[13]

States which happen to be members of both the Council Europe and the E.U. are therefore faced with the dual challenge of harmonizing their domestic law to the Convention on Cybercrime and the framework-decision alike.[14] Yet the E.U. might not realistically dispense with the need of proposing a legal instrument of its own by merely becoming a party to the Council of Europe Convention. This is because a supranational organization such as the E.U. is in a much better position to bind its member States to follow its dictates; in addition, it can expand the proscribed types of conduct, adjust the applicable rules to correspond to ever-evolving needs, and determine not only "what" will be punished but also "how" it will be punished.[15] In doing so, it is to keep an eye open for initiatives by the Council of Europe affecting its member States, so that it may align its actions accordingly.

It follows that States like Greece had better subscribe to a comparative approach, starting from the upcoming E.U. directive, while keeping to both the existing framework-decision and the Council of Europe Convention on Cybercrime.

### 2.2. The reasons for a new proposed E.U. directive and the core questions arising in a comparative context

On September 30, 2010, the Commission came up with a proposed directive on attacks against information systems, aiming at replacing the existing framework-decision 2005/222/JHA.[16] Less than one year before, the Lisbon Treaty had come into effect, by virtue of which the E.U. was granted the authority to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension based on qualified majority (article 83, par. 1 TFEU).[17]

The declared reason for this initiative was “emerging threats highlighted by recent attacks across Europe since the adoption of the framework decision, in particular the emergence of large-scale simultaneous attacks against information systems and the increased criminal use of the so-called 'botnets'”.[18] These factors, which had not attracted attention by the time the framework decision was adopted, prompted the Commission to seek more effective ways of addressing the threat. According to the Commission, “the main cause of cybercrime is the vulnerability of information systems resulting from a variety of factors, while insufficient response by law enforcement mechanisms contributes to the prevalence of these phenomena, and exacerbates the difficulties, as certain types of offences go beyond national borders. Furthermore, variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with. Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions.”[19] In this new environment, the Commission has attempted to formulate its proposal,[20] taking into account novel forms of cybercrime, including the use of botnets.[21]

On the other hand, the proposed directive explicitly relies on the Council of Europe Convention on Cybercrime, which is in fact regarded as important enough as to prompt the Commission to actively encourage its ratification by those member States which have yet to do so.

The aforementioned proposed directive poses three core questions:
(i) How are criminal law provisions to be delineated to address attacks against information systems, and what are the new provisions in comparison with the existing framework decision?
(ii) What is the relationship between the proposed E.U. directive with the pertinent provisions of the Council of Europe Convention on Cybercrime?
(iii) Last but not least, what is the underlying foundation of the choices made in this proposal, placed in the context of fundamental principles of European criminal law after the Lisbon Treaty?[22]

Answering these questions is a prerequisite to shedding some light on what the international framework on attacks against information systems –and especially the proposed directive- entail for the Greek legal order.

### 2.3. A comparative survey of the criminal law rules on attacks against information systems on a European and international level

#### 2.3.1. An initial approach

As already noted, the Commission proceeded to its proposal for a new directive on attacks against information systems, because it deemed the existing framework decision deficient in terms of addressing the full array of cybercrime, safeguarding against large-scale attacks, and providing for adequate sanctions.[23]

Specifically, the proposed directive requires member States to proscribe two additional types of conduct (in line with the Council of Europe Convention), namely

the illegal interception of computer data (article 6) and the production, sale etc. of tools used for committing computer offenses (article 7), in addition to the ones already covered (illegal access to information systems – article 3; illegal system interference – article 4; illegal data interference – article 5). Even with regard to conduct already covered by the framework decision, the proposal introduces changes pertaining to incitement, aiding and abetting, attempt (article 8), and especially applicable penalties (articles 9 to 12), including aggravating circumstances (article 10). In terms of procedural matters, the proposal introduces provisions on jurisdiction (article 13), as well as exchange of information (article 14), requiring member States to ensure that they have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered. At the same time, the proposal requires the establishment of a system for the recording, production and provision of statistical data on the offences referred to in articles 3 to 7 (article 15).

### 2.3.2. Proscribed types of conduct

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*, 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.[24] 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".[25] 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),[26] particularly in view of the fact that efficient security measures could protect information systems much more efficiently than unrestrained criminalization.[27] In that

sense, one can only applaud the now pending proposal by the E.U. Presidency (incorporating a provisional agreement between certain member States), which reintroduces the infringement of security measures as a requirement for the affirmation of illegal access to information systems.[28]

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.[29] Such choice shows respect for the *ultima ratio* principle,[30] 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.[31] Aside from this deficiency, the proposed directive does not even attempt to delimit the notion of 'interception', thus creating some 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.[32] 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.[33]

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, 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 that a number of tools be possessed before criminal liability attaches to their use, 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,[34] 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.[35] It is no wonder, then, that consensus has yet to be arrived at concerning article 7 of the proposed directive.[36] The only viable for a compromise derives from the Presidency's proposal, which suggests confining criminalization to essentially software that has been designed for attacks against information systems and passwords, while leaving member States a single option with respect to proscribing preparatory acts by means of other devices.[37]

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 confines attempt to the offenses of illegal system and data interference, respectively.[38]

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 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".[39] From a purely rule-of-law standpoint, such definition appears problematic, as it effectively allows the owner to unduly restrict the free flow of information,[40] which is absolutely essential in a democratic society, thus affecting the limits of the proscribed conduct.

### 2.3.3. Criminal sanctions

In the exercise of the E.U.'s newly-recognized competence to establish minimum rules concerning penalties, the proposed directive contains specific sentences to be imposed, going further than article 13 of the Cybercrime Convention, which is confined to declaring the need for effective, proportionate and dissuasive sanctions. In addition, there are demonstrable differences even compared to the existing framework decision, leading to an overall strengthening of criminal repression.

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).[41] 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 proportionality is clearly better served by the abolished provision, in terms of both meting out penalties for each offense and delimiting each particular sentence.[42] 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.[43] To begin with, 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 7, par. 1 of the framework decision) to be imposed in the event of commission of any offense, including preparatory acts proscribed under article 7.

As expected, the above proposals have spawned an adverse reaction, leading the E.U. Presidency to request *Ministers to provide guidance* so as to avoid a stalemate.[44] Two possible solutions are currently put forward by the Presidency: (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).[45] The proposed aggravating circumstances include: (i) commission of illegal interference through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage (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 harm 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 is included as an aggravating circumstance, without envisaging a specific level of penalty, when committed in relation to a person other than the perpetrator with the aim of gaining trust of a third party.[46]

### 2.3.4. Regulating jurisdiction

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.[47] 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 so far prevented a compromise on this point, which is why the E.U. Presidency is now attempting to reintroduce double criminality as a prerequisite to establishing jurisdiction over acts committed in third countries by citizens of member States.[48]

### 2.3.5. Assessing the E.U. policy on criminalizing attacks against information systems in a comparative context

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., 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. 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[49] and would protect against inhibiting technological innovation or blocking the free flow of information. 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 to minimum rules concerning the definition of offenses and criminal sanctions.[50]

A close look at the preamble to the proposal for an E.U. directive[51] 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 –at least in its initial form- neither ensures respect for fundamental rights nor observes the principles recognized by the Charter of Fundamental Rights of the European Union, 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.[52] 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.[53] The principle of proportionality[54] on its part is also undermined: how else could it be, when the required sentence applicable to preparatory acts is the same as that attaching to regular offenses? How is proportionality respected, when the maximum sentence is doubled on the grounds of employing devices that can cause serious harm, regardless of whether the harm has occurred, or 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 gravity of each particular case?[55] The answer to these questions is simple: not only is the principle of proportionality not served, it is outright violated.

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 to attack information systems. Coupled with the distance between these acts 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.[56] The fact that the E.U. (unlike the Council of Europe) does not leave room for limitations

in this field, coupled with the recognition of extraterritorial jurisdiction absent double criminality, makes things even worse.

Thus, serious concerns in view of the transposition required by member States, which might even trigger invocation of the emergency break clause provided under article 83, par. 3 TFEU. It becomes imperative, then, to support and complement the Presidency's proposals, which can improve the proposed directive in terms of preserving the *ultima ratio* principle, as well as the principles of legality, proportionality, and respect for each member State's domestic legal order. Necessary corrections would include defining 'illegal interception', amending the provisions on penalties, aggravating circumstances, and jurisdiction, as well as drastically narrowing down the scope of article 7 concerning preparatory acts.

Even though lack of a compromise means that the regulatory framework has yet to be crystallized on the E.U. level, it is in order to examine what would be the potential implications for our domestic legal order, at least based on the tentative agreement which has emerged so far.

## 3. The proposed directive and the Greek legal order: points of convergence and some pertinent problems

Once the proposed directive is officially adopted, it will require both the amendment of existing provisions and the introduction of new ones into Greek law.

In particular, *illegal access* to computer data (including data stored in peripheral devices or transmitted through telecommunications systems) without a right is currently punishable under article 370$^{quater}$, par. 2 of the Greek Criminal Code[57] [hereafter CC] by imprisonment of up to 3 months or a fine of at least 29 €, unless the act jeopardizes the international relations or national security, in which case it is charged in the vein of espionage under article 148 CC. On the other hand, article 370$^{ter}$, proscribing interception of computer data, is narrowly interpreted so as to only address classified data (such as State, scientific or professional data),[58] thus covering cases such as industrial espionage (punishable with imprisonment of up to 3 months). Illegal access to specific types of computer data is proscribed under two criminal statutes: statute no. 2472/1997 on the protection of personal data (article 22, par. 4), and statute no. 3471/2006 on the protection of personal data and privacy in the electronic telecommunications sector (articles 4, par. 2 and 15, par. 1).[59] These statutes essentially provide for harsher penalties, while they even proscribe negligent offenses (article 22, par. 8 of statute no. 2472/1997, and article 15, par. 4 of statute no. 3471/2006).

Based on the above, Greek law addresses illegal access to computer data based on the combination of criminal law provisions and special statutes.

Keeping in mind article 3 of the proposed directive, Greek law will have to be amended in three directions so as to meet the dictates of the E.U.:
(i) rephrase article 370$^{quater}$, par. 2 CC so that it covers illegal access to information systems alongside illegal access to data;[60]
(ii) adjust the sentence, so that its maximum limit is at least 2 years; and

(iii) exempt minor cases from the ambit of the provision, providing an adequate delineation of 'minor cases'.[61]

In addition, should 'infringement of security measures' ultimately become an element of the directive, its incorporation into Greek law would be highly advisable,[62] particularly in view of the sentence to be imposed.

Based on these amendments, the introduction of aggravated forms of the offense should further be examined, particularly as regards illegal access to classified data, such as those currently covered under article 370[ter] CC.[63] At the same time, transposition will have to take into account coordination with statute nos. 2472/1997 and 3471/2006 concerning illegal access to digital personal data or personal data transmitted via electronic telecommunications.

On the other hand, *illegal system interference*, i.e. the intentional serious hindering or interruption of the functioning of an information system, e.g. by inputting or rendering inaccessible computer data (article 4 of the proposed directive) should be included in a separate provision,[64] as its key element lies not in the potential damage to the system, but rather to the data itself. Again, it would be wise to exempt minor cases, especially in view of the 2-year sentence requirement (even though this coincides with the sentence for criminal property damage under Greek law).

As regards *illegal data interference*, namely the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system (article of the proposed directive), it would also require the introduction of a separate provision.[65] Indeed, such conduct is currently addressed only to the extent electronic documents are protected under the Criminal Code (article 13(c) CC).[66] Pertinent offenses would be forgery (article 216 CC), spoliation (article 222 CC), or even breaches of personal data or intellectual property rights (article 22, par. 4 of statute no. 2472/1997, article 15, par. 1 of statute no. 3471/2006, and article 66, par. 1 of statute no. 2121/1993, respectively), while possible material damage might call for the application of article 381 CC proscribing criminal damage to property.[67] Although it is true that these provisions do not adequately address the full extent of data interference,[68] the new provision should exempt minor cases.

Lastly, *illegal interception by technical means of non-public transmissions of computer data* (article 6 of the proposed directive), including the monitoring, surveillance or even the recording of content as per the Council of Europe, would also require the introduction of a new provision. Indeed, neither article 370[ter] nor article 370[quater], par. 1 CC aspire to protect privacy in terms of communications[69] or cover the full array of acts proscribed under the proposed directive. On the contrary, article 6 of the latter covers transmissions even within a computer system, which goes beyond cases of communication between two persons.[70] The same provision –just like article 3 of the Cybercrime Convention- also proscribes the interception of electromagnetic emissions from an information system carrying computer data.[71] Such electromagnetic emissions can be captured without right, thereby enabling the culprit to record data at any point in time.[72] It follows that article 6 of the proposed directive covers a broad range of cases involving interception even absent communication between individuals. Its transposition into Greek law would have to take into account article 15

of statute no. 3471/2006, which refers to the protection of electronic telecommunications.

Given the need to incorporate the offenses of illegal system and data interference, as well as illegal interception of data, it might be suitable to create a *distinct chapter* in the Criminal Code on attacks against information systems, which would include articles 370$^{ter}$ and 370$^{quater}$ (in their amended forms). This would highlight the confidentiality, integrity and availability of information systems and data as a distinct fundamental interest worthy of protection by criminal law.[73] At the same time, it would be in order to include a clear-cut definition of "information system" and "computer data" under article 13 CC, based on the definitions contained in the proposed directive and the Council of Europe Convention.[74]

The greatest problem to be faced by the Greek legal order would admittedly relate to the incorporation of article 7 of the proposed directive, proscribing the preparatory acts of production, sale, procurement for use, import, possession, distribution or otherwise making available of devices employed to commit any of the above offenses. The two issues raised concern the extent of criminalization and the imposition of the same penalty applied to the other offenses. Even assuming the latter problem is eliminated based on the Presidency's proposal,[75] the former will still have to be addressed. To the extent the Presidency's proposal retains a blanket provision covering computer software designed or adapted to facilitate the commission of any of the offenses to be proscribed in the directive,[76] the problem of excessive criminalization indeed remains. Unless the provision in question is eliminated, domestic law will have to narrow down its scope by appropriately delineating the notion of acting "without right".

One way to achieve this would be to introduce an additional element, namely that the production, sale, etc. of software capable of attacking information systems (as described in article 7 of the proposed directive) be carried out 'without a right'. Aside from contributing in putting together a list of software applications that pose a genuine threat to information systems (which would enable the outlawing of some of them), such element would help keep tabs on those producing or selling these applications, thus enabling the introduction of variations of the offensive conduct. Accordingly, any person producing or selling them with permission would not incur criminal liability, at least not until launching an attempt against an actual information system. On the other hand, lack of a permit would not necessarily connote that the person is acting without a right; indeed, such right might derive from other exceptional circumstances precluding wrongfulness, such a state of necessity or even self-defense.

In addition, domestic law should follow the example of article 6, par. 2 of the Council of Europe Convention and explicitly state that every act proscribed in article 7 of the proposed directive is justified (even absent a permit) if carried out for the purpose of authorized testing or protection of a computer system. Such a clause would not contradict the proposed directive, as the latter indeed requires a special intent which is all but absent in the situations described above.

In point of fact, one might consolidate the two limitations into a clause exempting the procurement of the applications in question by the authority issuing permits,

providing that such procurement shall take place for the purpose of authorized testing or protection of a computer system in the context of personal or professional use.

Finally, it must be said that the Presidency's proposal[77] on aggravating circumstances largely addresses the problems related to the principle of proportionality in an effective manner. Even so, article 187, par. 1 CC (concerning participation in a criminal organization) would have to be updated so as to include the purpose of system or data interference. Should that amendment take place, there would be no actual need to introduce the aggravating circumstance encompassed under article 10, par. 1 of the proposed directive, as the cumulative charges for participation in a criminal organization and illegal system or data interference would ensure aggravation of the penalty anyway.

## 4. Instead of a conclusion

The above analysis makes it plain that the task of E.U. member States in adopting criminal law rules within an international context focused on the combating of cross-border crime is not an easy one. In the post-Lisbon era, the Union's ability to bind its member States has been extended so as to allow it to not only establish minimum rules concerning the definition of offenses, but also to partly determine the applicable sentences. It therefore becomes imperative for national delegations –if not parliaments themselves- to actively engage in the lawmaking process, so that fundamental principles of criminal law are better served, and the E.U. may achieve its declared goal, i.e. place the individual at the heart of its activities.[78]

[1] See indicatively *Furnell* (2006), Cybercrime – Vandalizing the information society, 1 ff., *Gercke,* Herausforderungen bei der Bekämpfung der Internetkriminalität, in *Gercke*, and *Brunst* (2009), Praxishandbuch Internetstrafrecht, 7-9; *cf*. the Explanatory Report to the Cybercrime Convention by the Council of Europe, paras. 1-6.
[2] *Cf*. the analysis of *Sieber*, Computer crimes, cyber-terrorism, child pornography and financial crimes, in Spinellis D. (ed.) (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, 14 ff.
[3] For a survey of pertinent developments through time see, inter alia, *Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Arm, 1059, with further citations.
[4] Articles 370$^{ter}$ and 370$^{quater}$ were introduced into the Greek Criminal Code in 1988, while German law had incorporated similar provisions by virtue of a statute dated 15.5.1986 (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität – 2. WiKG).
[5] See the Explanatory Report to the Cybercrime Convention, paras. 5-6, and *Gercke* (2010), Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, CRi, 75.
[6] On the pertinent competence of the E.U. see indicatively *Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 29 ff.
[7] See CETS No. 185, Budapest, 23.XI.2001, in force 1.7.2004.
[8] On the distinction between genuine and non-genuine computer crimes see *Kaiafa-Gbandi* (2007), Arm, 1062.
[9] With respect to matters pertaining to fundamental rights, personal data, and procedural rights see, inter alia, *Breyer* (2001), Die Cyber-Crime-Konvention des Europarats, DuD, 600, *Dix* (2001), Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV, DuD, 588 ff., *Kugelmann* (2001), Die Cyber-Crime Konvention des Europarates, DuD, 222 ff., *id.* (2002), Völkerrechtliche Mindeststandards für die Strafverfolgung im Cyberspace-Die Cyber-crime Konvention des Europarates, TMR, 21 ff., *Valerius* (2004), Der Weg zu einem sicheren Internet?, K&R, 517-518; with respect to substantive criminal law see *Carr*, and *Williams* (2002), Draft Cyber-Crime Convention, Criminalization and the Council of Europe (Draft) Convention on Cyber-Crime, Computer Law & Security Report, 83 ff.
[10] See, e.g., *Csonka* (2000), The draft Council of Europe Convention on Cyber-Crime: A Response to the Challenge of Crime in the Age of the Internet?, Computer Law & Security Report, 329, *Gercke* (2004), Die Cybercrime-Konvention des Europarates, CR, 782 ff., esp. at 786, *id.* (2004), Analyse des Umsetzungsbedarfs der Cybercrime-Konvention, MMR, 728, *id.* (2006), The Slow Wake of A Global Approach Against Cybercrime – The potential of the Council of Europe Convention on Cybercrime as international model law, CRi, 144-145, *Kaspersen* (2001), Council of Europe's Cybercrime Convention, in ERA, Cybercrime: Developing the legal Framework in Europe-Documentation, London, 11-12.11.2010.
[11] See COM (2010) 517 final, 30.9.2010, 3.
[12] 2005/222/JHA, 24.2.2005, OJ L 69 of 16.3.2005, 68.
[13] See Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA in COM (2010) 517 final, of 30.9.2010; *cf*. the Presidency's proposal to the Council 8795/11, DROIPEN 27-TELECOM 43- CODEC 609, of 8.4.2011; also see *Brodowski* (2010), Strafrechtsrelevante Entwicklungen in der Europäischen Union-ein Überblick, ZIS, 753-754.
[14] *Cf*. *Sanchez-Hermosilla* (2003), Neues Strafrecht für den Kampf gegen Computerkriminalität- Konvention des Europarates und neuer Rahmenbeschluss der Europäischen Union im Vergleich mit dem deutschen Strafrecht, GR, 774 ff.
[15] On the competence of the E.U. in the field of substantive criminal law after the Lisbon Treaty see *Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 28-34.
[16] See pertinently *Bier* (2005), Kampf gegen die Cyberkriminalität, Der Rahmenbeschluss 2005/222/JI des Rates der EU über Angriffe auf Informationssysteme, DuD, 473 ff.
[17] It is noteworthy that the TFEU (article 83, par. 1) explicitly enumerates computer crime among types of crime with a cross-border dimension triggering the E.U.'s competence to establish minimum rules in the field of criminal law. In fact, the term 'computer crime' was deliberately chosen to cover a broder array of cases compared to 'cybercrime' as provided in the Council of Europe Convention: see *Gercke* (2010), CRi, 79.
[18] COM (2010) 517 final, 30.9.2010, 2.
[19] *Ibid*., at 3.
[20] The need for further measures to combat cybercrime has been highlighted by the Commission in the context of the Stockholm Program (and the pertinent action plan); moreover, the digital agenda drafted in the framework of the "Europe 2020" strategy features new forms of crime –and especially cybercrime- as its first item: see COM (2010) 517 final, 30.9.2010, 4. *Cf*. the opinion of Europol member *Dileone*, Cybercrime: Developing the legal framework in Europe, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010, and Commissioner *Jansky*, EU legislative and non-legislative instruments against cybercrime, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010.
[21] On 'botnets' and the dangers inherent in their use see COM (2010) 517 final, 30.9.2010, 3-4.
[22] See pertinently *European Criminal Policy Initiative* (ECPI) (2009), A Manifesto on European Criminal Policy, ZIS, 707 ff.; *cf*. *Mylonopoulos* (2011), European Criminal Law after the Lisbon Treaty: The legitimization of European Criminal Law and the importance of criminal law doctrine for its shaping, PChr, 86-87.

[23] See COM (2010) 517 final, 30.9.2010, 4.
[24] See the Explanatory Report by the Council of Europe, para. 49.
[25] See, along these lines, *Brodowski* (2010), ZIS, 753.
[26] On the application of this principle in European Criminal Law see *ECPI* (2010), at 707.
[27] *Cf*. the Explanatory Report by the Council of Europe, para. 45; also see *Carr*, and *Williams* (2002), Computer Law and Security Report, 84.
[28] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 7, 26.
[29] See pertinently the Explanatory Report by the Council of Europe, paras. 64, 69.
[30] For the importance of this principle on a European level see *Kaiafa-Gbandi* (2010), The importance of core principles of substantive criminal law for a European criminal policy respecting fundamental rights and the rule of law [in Greek], NoV, 2186 ff.
[31] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 7, 27.
[32] See *Kaiafa-Gbandi* (2010), NoV, 2196 ff.
[33] See the Explanatory Report by the Council of Europe, para. 53.
[34] *Ibid*., at 72-78.
[35] Even on a European level, criminalization needs to rely on a clear-cut affirmation of a fundamental interest which incurs serious damage by the act in question: see *ECPI* (2010), at 707.
[36] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 3, 6, 7, 17.
[37] *Ibid*., at 6.
[38] *Ibid*., at 18.
[39] See the Explanatory Report by the Council of Europe, paras. 38 and 47.
[40] See *Kaiafa-Gbandi* (2007), Arm, 1084.
[41] See COM (2010) 517 final, 30.9.2010, 16.
[42] See pertinently *ECPI* (2009), at 709.
[43] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 3-5, 7, at 17.
[44] *Ibid*., at 18-19.
[45] *Ibid*.
[46] *Ibid*., at 19.
[47] COM (2010) 517 final, 30.9.2010, 18.
[48] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 5, 7, 29.
[49] See *Kaiafa-Gbandi* (2010), NoV, 2187, at n. 29, *Mylonopoulos,* European criminal law and general principles of E.U. law (2010), PChr, 161.
[50] On this requirement as it emerges after the Lisbon Treaty see *Kaiafa-Gbandi* (2010), NoV, 2187-2190.
[51] See COM (2010) 517 final, 30.9.2010, 11 ff.
[52] See *ECPI* (2009), 707 ff., as well as *Kaiafa-Gbandi* (2010), NoV, 2190 ff.
[53] *Cf*. *Brodowski* (2010), ZIS, 753.
[54] See *ECPI* (2009), 707, *Kaiafa-Gbandi* (2010), NoV, 2183-2184, at n. 29, *Mylonopoulos*, (2010), PChr, 161.
[55] On the principle of coherence see *ECPI* (2009), at 709.
[56] *Ibid.*, at 707. On the criminalization of preparatory acts in connection with attacks against information systems see *Kaiafa-Gbandi* (2007), Arm, 1085, and, more extensively, *Chatziioannou*, The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data (under publication in Proceedings of the 4th International Conference on Information Law, Values and Freedoms in Modern Information Law and Ethics, 20th & 21st May 2011, Thessaloniki, Greece).
[57] See *Vassilakis*, Combating computer crime [in Greek] (1993), 80 ff., *Kaiafa-Gbandi* (2007), Arm, 1065, *Kioupes* (1999), Criminal law and the Internet [in Greek], 126-127, *Mylonopoulos*, Computers and criminal law [in Greek law] (1989), 92-93.
[58] See *Kaiafa-Gbandi*, *ibid*., at 1068, *Kioupes*, *ibid*., at 132, *Mylonopoulos*, *ibid*., at 83-84. In terms of case-law see indicatively S.Ct. 121/2003, PChr 2003, 910 ff., (comment by *Konstantinides*), also published in PoinDik 2003, 619 (comment by *Nouskales*), Athens Ct. App. 217/1997, Yper. 1997, 846 ff. (comment by *Kaiafa-Gbandi*).
[59] See extensively *Kaiafa-Gbandi* (2007), Arm, 1068 ff.
[60] Illegal system interference without yet obtaining access to data or software is punishable under articles 370quater, par. 2 and 370ter CC in the form of attempted data interception.
[61] See extensively *Kaiafa-Gbandi* (2007), Arm, 1084. On the European level see the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 10, including the proposed addition to the Preamble of the proposed directive (under 6a), according to which: "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".

[62] In the context of article 370[quater], par. 2 CC as it currently stands, it has been argued that the element of acting 'without a right' is indirectly derived from the prohibitions and security measures alluded to in the provision and that, in any event, it would suffice for the rightful owner to have expressed contrary will in any fashion: see *Mylonopoulos*, Computers and criminal law, 97 ff.; for a discussion of cases involving data transmitted via telecommunications systems, and especially via the Internet, see Kioupes, *op. cit*., at 126.

[63] Regarding this provision, see the criticism voiced by *Mylonopoulos, ibid*., at 81: the author questions the rationale of introducing an aggravated form of the offense in the absence of an intent to cause damage or derive benefit, which would curb the free flow of information.

[64] See *Kaiafa-Gbandi* (2007), Arm, 1077, 1084, noting that, although illegal system interference normally presupposes illegal data interference (in the form of intentional deletion, damaging, deterioration, etc.), it might occur independently, for instance in cases of blocking or shutting down a computer system through 'flooding' (see *Kioupes* (2000), Deterioration of computer data and illegal data interference [in Greek], Yper., 967, noting the possibility of applying article 292 CC in cases where the system affected is intended for public usage). Even when system interference is achieved through illegal data interference, however, it does bring additional harm to the system *itself*, thereby justifying distinct treatment.

[65] See *Kioupes* (2000), Yper., 966; also see *Kaiafa-Gbandi* (2007), Arm, 2007, 1076, 1084.

[66] On the defining attributes of a 'document' (fixed imprinting on a material body, attribution to a person, probative value) see *Mylonopoulos*, Computers and criminal law, 42 ff., *id.* (2005), Criminal Law – Special part: Crimes in relation to documents, 23 ff.

[67] On these offenses see *Kaiafa-Gbandi* (2007), Arm, 1075; on criminal damage to property *cf*. *Mylonopoulos* (2006), Crimes against property, 2nd ed., 348, speaking of criminal damage to property in the event of deletion or alteration of data by a virus, not just on account of the fact that such acts change the direction of the magnetic field in any given storage device, but also on account of the fact that they impair the use of the computer *itself*.

[68] See *Kaiafa-Gbandi* (2007), Arm, 1076, *Kioupes*, Criminal law and the Internet, 140-141, *id.* (2000), Yper., 965 ff.; *cf*. *Farantoures* (2003), Contemporary trends in Internet criminality: Defining and addressing hacking and virus attacks [in Greek], PoinDik, 194 ff.

[69] See the Explanatory Report by the Council of Europe, para. 51; also see *infra*.

[70] *Ibid*., at 55.

[71] See article 1 of the Cybercrime Convention and the Explanatory Report, at 57.

[72] *Lloyd* (2004), Information technology law, 4th ed., 264.

[73] See *Kaiafa-Gbandi* (2007), Arm, 1077-1078, noting that both computer systems and data have indeed been elevated to the status of fundamental interests worthy of protection. To the extent that such data is stored, are accessible and can be the object of ownership rights, criminal law ought to protect both their confidentiality (namely the owner's right to restrict access thereto), and their integrity and availability (namely the owner's right to retain them in any desired form and be able to use them at will). On information as a fundamental interest worthy of legal protection see *Vassilakis*, Combating computer crime, 62 ff.; also see *Nouskales* (2004), The criminal law protection of digital information [in Greek], in *ENOVE*, Digital Technology and the Law, 120 ff.

[74] According to article 2(a) of the proposal for a directive (COM (2010) 517 final, 30.9.2010, 15), 'information system' is defined as "any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance". On the other hand, article 2(b) of the proposed directive defines 'computer data' as "any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function".

[75] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 7, 18.

[76] *Ibid*., at 6. It should be noted that the Presidency's proposal retains the *possession* of tools used for committing cyber-attacks, although it mentions (*ibid*., at 3) that agreement was reached to exclude it in the 'Working Party on General Matters, including Evaluations'.

[77] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 4-5, 7, 18-19.

[78] See the Preamble to the E.U. Charter of Fundamental Rights.