The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data[1]

By Chatziioannou Konstantinos, LLM (Heidelberg), PhD candidate, Aristotle University of Thessaloniki, Faculty of Law, Department of Criminal Law and Criminology, Scholar of Program "Heracleitus II"

1.New threats in the field of information security

A number of programs, known as hacking tools, that could also be traced and downloaded via the internet, are used for the launching of attacks against information systems and electronic data. For example, we could mention programs that attack the confidentiality of computer systems, such as Trojan horses, but also programs, known as viruses and worms that threaten the integrity or availability of information systems and electronic data,

These programs could have enormous impact on the everyday life of individuals, provided they could attack the computer of every person, but also on the whole world, if these attacks are launched against the information systems of nuclear facilities. As a recent example the worm "Stuxnet" could be mentioned, which has attacked a large number of industrial information systems of nuclear facilities in Iran by damaging their physical integrity, an event that heralds a new era of cyberwar (Menn/Watkins, 2010). In this framework on an international level there is a tendency of independent criminalization of the possession, production and distribution of hacking tools as a measure of fending off attacks against the confidentiality, integrity and availability (hereinafter c.i.a.) of information systems and electronic data. This paper is devoted to ascertain to what extent this is reasonable from the perspective of the protected legal interests.

2. International treaties that criminalize acts related to hacking tools

According to Article 6 par. a) i) of the Convention on Cybercrime each contracting party is called to criminalize acts as the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5. In other words, the parties are also called to penalize preparatory acts of offences against the c.i.a. of computer data and systems. Let us define, however, that this article shall not be interpreted as imposing

1

This research has been co-financed by the European Union (European Social Fund – ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: Heracleitus II. Investing in knowledge society through the European Social Fund.

criminal liability where the above acts are not for the purpose of committing any of these offences, such as the authorized testing or protection of a computer system. In Art. 6 par. 3 it is also provided that each party may reserve the right not to criminilise these acts, provided that the reservation does not concern the sale, distribution or otherwise making available of data by which the whole or any part of a computer system is capable of being accessed.

During the drafting of the Convention articles it was debated whether the devices should be restricted to those that are designed exclusively or specifically for committing offences, but this perspective was considered to be too narrow, because it could lead to insurmountable difficulties in criminal proceedings, rendering the provision practically inapplicable (Explanatory Report of the Convention on Cybercrime, margin no 73). However, except for the submission of substantive to procedural criminal law, as it will be analyzed, this could cause many complications regarding the necessity of the general criminalization of hacking tools with a view to the protection of the c.i.a. of information systems and electronic data.

Is has been argued that the limitation of the Cybercrime Convention of criminalization by the requirement of an intent to commit specific crimes represents an adequate compromise (Sieber, 2004: 26). However, as this analysis will show, the criminalization of hacking tools could cause many problems.

On E.U. level, while framework decision 2005/222/JHA of the 24th of February 2005 on attacks against information systems did not criminalize the specific acts, the Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA that was submitted on 30 September 2010 by the Commission to the European Parliament and to the Council, prescribed in Art. 7 par. (a) the criminalization of 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, i.e. for committing offences against the c.i.a. of information systems and electronic data, without giving the opportunity to member states to express any kind of reservation. The lack of possibility not to apply the provision under certain circumstances that is given for example in Art. 6 par. 3 of the Convention on Cybercrime has caused some considerations, and on 10 June 2011 the Council reached a general approach on the compromise text of the proposal. Art. 7 of the above Proposal for a Directive prescribes now that: " 1. Member States shall take the necessary measures to ensure that the production, sale, procurement for use, import, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6, at least for cases which are not minor:

(a) a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.". According to the above compromise text of the proposal the criminalization of other devices that are not programs and the criminalization of the mere possession of hacking tools are avoided.

Consequently, the following arguments that refer to the Convention on Cybercrime regard the specific Proposal for a Directive as well, which, in case of its adoption, will oblige member states, including Greece, to transpose such a criminalization to national law, without any possibility of limitation of criminal liability except for cases that will be considered as minor.

The present paper will focus on the criminalization of the production, possession and distribution of devices designed or adapted primarily for the purpose of committing any the offences against the c.i.a. of information systems and electronic data.

3. Considerations regarding the criminalization of preparatory acts against the c.i.a. of information systems and electronic data

3.1.Problems that are related to the criminalization of all programs designed or adapted primarily for committing crimes against the c.i.a. of the information systems and electronic data

As it is widely accepted in the civil law jurisdiction a necessary prerequisite of criminalization is the protection of a legal interest (Kaiafa-Gbandi, 2000: 263 et seq. /Manoledakis, 1998/ Margaritis, 1981: 41 et seq. /Paraskevopoulos, 2008: 94 et seq. /Roxin, 2006: 8 et seq. /Simeonidou-Kastanidou, 2001, 25 et seq.). The protected legal interest of Art. 6 par. 1 a) i) of the Convention on Cybercrime could be considered the legal interests that could be endangered by the preparatory acts that are criminalized, i.e. the c.i.a. of information systems and electronic data that are endangered by acts that intend to commit illegal access, illegal interception, data interference and system interference.

It is argued that for the more effective combat of the dangers that are related to hacking tools (i.e. the creation of a black market for their production and distribution), the criminal law should prohibit specific potentially dangerous acts at their source, preceding the committing of offences against the c.i.a. of information systems and electronic data (Explanatory Report of the Convention on Cybercrime, margin no 71). So specifically, Art. 6 could be regarded as a provision that protects the c.i.a. of information systems and electronic data at an earlier stage before the actual infringement of them. The main issue is if it is reasonable to protect the specific legal interest in such an early stage.

In the Exlanatory Report of the Convention on Cybercrime it is mentioned that a similar approach has also been taken in the 1929 Geneva Convention on currency counterfeiting (Explanatory Report of the Convention on Cybercrime,margin no 71). However, it should be emphasized that Art. 3 par. 5 of the specific Convention provides that: "The following should be punishable as ordinary crimes: ….(5) The fraudulent making, receiving or obtaining of instruments or other articles peculiarly adapted for the counterfeiting or altering of currency". The main difference lies in the fact that these tools must be peculiarly adapted for the counterfeiting or altering of currency and we could accept a form of distant endangerment of a protected legal interest. For the hacking tools, however, that are designed or adapted primarily for committing crimes against the c.i.a. of information systems it is not easy to trace from their nature if they contain a risk asset for the protected legal interest (cf. Kaiafa-Gbandi, 2007: 1086).

Besides, referring to computer programs that are used to committing crimes against currency we can refer to Article 149 of the German Criminal Code that penalizes whosoever prepares to counterfeit money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another 1... computer programs or similar equipment which by their nature are suitable for the commission of the offence. The criminalization of acts that are related to computer programs was introduced by a law that – inter alia- transposed the Framework Decision on increasing protection by criminal penalties and other sanctions against counterfeiting

in connection with the introduction of the euro to national law (Law, 2002). Article 3 par. 1(d) of this document prescribes the obligation of criminalization of the fraudulent making, receiving, obtaining or possession of instruments, articles, computer programs and any other means peculiarly adapted for the counterfeiting or altering of currency. It must be emphasized that also article 4 of Framework Decision on combating fraud and counterfeiting of non cash means of payment prescribes the criminalization of acts related to computer programs and any other means peculiarly adapted for committing counterfeiting or falsification of a payment instrument in order for it to be used fraudulently.

While Article 149 of the German Criminal Code refers to programs which by their nature are suitable for committing the above crimes, in German theory it is widely accepted that the suitability of the programs must be of a specific nature and only programs that are exclusively suitable for counterfeiting are penalized (Erb, 2005: margin no. 3/ Ruß, 2009: margin no. 3). In the relative Explanatory Report it is mentioned that in the devices that are criminalized a special applicability for the execution of counterfeiting should be inhererent by their nature (Stree/Sternberg-Lieben, 2006: margin no 3). In that case the above programs are per ser dangerous for the protected legal interest of currency and no specific problems of delimitation of the programs that are used for criminal purposes are created.

Furthermore, the German Federal Constitutional Court came to a strict construction of the purpose of software for the commission of such an offence against the confidentiality of electronic data that is prescribed in Art. 202c of the German Criminal Code, the provision that incorporated to national law the criminalization provided by Art. 6 par. 3 of the Convention on Cybercrime. The above provision of the German Criminal Law criminalizes acts that are related to software for the purpose of the commission of an offence against the confidentiality of data (Art. 202a and 202b of the German Criminal Code) and thereby it could be said that it can be interpreted openly. Article 149 of the German Criminal Code was used by the German Federal Constitutional Court to demonstrate the equivalent interpretation that is formulated for the specific article that refers to devices that are suitable for the counterfeiting of money or stamps. More particularly, the court in the framework of a systematic interpretation mentioned specific provisions that refer expressly to the suitability of items for the committing of specific crimes (Articles 149 and 275 of the German Criminal Code). According to the Court Article 149 of the German Criminal Code in combination with its Explanatory Report is ordinarily interpreted so that in the measures of counterfeiting that are mentioned here is inhererent a specific applicability for the committing of counterfeiting and this means that the specific measures should be suitable exclusively for the committing of counterfeiting (…). As a matter of fact, the Court came to the conclusion that we should perceive the term of purpose in Article 202c of the German Criminal Code more narrowly than the suitability or even specific suitability (BVerfG, 2009: margin no 62).

The above Court ruled that the programs that are subjective to the above Article 202c of the Germ. Crim.Code should be developed or adapted for the committing of specific criminal acts and that this purpose should have been manifested objectively (Id.: margin no 60). The mere suitability of the software for the committing of electronic crimes is not sufficient and programs which could merely be misused are not subject to the provision (Id.: margin no 63) and we could not argue that the so called dual use hacking tools are included in Art. 202c of the German Criminal Code (Id. : margin no 64).

Therefore, we consider fairer the adoption of criminalization of the programs that are exclusively adapted to the committing of crimes against the c.i.a. of information systems and electronic data. We should however mention that the letter of Art. 6 of the Convention on Cybercrime and of Art.7 of the Proposal for a Directive on Attacks against Information Systems –contrary to the provisions of the above mentioned Framework Decisions related to the protection of currency and non cash means of payment- does not restrict the applying force of these provisions from widely interpreting the contents of the scope of this program. It entails programs that are designed or adapted primarily for the purpose of committing specific crimes and the applying services are in no manner restricted to covering the cases only that the exclusive scope of the program is the perpetration of a crime against the c.i.a. of information systems and electronic data. Furthermore, it is referred in the Explanatory Report of the Convention that the drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances (Explanatory Report of the Convention on Cybercrime, margin no 73). Consequently, the Explanatory Report of the Convention contrary to the provision which was mentioned by the above Constitutional Court could not easily support efforts to closely interpret the term of purpose of the programs and devices respectively. All the more, they could easily support an interpretation that would include the specific programs to the actus reus of the crime and so would also penalize programs that are used in the field of security of information systems and electronic data.

Moreover, we should emphasize that the need of delimitation of hacking tools in comparison with the rest of the programs is even greater relative to the programs that are used to counterfeit currency. Programs that are suitable for the counterfeiting of currency are not at all useful for its protection. The authenticity of currency could for example be checked via special mechanisms. Contrary to that, tools that are designed or adapted primarily for committing crimes against the c.i.a. of information systems and electronic data constitute per se an essential part of the control of their security.

It should be emphasized that programs primarily adapted or designed for the purpose of committing crimes against information systems and electronic data are often used in the field of information security and in this way contribute to the further protection of their c.i.a. and not their breach. More particularly, these tools are usually used for the monitoring of security gaps and the development of security strategies (Stuckenberg, 2010: 43 et seq.). Consequently, an attempt to criminalize even the simple possession of such tools could pose innocent people in danger, while the proof of the further intent of committing a criminal offence against the c.i.a. of information systems and electronic data is very difficult in a digital environment.

The delimitation of the tools which are designed or adapted primarily for the committing of the above crimes is difficult. Programs are multidimensional and it is not easy to prove when there is an intent to breach the cia of information systems and electronic data. More precisely, this intent is always determined by people themselves and this in any case should be determined by objective criteria (cf. Cornelius, 2007: 685). However, the limits that are posed by them are indiscernible, provided experts in the framework of realistic examinations use programs that are designed for launching real attacks, for the simulation of attacks (Furnell, 2010: 181). Programs that are used by hackers are also used by companies in order to examine the

passwords that are used by their employees (Borges, 2007: 8). Consequently, many hacking tools cannot be delimited from applications that are necessary for the security of information systems (Sommer, 2006: 68).

The internet also contributes to that development, by giving the opportunity to everyone and not only to information security experts to exchange those types of programs with the goal to deepen their knowledge in security issues. The criminalization of dual use programs would deter the technological development and the improvement of the c.i.a. of information systems and electronic data, provided users would avoid possessing such types of programs due to their fear of possible criminal prosecution. This would result in the lack of control of the security of their information systems and electronic data and to the reduction of their protection in practice. As it has been noted "the experimentation and joy to write a code a little more clever than the others and to infringe the others' countermeasures has always been part of the internet culture and many times hackers help us by torturing and perfecting our "immunity system" " (Papadimitriou, 2004: 30).

It should be noted that the ban of such tools would also create adversities to those who want to function legally and trace security gaps in information systems despite the reservation that is laid down in the Convention (Furnell, 2006: 290). Art. 6 par. 2 expressly provides that this article should not be interpreted as imposing criminal liability where the acts referred to in paragraph 1 are not for the purpose of committing an offence, such as for the authorized testing or protection of a computer system. However, this provision has a declarative character, and obviously in this case it would be difficult to determine exactly when these acts take place.

Regarding the allegation that criminalization is significantly restricted by requiring a further intent of committing a crime against the c.i.a. of information systems and data, it should be mentioned that generally in preparatory acts it is often difficult to determine the intent with clarity (Jescheck/Weigend, 1996: 523). Even more difficult is the attempt to delimitate the intent of committing a crime against the c.i.a. of information systems and electronic data in a digital environment.

3.2. Problems that are related to the expansion of the power of the enforcement agencies

By criminalizing the possession of a hacking tool without demanding the attempt of any offence against the c.i.a., law enforcement agencies are empowered to monitor all people that have a high level of technological expertise. Many times due to technical reasons it is difficult to prove a connection of an illegal access to an information system or electronic data and a particular program (Hilgendorf, 2009: margin no 5). This difficulty concerns all forms of attacks against the c.i.a. of information systems and electronic data because they take place mostly digitally. Generally, in the modern society, the concept of the "suspect' -to whom investigative measures could be imposed- has been enlarged and it is not always connected to the perpetration of a specific offence (Paraskevopoulos, 2009: 27 et seq.). In this framework the mere possession of hacking tools could refer to a large number of users of information systems. This fact could result in the making suspects of individuals due to their electronic profiles, i.e. due to the mere habit of downloading software that could be used for criminal purposes. In other words, via the penalization of the possession of such programs law enforcement agencies could monitor acts of possession without the necessity of proving and reasoning the connection of specific tools to specific attacks against the c.i.a. of information systems and electronic data.

The determination of the purpose for committing a crime against the c.i.a of information systems and electronic data results to the unavoidable intrusion to fundamental rights of the users of information systems and data. And this stems from the fact that the intent of such programs could be examined mainly via the analysis and search of his information systems or the user's traces in the internet. However, these searches may often prerequisite some serious infringement of the protected legal interest of the c.i.a. of the information systems and electronic data of the possessor of a hacking tool, but also the breach of his fundamental rights, such as the confidentiality of communication, informational self-determination and private life (regarding the personal data of the user), but also the protection of the domestic sanctuary (when the systems are located in a protected area). They may also infringe the specification of the general right of personality (Art. 2 par. 1 in combination with Art. 1 par. 1 of the German Constitution) that covers the constitutional right for the warranty of confidentiality and integrity of information systems, as it was recognized by the Federal Constitutional Court (BVerfG, 2008: margin no 166) and could be based upon the Greek Constitution (Art. 2 par. 1 in combination with Art. 5 for the right of the free development of personality, but also Art. 5A regarding the information Society). It would be necessary to examine the information system of the possessor in order to determine if he had an intent to commit a crime against the c.i.a. of information systems and electronic data. This kind of intent would rarely be expressed in accessible digital space, such as internet fora or elsewhere.

It must be emphasized that the intent of the mere possession could not easily be proven. The above mentioned Constitutional Court of Germany in order to clarify the controversial term of the purpose of the program stated that what is needed apart from the purposes of the programmer is an externally perceived manifestation of these scopes. This manifestation was related to the formulation of the program itself, by term of the use scope, which could be determined by the facts themselves (…,), or by the sales policy and the advertisement of the manufacturer that clearly aims at illegal uses of the product(…) and the determination of the details is left to the competent authorities. (BVerfG, 2009: margin no. 66). However, even if the above criteria could determine the purpose of people that produce or distribute hacking tools, they could not easily determine the purpose of the mere possessor that downloads a specific program.

Besides, the penalization of such acts is closely related to the possibility of search for means of evidence by the law enforcement agencies. In Nr. 8 of the Appendix to Recommendation No. R (95) 13 it is stated that criminal procedural law should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offences against the confidentiality, integrity and availability of telecommunication or computer systems (Council of Europe, 47). By already criminalizing the preparatory acts of offences against the c.i.a. of information systems and electronic data, we pave the way for the surveillance of the information systems of individuals and the investigative power of authorities is extended. On the other hand the protection of the legal interest of the c.i.a. of information systems and electronic data could be undermined, provided that the possible perpetrator of the possession of a hacking tool could be anyone.

3.3. Additional problems regarding the criminalization of the mere possession of hacking tools

It is however mentioned in the Explanatory Report of the Convention on Cybercrime that as the commission of these offences often requires the possession of the means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market for their production and distribution (Explanatory Report of the Convention on Cybercrime, margin no 71). Even if somebody accepted the existence of a black market, it is not at all certain that the consumer contributes to it, so that the penalization of the mere possession of the specific tools could be rationalized. Besides, the suppression of this phenomenon, for example in Greece, would marginally contribute to addressing the problem in third countries where these products could be produced. It is indeed sure that- given the international character of the electronic crime- there "safe havens"- countries could be set up where these acts are not criminalized, a possibility that is provided also for contracting states by the Convention in Art. 6 par. 3 referring to the formulation of reservation. For that reason, the fear that was developed in Germany during the transposition of the provision of the Convention that the criminalization of hacking tools endangers the financial existence of German information security companies and poses the tangible threat of these companies taking their operations abroad (contra Stuckenberg, 2010 : 41).

It should be mentioned that the simple possessor of hacking tools contributes minimally to the creation of the specific market and this participation could not rationalize the penalization of his own act for the total aggregate that demands numerous actions (cf. Neumann, 2011: 206). The contribution of each possessor to the creation of the specific black market of production and distribution of hacking tools cannot rationalize the punishability of the mere possession, because in that case we would impute a result (i.e. the demand through which the creation of a black market takes place) that occurs only by the collective demand for such tools. Besides, many times the so called "black market" could also contribute to the implementation of greater safety by users, provided that the user of the information system uses such programs to monitor the safety of his system. We trace again the problem of delimitation of the term "black market" provided that the programs are not used exclusively for committing crimes against the c.i.a. of information systems and electronic data.

4. Proposals regarding the criminalization of acts that are related to hacking tools.

Provided that an obligation of Greece as a member state of the E.U. has not been enacted- via the final version of the Directive on attacks against information systems- for the criminalization of acts related to hacking tools, it is proposed during the ratification of the Convention on Cybercrime that was signed by Greece on 11/23/2001, to reserve the right that is prescribed in Art. 6 par. 3 not to criminalize acts related to the mere possession of hacking tools. In any case, the final version of the Directive should not oblige member states to criminalize the mere possession of hacking tools.

De lege ferenda for the other acts that are related to hacking tools the best solution would be to criminalize only the production and distribution of hacking tools according to Art. 6 of the Convention on Cybercrime that should be limited to tools that are exclusively designed or adapted to committing a crime against the c.i.a. of the information systems or electronic data. In this way we could avoid the excessive expansion of punishability and would rationalize the criminalization of such preparatory acts that constitute a threat for the protected legal interest of the c.i.a. of the information systems and electronic data. A similar approach has already been taken for the delimitation of the term "weapon" in the Greek law (Kaiafa-Gbandi/Simeonidou-Kastanidou, 2008: 612 et seq.).

It should be noted that the programs are not so unrelated to the function of weapons as they may initially seem. There is also an opinion that information warfare has made it possible for states, as well as nonstate actors, to engage in armed conflict by way of bits and bytes instead of bullets and bombs (Brown, 2006: 190). According to this view, the computer systems used to generate malicious codes may be classified as weapons, but the other computer systems, telephone relay stations, satellites and other communications hardware that innocently and automatically transmit any signal they receive probably should not be classified as weapons (Id.: 185). Indeed, programs that are used in the attacks against the c.i.a. of the information systems and electronic data play an equivalent role to weapons, but in that case the direct target are the systems themselves and the electronic data and not humans. In this framework we propose the adoption of the above criterion of weapon classification according to their exclusive use, to the hacking tools as well. In this manner, programs that are not exclusively designed or adapted for launching attacks against the c.i.a. are not per se dangerous for the protected legal interest and should not be criminalized.

Regarding the tendency to penalize acts that are related to the sale, distribution or otherwise making available of computer passwords, access codes, or similar data by which the whole or any part of a computer is capable of being accessed (Art. 6 par. 1 a) ii) of the Convention on Cybercrime and Art. 7 par. 1 b) of the Proposal for a Directive on attacks against information systems), we could state that it does not cause the above problems that have to do with hacking tools. These data are per se dangerous for the c.i.a. of information systems and electronic data and there are not many difficulties referring to the intent of the acts that are related to them. The mere possession of such data could remain, according to Art. 6 par. 3 of the Convention on Cybercrime, not punishable, and this is the reason why the user of the information system or electronic data could not easily be involved in a criminal proceeding. It would be more prudent, however, to provide the contracting states with the possibility to criminalize the acts of production and distribution of such data only in the cases that are related to a number of items, as prescribed in Art. 6 par. 1) b) for their mere possession.

References

Brown, D., (2006), A Proposal for an international Convention to regulate the use of information systems in armed conflict, 47 Harv. Int'L.J., 179-221.

Borges, G. (2007), Advisory opinion on the Amendment on combating computer criminality [in German], 19.3.2007, 1-9.

BVerfG, 1 BvR 370/07 of 27.2.2008, margin no. (1 - 333), available at http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

BVerfG (2009): 2 BvR 2233/07 of 18.5.2009, margin no. 1-77, available at http://www.bverfg.de/entscheidungen/rk20090518_2bvr223307.html

Cornelius, K. (2007), Referring to the criminal liability for the offering of hacking tools [in German], CR 2007, 682-688.

Council of Europe, Committee of Ministers, European Committee in Crime Problems, Committee of Experts on Problem of Criminal Procedural Law connected with Information Technology (1995), Problems of criminal procedural law connected with information technology: recommendation No. R (95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995, and explanatory memorandum

Erb, V. (2005), in Münchener Kommentar zum Strafgesetzbuch, Verlag C.H. Beck München, § 149.

Furnell, S. (2006), Cybercrime, Destroying the Information Society [in Greek], Papazisi Publications, Athens.

Furnell, S. (2010), Hackers, viruses and malicious software, in Jewkes, Y./Yar, M. (ed.), Handbook of Internet Crime, Willan Publishing, 173- 193.

Hilgendorf, E. (2009), in Leipziger Kommentar, 12th Edition, De Gruyter Recht-Berlin, § 202c.

Jescheck, H.-H./Weigend, T. (1996), Textbook of Criminal Law [in German], 5th Edition, Duncker & Humblot, Berlin.

Kaiafa-Gbandi, M. (2000), A look at millennium from the perspective of a member of the Greek criminal law community [in German], in Eser A./Hassemer W./ Burkhardt B. (Ed.), German criminal law at the turn of the millennium: Review and outlook , München 2000, 261-282.

Kaiafa-Gbandi, M. (2007), Criminal Law and Information Technology abuses [in Greek], Armenopoulos 2007, 1058-1087.

Kaiafa-Gbandi, M./Simeonidou-Kastanidou,E. (2008), Jurisdictional applications of Special Criminal Laws [in Greek], Nomiki Bibliothiki..

Law (2002): Law for the Implementation of the Second Protocol of the 19th of June 1997 for the Convention on the protection of the European Communities' financial interests, the Joint Action on combating corruption on the private sector of the 22th of December 1998, and the Framework Decision of the 29th of May 2000 on increasing protection by criminal penalties and other sanctions against counterfeiting in connection with the introduction of the euro of 22.8.2002[in German], BGBl I 2002, 3387

Manoledakis, I. (1998), The function of the concept of "legal interest" [in Greek], Sakkoulas Publications, Athens-Thessaloniki.

Margaritis, L. (1981), The legal object as a basis for the solution of interpretative problems of Article 224 of the Greek Criminal Code [in Greek], Thessaloniki.

Menn J./ Watkins M. (2010), Warning over malicious computer worm, online at http://www.ft.com/cms/s/0/e9d3a662-c740-11df-aeb1-00144feab49a.html

Neumann, U. (2011), The criminal liability of the participant in the purchase, in Kaiafa-Gbandi, M./Prittwitz, C., Surveillance and criminal suppression (in Greek), Nomiki Bibliothiki, 199-210.

Paraskevopoulos, N. (2009), Targeting Majorities, New Orientations of Penal Control, in Serassis, T./Kania, H. /Albrecht, H.J. (eds.), Images of crime III, Representations of Crime and the Criminal, Duncker & Humblot Berlin, 27-43.

Paraskevopoulos, N. (2008), The foundations of Criminal law [in Greek], Sakkoulas Publications, Athens-Thessaloniki.

Papadimitriou, C. (2004), Life imprisonment to hackers? [in Greek], Kastaniotis.

Roxin, C. (2006), Criminal law, General Part, Volume I, The structure of the theory of crime [in German], 4rth edition, Verlag C.H. Beck.

Ruß, W. (2009) in Strafgesetzbuch Leipziger Kommentar, 12th Edition, De Gruyter Recht-Berlin, § 149.

Sieber, U. (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, General Report for Round Table II of the 17th International Congress of Penal Law, in Spinellis, D. Computer crimes, Cyber-terrorism, child pornography and financial crimes, 11-50.

Simeonidou-Kastanidou, E. (2001), Crimes against life [in Greek], 2nd edition, Sakkoulas Publication.

Sommer, P. (2006), Criminalising hacking tools, Digital investigation, 68-72.

Stree/Sternberg-Lieben (2006), in Schönke/Schröder, Strafgesetzbuch-Kommentar § 149.

Stuckenberg, C.-F. (2010), Too much fuzz for nothing ? (in German), wistra 2010, 41-46.