EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

IT SECURITY AND § 202c StGB

CRIMINAL LIABILITY FOR THE USE OF IT SECURITY TOOLS UNDER THE 41ST CRIMINAL LAW AMENDMENT ACT TO COMBAT COMPUTER CRIME

by Dennis Jlussi*
developed from a project work together with Christian Hawellek*.
*candi. iur. at the Gottfried Wilhelm Leibniz University of Hanover

Content

Dennis Jlussi: IT Security and § 202c StGB

Introduction

The introduction of Section 202c of the German Criminal Code (StGB) by the 41st Criminal Law Amendment Act to Combat Computer Crime[1] (41st StrÄndG) has been sharply criticized in the media and by affected experts; IT security measures would be criminalized and even according to general opinion benign users of hacker tools would be "at the mercy of the judge".[2] For companies and employees in the field of IT security, the question of whether their actions are punishable is existential. This is no less true for customers, however, because professional IT security checks and audits are important components of corporate information protection and, not least, of corporate risk management, which has also been a legal requirement for stock corporations at the latest since the introduction of Section 91 (2) of the German Stock Corporation Act (AktG) by KonTraG.[3]

The 41st StrÄndG was passed by the German Bundestag in June 2007. It was promulgated on August 10, 2007 and entered into force on the following day. The Act is based on international and European Union law: On the one hand, it serves to implement the Council of Europe's Convention on Cybercrime of 23.11.2001 ("Cybercrime Convention") and, on the other, to implement EU Framework Decision 2005/222/JI on attacks against information systems of 24.02.2005. Section 202c of the German Criminal Code, however, only implements the Cybercrime Convention and has no basis in the Framework Decision.

The Act amends and supplements the criminal law provisions on computer crime: in the case of spying on data (Section 202a of the Criminal Code), it is no longer a matter of success, i.e., it is now irrelevant whether the perpetrator actually obtains data; the possibility of accessing data is sufficient. The elements of the crime of interception of data (Section 202b StGB) has been newly created and that of computer sabotage (Section 303b StGB) has been expanded.

However, the introduction of Section 202c of the German Criminal Code (StGB) in particular has led to concern and criticism. This study is intended to clarify the legal dogmatic aspects of this provision and to use it to provide practical advice for the professional groups concerned, i.e., in particular IT security companies and their employees.

Activities that could fall under Section 202c of the Criminal Code include, in particular, the procurement, creation, adaptation and use of software, namely, on the one hand, vulnerability analysis software designed for IT security (e.g. AppScan, GFI Languard, Nessus). Such software attempts (among other things) to detect security vulnerabilities by passing certain potentially harmful values to the system to be tested and then evaluating reaction patterns ("signatures"). On the other hand, malware (viruses, Trojans, worm exploits, etc.) can also be used, which is procured and applied to test whether computer systems are vulnerable to certain attacks or whether the systems are sufficiently and effectively protected by current patches and -security software (e.g. virus scanners). Frequently, there is also an exchange of adapted exploits, etc., with friendly companies or as part of cross-company working groups[4] , so that the urgent question arises as to whether such measures should qualify as punishable in the future.

The question is, whether such measures will qualify as punishable in the future.

1 BGBl I No. 38/2007, p. 1786 ff.
2 Lischka, Law Criminalizes Programmers, Spiegel Online, http://www.spiegel.de/netzwelt/web/0,1518,492932,00.html.
3 Law on Control and Transparency in the Corporate Sector, Federal Law Gazette I No. 24/1998, pp. 786 ff.
4 E.g. in the CERT network, see http://www.cert-verbund.de

B. Origin of § 202c StGB

§ 202c - Acts preparatory to data espionage and phishing

(1) Whoever prepares the commission of an offence under section 202a or 202b by producing, acquiring for themselves or another, selling, supplying to another, disseminating or making available in another way

1. passwords or other security codes which provide access to data (section 202a (2)) or

2. computer programs for the purpose of the commission of such an offence

incurs a penalty of imprisonment for a term not exceeding two years or a fine.

(2) Section 149 (2) and (3) applies accordingly.

I. Emergence of the standard from the Cybercrime Convention

Section 202c of the German Criminal Code implements Article 6 of the Council of Europe's Convention on Cybercrime of November 23, 2001 ("Cybercrime Convention," also known as the "Budapest Convention"). The Cybercrime Convention was the world's first multilateral convention on computer crime.[5] Extensive explanations of the Convention can be found in the Council of Europe's Explanatory Report.[6] The signatory states undertake to introduce certain substantive criminal offences in the area of cybercrime to protect the confidentiality, integrity and availability of computer systems[7] and to introduce certain powers for criminal investigation procedures. Germany has adopted the cybercrime convention; the German government plans to ratify it soon after the pending implementation of the procedural powers of investigation.[8][9]

Article 6 - Misuse of devices

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i.) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii.) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b.) the possession of an item referred to in paragraphs (a)(i) or (a)(ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

5 Pocar, New Challenges for International Rules Against Cyber-Crime, European Journal on Criminal Policy and Research 2004, 27-37 [30].
6 Council of Europe Treaty Office, Explanatory Report on the Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
7 Explanatory Report (footnote 6), para. 71.
8 Draft Law on the Reorganization of Telecommunications Surveillance and Other Covert Investigation Measures and on the Implementation of Directive 2006/24/EC, BT-Drs. 16/5806.
9 BT-Drs. 16/5806, p. 2.

B. Origin of § 202c StGB

(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established inaccordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a)(ii) of this article.

1. Subject of regulation

Art. 6 of the Cybercrime Convention obligates the contracting states to independently punish preparatory acts in the area of Art. 2 - 5. Computer crimes typically require the use of certain software ("hacking tools"); prohibiting the use of such software under criminal law already covers the preliminary stage of the crime and therefore has a preventive effect. A similar approach, i.e., prohibiting the trade in corresponding crime-fighting tools in advance, was already taken at the international level in 1929 in the "Geneva Convention on Counterfeiting," with the penalization of the trade in printing presses and other counterfeiting material.[10]

Paragraph 1(a)(i) criminalizes the above-mentioned ways of using computer programs that are "primarily" intended for the commission of computer crimes. This includes, for example, programs, which are intended to modify or delete computer data without authorization or to disrupt the operating system, such as viruses or programs for gaining unauthorized access.[11] The conferees have discussed at length whether to cover only those programs that are exclusively and specifically designed to commit computer crimes.

Ultimately, however, such a definition of the offense was found to be too narrow, because it would make the provision virtually inapplicable in view of evidentiary difficulties.[12] Likewise, however, it was rejected that objective suitability alone should suffice and that subjective intent to commit computer crimes alone should be used as a filter for criminal liability.[13] The compromise solution is to cover computer programs that were created "primarily" for the purpose of committing computer crimes; this should "usually" exclude programs with "dual use".[14]

The conferees have seen the problem of the threat of overcriminalization in the area of IT security. Therefore, Art. 6 Cybercrime Convention only covers acts where there is not merely ordinary intent, but where there is specific and direct intent with regard to use in a computer crime.[15] Article 6(2) makes it clear that the scope of the Cybercrime Convention does not cover the aforementioned ways of handling computer programs if there is no such intent but the purpose of the handling is, for example, authorized testing or the protection of computer systems.

10 Spannbrucker, Convention on Cybercrime - A Comparison with German Computer Criminal Law in Substantive and Procedural Respect, diss. iur., Regensburg 2004, p. 79.
11 Explanatory Report (footnote 6), para. 72.
12 Explanatory Report (footnote 6), para. 73.
13 Same place. [14] At the same place.
15 Explanatory Report (footnote 6), para. 76.

2. Significance of Art. 6 Cybercrime Convention for the Interpretation of Section 202c StGB

The Cybercrime Convention is an intergovernmental agreement that obligates the Federal Republic of Germany under international law to introduce corresponding criminal provisions into national criminal law. The Convention does not have any direct effect on citizens; it requires implementation in German law. The Convention also does not prevent the German legislature from enacting stricter provisions than those provided for in the Convention.

Nevertheless, the legislator has expressed in the official explanatory memorandum that the introduction of Section 202c of the Criminal Code specifically serves to implement Article 6 of the Cybercrime Convention.[17] The legislator has given specific reasons for deviations and reservations in each case[18], so that it can be assumed that, insofar as no deviation is specifically justified, the legislator's intention is to implement the Cybercrime Convention exactly. In this respect, the Convention and the Explanatory Report can be used for the historical interpretation of Section 202c of the Criminal Code.

Nevertheless, the possibilities of interpretation in conformity with international law are limited, especially in the area of criminal law. Special requirements must be placed on the definiteness of the criminal law, which may not be relativized by interpretation in conformity with international law. Therefore, in contrast to European Community law, in the interpretation of international law transpositions, the conforming interpretation is a possible method, but not the interpretation method to be necessarily preferred for the sake of effective implementation.

II. Implementation in the German Criminal Law

The legislator has modeled Section 202c of the Criminal Code on existing criminal law provisions, all of which aim to punish certain preparatory acts in advance by making it a punishable offense to manufacture and procure essential means required for the offense. The legislature has already previously criminalized the production and procurement of means for counterfeiting money (Section 149 of the German Criminal Code), means for counterfeiting identity documents (Section 275 of the German Criminal Code), software for computer fraud (Section 263a (3) of the German Criminal Code) and software for speedometer manipulation (Section 22b (1) No. 3 of the German Road Traffic Act). The fact that Section 202c of the Criminal Code is intended to follow the same system can be seen above all from the fact that - just like Sections 263a, 275 of the Criminal Code and - Section 22b of the StVG - it refers to Section 149 (2) and (3) of the Criminal Code with regard to "withdrawal" from preparation.

However, there is practically no enlightening case law from the highest or higher courts on the model standards - apart from a decision by the BVerfG on § 22b StVG, see D.I. below.[19] The legislator was therefore unable to refer to established interpretative tendencies.

16 On the development of binding force under international law, Spannbrucker (supra note 10), p. 6.
17 BT-Drs. 16/3656, p. 11f.
18 Ibid.
19 On § 149 StGB: BGH wistra 2004, pp. 265-267; on Section 275 StGB: OLG Köln, NStZ 1994, p. 289; both decisions concern only the scope of application of the respective norm.

C. The elements of § 202c StGB

I. Legal Dogmatic Classification of § 202c StGB

1. Independent preparatory offense

In implementation of the Cybercrime Convention, Section 202c of the Criminal Code is an independent preparatory offense. Whereas an attempted criminal offense is only considered when the perpetrator has done everything that is essential from his point of view in order to make the crime occur, Section 202c of the Criminal Code establishes criminal liability even before the attempted stage if the perpetrator produces, procures, etc. the corresponding means with the intention of committing a computer crime.

2. Abstract endangerment offense

§ Section 202c is an abstract endangerment offense. With abstract endangerment offenses, the legislator intends to prohibit certain types of conduct that typically pose a significant risk of violating legal interests. It is irrefutably presumed by law that these behaviors are generally dangerous. A threat to legal interests is thus not a constituent element and not a prerequisite for criminal liability, but a legal policy reason for the criminal provision.[20] Criminal liability therefore exists precisely irrespective of a danger to a person or thing that actually exists in the individual case. The punishable behaviors are those that can particularly easily trigger a concrete danger and therefore already appear to the legislator to be worthy of punishment as such.

§ Section 202c of the Criminal Code is - in contrast to the other computer crimes of the 41st Amendment Act - not covered by the requirement to file a criminal complaint (Sections 205, 303c of the Criminal Code).

Section 202c of the Criminal Code is therefore an official offense and must be prosecuted ex officio.

II. The objective facts

1. Offence

As variants of the criminal act, the law mentions producing, procuring for oneself or another, selling, giving to another, distributing or otherwise making available. In this context, "distributing" means actively passing on, while "making accessible" means passively making available (especially for downloading).

"Procuring" includes any form of procurement, be it by download, by e-mail, on a physical data carrier or in any other way. It does not matter whether the software is provided for a consideration, so that free software is also covered; it also does not matter whether the software is available as an installation file or directly executable.

In its explanatory memorandum, the legislator does not go into further detail as to whether - as provided for in the Council of Europe Convention - this also covers importation and appears to presuppose this; however, it appears very doubtful whether, for example, the mere transfer of software that is already in one's direct possession can be subsumed under "procuring" within the territorial scope of the StGB. Whether the occurrence of the abstract risk situation within the territorial scope of the StGB constitutes a place of success within the meaning of Section 9 StGB is disputed. Since abstract endangerment offenses do not require a concrete danger or any consequence, they are often regarded as simple crimes of activity.[21]

20 Wessels / Beulke, Strafrecht AT, para. 29.
21 Tiedemann / Kindhäuser, NStZ 1988, pp. 337-346 [346]; Ostendorf, JuS 1982, p. 429; Jescheck / Weigend, Lehrbuch des Strafrechts, p. 178; Lackner/ Kühl, § 9 Rn 2; Sch/Sch-Eser, § 9 Rn. 6.

C. The elements of § 202c StGB

Only occasionally is the abstract danger seen as a constituent success in the sense of § 9 StGB;[22] this is not convincing, however, because an abstract danger is precisely not a "success belonging to the elements of the crime". Under it fall only such successes, which are constituent element, while however with abstract endangerment offences the "success" of the abstract endangerment is evenly only legal-political punishability reason. If, however, neither the place of the offense (place of procurement) lies within the scope of the StGB nor is there a place of success at all - and thus none within the scope of the StGB - the importation of means procured abroad is unpunishable under German law, at least insofar as the offense is not also punishable in the respective foreign state (Section 7 (2) StGB). Since an interpretation in - conformity with international law is not necessarily required - at the cost of adhering to the principles of criminal law dogma - and, moreover, importation can no longer be subsumed under "procuring" in terms of the wording alone, the legislator has failed to implement the provision in this respect.

2. Objects of crime

Passwords and other security codes (Section 202c (1) No. 1) as well as computer programs (No. 2) can be considered as objects of crime.

Passwords and other security codes include all identifiers that enable access to data. In addition to classic passwords, this also includes PINs, TANs, authentication certificates, and digitized biometric features (e.g., for the deception of a fingerprint sensor) regardless of how they are passed to the hardware to gain access (keyboard input, smart card, RFID, electrical signal passing, etc.).

What a computer program is, is not legally defined. According to the common definition, computer programs are sequences of commands that are executed on a computer in order to provide a certain functionality.[23] § Section 202c itself covers the preparation of offenses §§ 202a, 202b as a protective purpose; §§ 303a, 303b additionally refer to § 202c. Computer programs within the meaning of § 202c can therefore initially be all those that are suitable by their nature for committing these criminal offenses.

Beyond simple suitability, § 202c still requires that the purpose of the computer program, i.e. its intended use, is the commission of such crimes. This, too, leaves a gray area, however, because this is doubtful for instructions that merely call another program, which then causes the damage. Whether, for example, a batch file that contains "*format c:*" alone as an instruction, or an HTML file that merely embeds malware, are computer programs at all within themeaning of the provision, and if so, such programs whose purpose is the commission of the relevant computer crimes, seems questionable. Therefore, on the one hand, computer programs must be defined at all and distinguished from non-computer programs, and on the other hand, it must be determined when a purpose corresponding to the objective elements of the offense exists.

22 OLG Saarbrücken, NJW 1975, p. 506-509 [507]; Martin, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, 1989, p. 119.
23 Wikipedia: Computer program; very similarly Zimmermann (ed.), Das Lexikon der Datenverarbeitung.

C. The elements of § 202c StGB

a) Computer program

"Computer program" as a legal term has so far been discussed mainly with regard to the copyright protection of computer programs. There, the term is controversial: One view is based on DIN standards, according to which a computer program is a sequence of instructions which, after being recorded in a machine-readable medium, are capable of executing a specific function or task by means of an information-processing machine or of bringing about, indicating or achieving a specific result.[24] The prevailing opposing view requires a certain algorithmic flow logic and does not allow it to suffice if only predefined representations are generated on the ultimately executing computer (e.g. HTML).[25]

However, the arguments put forward in the copyright discussion are not entirely transferable. In copyright law, the decisive factor is above all that trivial sequences that do not make logical algorithmic distinctions, as well as code in pure markup languages, should not enjoy copyright protection because there is a need to keep them free for the general public. In contrast, criminal law has a different protective purpose; even programs that are not protectable by copyright may be suitable and intended for the commission of computer crimes. Therefore, the concept of a computer program within the meaning of Section 202c must be interpreted teleologically in light of the protective purpose of the criminal provision. - However, a certain sequential logic cannot be dispensed with for the fulfillment of the wording.

The purpose of protection therefore also covers scripts that perform (e.g., operating system) functions on the computers, which in themselves pursue neutral purposes, but are triggered or combined by the script with exclusively malicious intent. The batch script mentioned as an example, which formats the hard disk, would thus be covered.

By contrast, pure references to malware that must be interpreted independently by an application and merely influence a display are likely to exceed the wording "computer program". An HTML page that embeds malware is therefore not in itself a computer program, since it merely refers to malware.

In between are programs that are interpreted and executed with middleware, interpreters or virtual machines. Java programs, for example, are executed by the Java Virtual Machine. The "physical" execution of the commands on the computer is not carried out by the Java application, but by the virtual machine. Such programs, although they are only indirectly executed on the computer, are, however, according to the - general view of the market, computer programs and not merely references that only control a representation of an application.

Nevertheless, the distinction cannot be drawn clearly in every case. The distinction between code that merely influences the presentation of an application and code that triggers operating system functions, - even indirectly via middleware or similar, must be made on a case-by-case basis.

Computer programs, on the other hand, are not descriptions in general language, i.e., mere paraphrases of certain algorithms, without being implemented in a programming language.

24 Koch, GRUR 1997, 417 [420]; Cichon, ZUM 1998, 898
25 Gaster, MMR 1999, 734; Köhler, ZUM 1999, 548

C. The elements of § 202c StGB

The copyright license as such is also not a computer program, because a right to use a computer program does not in itself constitute a computer program; the mere acquisition of a license, without the software being procured in the form of the program code, is therefore not sufficient for criminal liability.

b) Objective purpose

Only computer programs whose purpose is the commission of an offense under Sections 202a, 202b, 303a, 303b of the Criminal Code are covered by the criminal provision. The objective purpose is to be taken into account.[26] According to the legislator's intention, only those programs are to be covered which *"have the illegal use immanent, i.e. which are designed for the commission of computer crimes according to the way they are constructed or their nature";*[27] whereby, according to the wording of the law, the provision for any computer crimes is not sufficient, but the objectified purpose - must refer to those computer crimes which are mentioned in Section 202c of the Criminal Code or refer to Section 202c of the Criminal Code.

This is intended to exclude computer programs that serve security screening purposes and also to exclude computer programs that are not clearly intended to be used for a criminal purpose and are only used either criminally or legally through their application *(dual use tools).*

Therefore, the objective facts do not include, on the one hand, programming and scripting languages that are only suitable for programming malware, as well as programs which are security software recognized by the public and which serve to detect, but not to exploit, security vulnerabilities.

In principle, however, any program, including malware, can be used for benign testing purposes, so that pure "single use tools" practically do not exist. The legislator therefore focuses on an "objectified" purpose. While a purpose is by nature subjective, the legislator wants to objectify this purpose. In doing so, the perception of the public will be decisive. Programs whose own functionality is merely "malicious" will fall under the offence, because even if they are used for benign testing purposes in individual cases, their objectified purpose worthy of punishment will remain the same. Malware, i.e. in particular viruses, worms and spyware, are therefore covered by the objective elements of the offense.

Here, too, there is a gray area in which a classification can only be made on a case-by-case basis. An exploit, for example, is in itself worthy of punishment according to its objectified purpose. However, it is very questionable whether this also applies to exploits that are created by IT security staff and test vulnerabilities that are known and should be closed; these can possibly also be intended for benign use according to objectified purpose.

With regard to the intended purpose, the way in which the vulnerability is exploited must also be taken into account. If, for example, the vulnerability consists of storing an unauthorized file on the hard disk, then it seems appropriate to consider the objectified determination.

The purpose of the exploit can also be measured by whether it deposits a file that can cause further damage or a harmless file, such as a plain text file with a security notice.

26 BT-Drs. 16/3656, p. 12.
27 BT-Drs. 16/3656, p. 19.

C. The elements of § 202c StGB

III. The subjective facs

1.General intent

The general intent consists of the knowledge of the objective elements of the crime and the intention to commit the crime. The perpetrator must therefore know that it is a computer program in the sense described and want to obtain it (etc.).

2.Preparation of a computer crime

In addition to the objectified purpose of the computer program, the preparation of a computer crime is the second essential "filter" with which the legislator intends to keep benign use free of punishment. In the wording *"Whoever prepares a criminal act [...]* by *[...]"*, "by" is not to be understood in such a way that the preparation of a criminal act already consists in the fact that the criminal acts are committed, but these are different elements of the offense.[28] The perpetrator must therefore commit the offense because he intends to prepare a contemplated offense (§§ 202a, 202b, 303a, 303b) with the offense. When preparation is to be assumed is questionable and has been left open by the legislator.

a) Excessive internal tendency

It is disputed whether the preparation of a crime must be objectively present or whether the element of the offense is based solely on the intention of the perpetrator (overriding internal tendency).

According one view, it is an objective element of the offense because it is formulated objectively.[29] According to the general opinion, however, it is an - overshooting internal tendency, since it depends only on the perpetrator's imagination.[30]

This is also convincing because the objective preparation of a criminal act is not important. In the preparatory stage covered by criminal liability here, preparation can in any case only be determined on the basis of the perpetrator's imagination. Preparation as an objective element of the offense would also lead to gaps in punishability, namely where (especially in the case of making available to unspecified third parties) no preparation has objectively occurred (because this does not lie solely in the act of committing the offense, see above), but this was subjectively intended: For lack of fulfillment of the objective elements of the crime and for lack of punishability by attempt, the perpetrator would then be exempt from punishment, although an abstract danger was created. The assumption that *the elements of the crime are* only subjective is also supported by the Cybercrime Convention, Article 6 of which speaks of intent, i.e. *"intent that the device is used for the purpose of committing [...] offences"*.[31]

b) Required form of intent

In the case of an overshooting internal tendency, dolus eventualis is sufficient in itself, insofar as the legislator does not make "intention" a literal requirement of the offense.[32] It would therefore be sufficient if the perpetrator seriously considers it possible and accepts the fact that his act serves the preparation of one of the of the above-mentioned computer crimes.

28 BT-Drs. 16/3656, p. 19.
29 NK -Puppe, § 149 marginal no. 3.
30 LK -Ruß, § 149 marginal no. 4.
31 Explanatory Report (footnote 6), para. 76.
32 LG München I, NJW 2003, pp. 2328-2331 [2329].

C. The elements of § 202c StGB

This goes beyond the requirement of the Cybercrime Convention, which requires intent in the technical sense, i.e. dolus directus of the first degree.[33] However, the Cybercrime Convention is only an instrument of minimum harmonization, so the German legislature is at liberty to insert stricter provisions. The legislature has refrained from using the technical concept of intent in the wording or the explanatory memorandum, and instead focuses on an intent and on the fact that there are no indications that the perpetrator is committing a computer crime of his own or of a third party.[34] If it is sufficient that the perpetrator sees indications of a computer crime, this suggests that dolus eventualis is sufficient with regard to the preparation of a computer crime.

c) Concretization of the prepared offense

It is then still questionable to what extent the contemplated computer offense must be concretized. This is disputed in the case of similar offenses: According to one view, the perpetrator must see a concrete act in front of his eyes, which has shape in its essential outlines; according to this view, a completely vague plan is not sufficient, but details of the commission of the act need not yet be finally determined.[35] According to the alternative view, it should be sufficient if the perpetrator acts in the knowledge that the objects of the crime could at some point serve a computer crime.[36]

The latter view, however, would allow the penal the area of deliberate negligence.

However, neither the wording nor the legislator intended to make it a punishable offense due to negligence.

It will therefore be necessary to require that the offender prepares a computer crime that he or a third party has already envisaged at the time of the offence. This is the case if at least some essential key points are known, such as the computer system to be attacked or the person of the victim or a definable target group (e.g., the users of a certain operating system or a certain application). In the case of making available (downloading), it is sufficient if the perpetrator expects and accepts at the time of the act that others will obtain the hacking tool in order to commit a crime. The perpetrator must therefore know or expect that his action will promote a planned offense,[37] without all concrete modalities of the offense having to be known.[38]

If it is not clear which computer crime is to be committed, and the crime is nevertheless intended (e.g. if the victim is already known and the object of the crime is capable of committing several crimes), it is possible to make an elective finding, i.e. a conviction leaving open the question of whether the perpetrator has prepared a crime under § 202a, § 202b, § 303a or § 303b.

The elements of computer criminal law - especially those newly introduced by the 41st Criminal Law Amendment Act - have caused a stir among IT security experts. Not entirely without reason, because at first glance the standards are unclear and even on closer inspection not all risks of criminal liability can be completely negated. Nevertheless, the Council of Europe and also the German legislator have made it quite clear that the regulations are not intended to criminalize the work of IT security, and the risks of criminal liability can be minimized with a few behaviors that should be taken with caution.

33 Explanatory Report, para. 76: "direct intent"; a. A. ohne besondere Begründung Spannbrucker, p. 81; on English terminology Burgess, For sight of Consequences is not the same as intent, http://www.peterjepson.com/law/burgess%20A2-1.htm.
34 BT-Drs. 16/3656, p. 19.
35 LK -Ruß, § 149 marginal no. 6; Sch/Sch-Stree / Sternberg-Lieben, § 149 marginal no. 5.
36 NK -Puppe, § 149 marginal no. 3.
37 Sch/Sch- Sternberg-Lieben, § 149 marginal no. 8.
38 Lackner/Kühl, § 263a marginal no. 26c.

D. Statement and possible solutions

The legislator has formulated Section 202c of the German Criminal Code (StGB) in a similar way to existing predicate offenses and has not been able to fall back on established case law: There is almost no supreme or higher court case law. At the same time, different opinions are expressed in the literature with regard to several crucial aspects, as explained in detail just now. In addition, there are terms ("computer program") that are not legally defined.

The legislator has apparently found itself unable - as the Council of Europe[39] has already done - to clearly exclude benign activities such as those in the area of IT security in the wording without allowing criminal liability loopholes to arise for malicious activities. The legislator relies on an appropriate, case-by-case - application of Section 202c of the German Criminal Code (StGB) by the public prosecutors and courts and expects those employed in the IT security sector personally as well as the companies (in conjunction with Sections 30, 130 OWiG) to take on the corresponding risks of criminal liability or administrative offenses and "take their chances".

Even if, in view of this, it is by no means completely beside the point to speak of a dependency "at the mercy of the judge"[40] , according to the view expressed here, if Section 202c of the German Criminal Code (StGB) is correctly applied and interpreted (especially teleologically and historically) by the public prosecutors' offices and courts, there should be no criminal liability in the context of IT security if a few requirements are met.

However, it cannot be completely ruled out that this - would be handled differently in practice in parts - and especially with regard to the controversial aspects - and that there could at least be investigative proceedings and measures, indictments and lower-instance convictions. Even if there were no conviction at the end of such proceedings, the commencement of proceedings and the implementation of investigative measures (e.g., searches, seizure or confiscation of computers) alone would have a significant impact on the ability to work in the area of IT security.

The following precautions can therefore be taken to minimize the risks outlined:

I. Possibility of invocation of the BVerfG

With regard to the similar (and similarly unclear) punishability of the manufacture and distribution of computer programs for the falsification of odometers (Section 22b I No. 3 StVG), a manufacturer has filed a constitutional complaint with the BVerfG. With its decision, the BVerfG has at least provided a little more legal certainty with regard to the limits of criminal liability.[41]

It would therefore be worth considering seeking at least partial clarification of the legal issues by the BVerfG, also with regard to Section 202c of the Criminal Code.

39 Explanatory Report (above footnote 6), para. 73.
40 Above fn. 2.
41 BVerfG NJW 2006, 2318.

II. Dealing with hacking tools and malware

To minimize the risk of criminal liability, it is also necessary to observe a number of guidelines when dealing with hacking tools:

1. Care

Special care must be taken when dealing with hacking tools and malware obtained or created for testing purposes. Such software should not be passed on to anyone who is not certain that they intend to use the software for benign testing purposes. It should only be passed on to known and reliable partners. Under no circumstances should such software be made available to an undefined group of recipients.

The affected computer programs should also be kept secure, both in terms of any installation media and in terms of securing the computers on which they are installed.

2. Documentation

When a hacking tool or malware is obtained - whether free or commercial - or created or created, there should be a clear record of the testing and security which testing and security purposes the program is procured and which use of the program is intended.

The documentation should show beyond doubt that the software was not procured to commit crimes, but to perform benign activities. The use of the program must also be documented accordingly - in writing and in a way that cannot be changed.

3. Consent

Since Section 202c of the Criminal Code is an abstract endangerment offense and there is therefore by its very nature no specific legal entity affected, consent is out of the question. However, consent is possible with regard to those criminal acts that the offence under Section 202c of the Criminal Code is intended to prepare, namely Sections 202a, 202b, 303a and 303b of the Criminal Code. If the authorized person whose computer systems or data are to be attacked for testing purposes consents to the measures, the prepared act is not punishable and, consequently, the preparation is not punishable either. If possible, consent should be given in writing and should be sufficiently specific as to the measures to which consent is given. Care must be taken to ensure that there is a closed chain of legitimation from the company management (board of management) to the person giving the consent. Employee participation rights must also be safeguarded, which may depend on the specific circumstances (e.g. permitted private use) and must therefore be examined on a case-by-case basis.