Filip Radoniewicz*

Network eavesdropping

Abstract

The subject of the article is the surveillance of ICT networks, commonly known as network eavesdropping or network wiretapping. First, the author presents the basic technical aspects of wiretapping. The main part of the article discusses international regulations (the Convention on Cybercrime), European Union regulations (Directive 2013/40 on attacks against information systems) and Polish regulations (Penal Code) concerning network eavesdropping. The last part of the article contains conclusions from the comparison of the provisions of the Cybercrime Convention, Directive 2013/40 and the Polish Penal Code.

Key words: surveillance of ICT networks, network eavesdropping, network wiretapping, cybercrime, Convention on Cybercrime, directive 2013/40

* Filip Radoniewicz, PhD, Department of Cyber Security Law and New Technologies of the Institute of Law of the War Studies Academy in Warsaw, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Introduction

The network eavesdropping is a colloquially term for the surveillance of information and communication networks. There are two types of surveillance: passive eavesdropping, where the perpetrator only reads the contents of intercepted information, and active eavesdropping, where the data is modified, for example by directing data transmission to another location in the network.

An example of passive eavesdropping is sniffing, which is the interception of packets (in other words, data divided into "portions" for the purpose of their transmission by the network).

An example of active eavesdropping is the 'man-in-the-middle' attack, which involves, putting things simply, "joining" ongoing data transmissions between two computers and acting as a relay of exchange of communication between them. The perpetrator directs queries sent between the victim's computer (Computer A) and the target computer (Computer B) to their own device, and only from there is data directed back to computer B. As a result, the communication between Computer A and Computer B runs through the computer owned by the perpetrator, who gains access to such data. Furthermore, the data can be modified. Even encrypted data transfers are vulnerable to this type of attack. The perpetrator gains access to an encrypted connection after redirecting messages from computer A to his or her own computer as a result of presenting to the victim a false security certificate or a public key (seemingly belonging to Computer B, which can be, for example, a server of the bank rendering services to the person using Computer A). The perpetrator then establishes a connection with Computer B, "posing as" computer A, and sending data received from Computer A to Computer B (and vice versa). This way, all the network traffic between Computer A and B (including the login and password to an online banking service) runs through the perpetrator's computer[1].

Another example of active eavesdropping is session hijacking. It involves an interruption to an authorised connection between two computers, and "intercepting" the session. This session continues, but the attacker takes the place of a trusted host (or server). It is achieved through "inserting" portions of

1 K. Krysiak, *Sieci komputerowe. Kompendium [Computer Networks. A Compendium]*, Gliwice 2015, pp. 495, 497–498; D. Lisiak, I. Politowska, M. Szmit, M. Tomaszewski, *13 najpopularniejszych ataków [13 Most Popular Attacks]*, Gliwice 2011, pp. 69–70; *Hack Proofing Your Network. Polish Edition*, red. R. Russell, Gliwice, p. 382.

transport protocol into the data stream exchanged in an authorised (properly established) connection between the victim of the attack and a trusted system. The attacker prepares a correct protocol portion and then inserts it as an authentic one, as if coming from the original source. To this end, the attacker must have previous access to the contents of the data stream (e.g. through sniffing)[2].

Perpetrators of computer crimes often use special software belonging to the group of so-called malware (short for malicious software); one of the most popular being Trojan horses, colloquially called Trojans. This type of software is at first sight harmless, but it has additional instructions in its code. The instructions initiate activities of which the user is not aware. Trojans are used by hackers to bypass system protection. After installing Trojans, perpetrators can obtain access to data. Moreover, Trojans can perform certain actions, such as deletion or modification of data, sending files to the perpetrator's computer, or intercepting data sent and received by the victim (including logins and passwords). Trojans are often disguised as harmless software or scripts installed on websites, which are then downloaded onto users' computers the moment they enter such a compromised website[3].

Other types of software, which may be classified as malware, include spyware, keyloggers, and also viruses and bugs, which are not used for surveillance, so as such will not be discussed further in this paper. Spyware collects data stored in a given user's computer (e.g. contact details, credit-card numbers, passwords, addresses of websites they visit). They can be placed inside the victim's system as a result of an unauthorised access to the system (break in) or by using a Trojan. Other installation methods include sending software by email as an attachment, which, once opened, installs itself in the system. It happens that some spyware is distributed together with utility programs (as in the case of AOL communicator)[4].

Keyloggers are software, which read and record the keystrokes made by users on their keyboards. This way valuable information is obtained, e.g. passwords. There are also hardware keyloggers, which are devices installed

2 For more information, see, for exam red. R. Russell, ple, *Hack Proofing…*, pp. 359–366.

3 See: *Hack Proofing…*, pp. 570–571; D.L. Shinder and E. Tittel, *Scene of the Cybercrime. Computer Forensics Handbook; Polish Version*. Gliwice 2004, p. 286. For more details, see A. Warhole, *Internet attac*k. Warsaw 1999, pp. 96–101.

4 Cf.: C. Easttom and J. Taylor, *Computer Crime, Investigation, and the Law*, Boston 2011, pp. 176–178.

between a keyboard and a computer. They usually have the form of small adapters plugged into the keyboard ports (currently it is mostly a USB port). Next, the keyboard cable is connected to the adapter. It is sometimes the case that a keylogger is placed in the cable or the keyboard itself. The device records all the characters written by the user from the moment of switching on the computer. The flaw of this method is the need to obtain physical access to the computer, which is not necessary in the case of software keyloggers. They record data from the moment of launching the system, and do not have the ability to record the password onto the system.

Convention on Cybercrime

The only international agreement, which addresses the issue of counteracting crime committed via the Internet and computer networks, is the Council of Europe Convention on Cybercrime of 23 November 2001[5] (further referred to as the Convention on Cybercrime or the Convention). It was the outcome of work carried out for over four years by not only representatives of most Member States of the Council of Europe (including Poland) but also, in the capacity of observers, delegates from the USA, Japan, and Canada, representatives of EU institutions, and independent experts. The objective of the Convention on Cybercrime was to create a legal framework for prosecuting computer crime with an international reach.

The Convention, similarly to the majority of actions of this type, established certain minimum standards[6] with regard to punishment for the offences listed in the convention. This means that the Parties may adopt more-restrictive solutions in relation to both the scope of criminal liability and the grounds for

5 Journal of Laws of 2015, item 728.

6 *Explanatory Report to the Convention on Cybercrime*, Point 33, https://rm.coe.int/CoERM-PublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [1.06.2021. Explanatory Report to the Convention on Cybercrime is a certain type of commentary to the Convention on Cybercrime (or a justification of the draft convention) prepared by the authors. It does not constitute an authoritative interpretation imposed by the authors of the Convention (which was asserted in Point II, in which it was also pointed out that it might "facilitate the application of the provisions contained therein"), further referred to as the Explanatory Report.

applying such liability, which is limited to intentional acts under the Convention on Cybercrime[7].

Article 3 of the Convention on Cybercrime relates to an offence entailing the intentionally committed interception without right, made by technical means, of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

As asserted by the authors of the Convention[8], the provision laid down in Article 3 of the Convention aims to protect the right to the privacy of data communication, provided for, i.a., in the European Convention on Human Rights[9] (as in the right to respect for a private life).

Pursuant to Article 3 of the Convention on Cybercrime, the Parties are obliged to establish as criminal offences any acts committed in breach of the confidentiality of information with the use of a computer system, in particular data transmission on a network, telephone conversations, and transmissions as part of the computer system itself (for example, from CPU to printer). However, the Parties may limit criminal liability to the interception of communication between computer systems within the network.

In line with the said provision, protection is provided to non-public transmissions of computer data, which are communications between individual entities or specified entity groups. In the Explanatory Report,

7 A. Adamski, *Przestępczość w cyberprzestrzeni Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy [Crime in Cyberspace. The legal measures for counteracting the Phenomenon in Poland in the Light of the Draft Convention of the Council of Europe]*, Toruń 2001, p. 17.

8 See: *Explanatory Report*, Point 51.

9 Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (Journal of Laws of 1993, no. 61, item 284, as amended, further referred to as "ECHR"). Pursuant to Article 8(1) ECHR "everyone has the right to respect for his private and family life, his home, and his correspondence." According to the case law of the European Court of Human Rights, the notion of correspondence refers to any form of direct communication between specified persons in writing, and any form of transmitting information with the use of technical means, including telephone conversations and the exchange of information via electronic means of communication (for example, email, or other Internet services). See ECtHR decision of 29 June 2006 in the case of Weber and Saravia vs Germany, Application no. 54934/00, Point 77; ECtHR Judgement of 3 April 2007 in the case of Copland vs the United Kingdom, Application no. 62617/00, Points 41 and 42; and Judgement of 1 July 2008 in the case of Liberty et al. vs the United Kingdom, Application no. 58243/00, Point 56. Cf.: *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, t. I, Komentarz do art. 1–18 [*Convention for the Protection of Human Rights and Fundamental Freedoms. vol. I. Commentary to Articles 1–18*], red. L. Garlicki, Warsaw 2010, pp. 542–543.

it was stressed that the term „non-public" does not describe the nature of the data transmitted but the wish of the parties to keep the communication confidential. The reasons for keeping the transmitted data unavailable to third parties might be of a strictly commercial nature. This is, for example, the case with rendering paid services, such as cable television. For such a category of transmission, it is irrelevant whether or not the communication was held via public (generally accessible) networks[10].

The obligation to criminalise interception stipulated in Article 3 of the Convention on Cybercrime was restricted to the instances in which such an interception was performed with the use of technical means. It is a comprehensive concept. Technical means include devices to intercept computer data (transmitted via telecommunication networks with the use of various means, including wireless mobile networks), and devices used for electromagnetic analysis, as well as software (e.g. sniffers), passwords and codes.

For perpetrators to be prosecuted, their actions must be undertaken "without right". Therefore, no criminal liability shall be attached to surveillance if the intercepting person has the right to do so; for example, if he or she acts when authorised by the participants in the transmission (including, e.g., system testing), or if surveillance is authorised by law in the interests of national security or the detection of offences by State authorities as part of their rights and obligations (defined in legal regulations with the status of an Act).

The provisions laid down in Article 3 impose an obligation to criminalise only the interception of content data, without addressing the issue of traffic data[11]. Article 3 refers to activities entailing the interception of communications (i.e. the contents)[12]. As follows from the definition in Article 1(d) of the Convention on Cybercrime, traffic data means computer data relating to communication. It is worth mentioning that the ECtHR maintained that the use of traffic data also constituted interference with the right of respect for private life,

10 *Explanatory Report*, Point 54. Cf.: A.M. Hubbard and S. Schjølberg, *Harmonizing national legal approaches on cybercrime*, http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf [1.06.2021], p. 12.

11 Traffic data, transmission data – data generated and processed in relation to transmitting data via networks. In Article 1(d) of the Convention on Cybercrime, traffic data is defined as any computer data relating to a communication by means of a computer system, generated by a computer system which forms part of a chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

12 Cf.: *Explanatory Report*, Point 53.

within the meaning of ECHR Article 8. In the Judgement in the Malone vs the United Kingdom case[13], the Court found that so-called metering (recording phone calls made from a given device by registering the dialled numbers with the date and duration of each connection), which is a standard procedure of telecommunications service suppliers, per se cannot be considered as interference in the right to privacy, but the disclosure of the data obtained this way without the consent of the subscriber concerned constitutes a violation of ECHR Article 8. In the view of the Court, this results from the fact that it is an integral element in communications made by telephone[14]. In addition, in the aforementioned judgement in the Copland case[15] the Court stressed that the data related to e-mail and Internet usage (i.e. traffic data) were subject to protection equivalent to that of telephone conversations.

As already mentioned, the Parties may limit the scope of criminal liability by introducing the requirement of a connection between the computer system under surveillance and another system, thus criminalising the interception of data within computer networks and exempting from criminal liability actions, which involve the surveillance of single computer systems with the use of technical means. Moreover, the Parties might decide that the condition for the criminal liability to apply is the occurrence of an intention on the part of the perpetrator in the form of "dishonest intent"[16].

Directive 2013/40/EU on attacks against information systems

The first attempt to regulate the issue of computer crime by EU legislative bodies was the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[17]. Under the Decision, Member States

13 ECHR Judgement of 2 August 1984, Application no. 8691/79.

14 For more details, see. A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 2.8.1984 r., 4/1983/60/94. Sprawa Malone przeciwko Zjednoczonemu Królestwu (cz. II) [Judgement of the European Court of Human Rights in Strasbourg of 02.08.1984, 4/1983/60/94. Malone vs the United Kingdom. Part II*] [in:] "Prokuratura i Prawo" 1997, issue 5, pp. 109–111.

15 ECHR Judgement in Copland vs the United Kingdom case, Points 43–44.

16 Such a construct can also be found in the Polish Penal Code, in Article 267(3), which defines an offence consisting of the perpetrator's actions undertaken to gain unauthorised access to information (See remarks below).

17 OJ EU L 69 of 16 March 2005, p. 67.

are only obliged to criminalise illegal access to information systems, and illegal interference in information systems and computer data, without addressing the interception of data. This was supplemented in Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA[18] (Further referred to as Directive 2013/40). In general, the provisions of Framework Decision 2005/222/JHA were retained and supplemented by a number of new solutions. Primarily, new types of offence were listed (e.g. the illegal interception of computer data, meaning eavesdropping and offences related to the use of hacking tools)[19].

In accordance with Article 6 of Directive 2013/40, illegal interception consists of intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right. For the purposes of the Directive, it was decided that an information system meant a device or group of inter-connected or related devices, one or more of which, emanating from a program, automatically processes computer data, as well as computer data stored, processed, retrieved[20] or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance[21] (Article 2(a)). Despite the similarity to the definition of a "computer system" in the Convention on Cybercrime, an information system is a more-comprehensive concept, as it means both a single device (e.g. a computer) and a group of interconnected devices, i.e. networks, both small (local) networks connecting several computers, and large-scale networks covering, for example, entire cities[22].

The discussed provision of Directive 2013/40 is almost an exact repetition of the contents of Article 3 of the Convention on Cybercrime. The authors of the Directive did not provide for a clause permitting Member States to make

18 OJ EU L 218 of 14 August 2013, p. 8.

19 For more details, see: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym [Penal liability for hacking and other offences against data and IT systems]*, Warsaw 2016, pp. 242–268.

20 Although the word "retrieve" used in the English version of the Directive means, i.a., "to recover", in this case the word has a different (IT-related) meaning – "to download".

21 In the English version of Directive 2013/40 the term "maintenance" was used, which should be understood and translated as "keeping in good condition" ("utrzymanie w dobrym stanie") or "technical maintenance" ("konserwacja").

22 F. Radoniewicz, *Odpowiedzialność karna…*, pp. 245–249, 275–277.

the punishment conditional on the dishonest intent of the perpetrator, or the requirement for the victim to be connected to another system in a network, similarly to the solutions adopted in the Convention on Cybercrime. Likewise, as in the case of the Convention on Cybercrime, Directive 2013/40 does not have any definition of "interception." The question might be posed as to whether this action involves the contents of communications only, or includes traffic data. Therefore, it should be assumed that when referring to the interception of data transmissions, the subject of the act is the content of the communication, similarly to the Convention on Cybercrime.

Polish Penal Code

As regards the Polish Penal Code[23], computer eavesdropping is an offence under Article 267(3). Under this provision, installing or using tapping, visual detection, or other devices or software to gain unauthorised access to information is an offence.

Although it is not expressly stated in Article 267(3), it should be stressed that this provision criminalises the interception of real-time computer-data transmission. It results from the "nature" of eavesdropping, which, in simple words, involves the interception of communications or information during their transmission with the use of various means, i.e. the human voice or computer data.

The legislator also cited alternative circumstances in Article 267(3), and criminal liability may be imposed for installing a device or software only (the perpetrator does not need to use them) or using a tool (or software) installed (placed in an IT system) by another person[24]. Whether any information was actually obtained this way is irrelevant. It is enough that the installed device or software facilitates the collection of information, even when the installation process is not complete[25].

23 Act of 6 June 1997 – the Penal Code (consolidated text Journal of Laws of 2020, item 1444, as amended.

24 It has a broader substantive scope than required by the Convention on Cybercrime, as it also imposes criminal liability on perpetrators who prepare for data interception by installing devices (or software) [Cf.: Adamski, 2005, pp. 55–56].

25 *Kodeks karny. Komentarz. Część szczególna, t. II, Komentarz do artykułów 117–277 k.k. [The Penal Code. The Specific Part, vol. III. Commentary to Articles 117–277]*, red. W. Wróbel, A. Zoll, Warsaw, p. 1506.

Such actions are not deemed illegal if they are lawfully performed by law enforcement (under the applicable legal regulations[26]).

Conclusions

The Polish regulations governing computer eavesdropping are compliant with the provisions of the Convention on Cybercrime, which stipulates the conditioning of criminal liability on the existence of "dishonest intent" on the part of the perpetrator (as regards the offence under Article 267(3) of the Penal Code, it is any action undertaken by the perpetrator in order to gain unauthorised access to information). However, this premise is not laid down in Article 6 of Directive 2013/40. It is necessary to either modify Article 267(3) of the Penal Code by removing the condition, or leave it in its existing (or similar) wording and add a provision (in compliance with Article 6 of Directive 2013/40), which would define the act without the circumstance in question. Consequently, the offence under the currently binding Article 267(3) of the Penal Code would constitute an aggravated form of interception.

Bibliography

Literature

Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, "Studia Prawnicze" 2005, Issue 4.

Adamski A., *Prawo karne komputerowe*, Warsaw 2000.

Adamski A., *Przestępczość w cyberprzestrzeni Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001.

Easttom C., Taylor J., *Computer Crime, Investigation, and the Law*, Boston 2011.

Hack Proofing Your Network. Polish Edition, red. R. Russell, Gliwice 2002.

Kodeks karny. Komentarz. Część szczególna, t. II, Komentarz do artykułów 117–277 k.k., red. W. Wróbel, A. Zoll , Warsaw 2013.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, t. I, Komentarz do art. 1–18, red. L. Garlicki, Warsaw 2010.

Krysiak K., *Sieci komputerowe. Kompendium*, Gliwice 2005.

Lisiak D., Politowska I., Szmit M., Tomaszewski M., *13 najpopularniejszych ataków*, Gliwice 2011.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warsaw 2016.

26 These mostly include the Act of 6 June 1997 – the Criminal Procedure Code (consolidated text; Journal of Laws of 2016, item 1749, as amended), the Police Act of 6 April 1990 (consolidated text, Journal of Laws of 2016, item 1782, as amended), and the Act on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text, Journal of Laws of 2016, item 1897, as amended).

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 2.8.1984 r., 4/1983/60/94. Sprawa Malone przeciwko Zjednoczonemu Królestwu (cz. II)*, "Prokuratura i Prawo" 1997, issue 5.
Shinder D.L. and Tittel E., *Scene of the Cybercrime. Computer Forensics Handbook*, Gliwice 2004.
Warhole A., *Internet attack*, Warsaw 1999.

Legal Acts

Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (Journal of Laws of 1993, no. 61, item 284 as amended).
Convention on Cybercrime of 23 November 2001 (Journal of Laws of 2015, item 728).
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA(OJ EU L 218 of 14 August 2013, p. 8).
Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (OJ EU L 69 of 16 March 2005, p. 67).
Act of 6 June 1997 – the Penal Code (consolidated text Journal of Laws of 2020, item 1444, as amended.

Podsłuch sieciowy

Streszczenie

Przedmiotem artykułu jest inwigilacja sieci teleinformatycznych, popularnie nazywana podsłuchem sieciowym. W pierwszej kolejności autor przedstawia podstawowe techniczne aspekty podsłuchu. W głównej części artykułu omawia regulacje międzynarodowe (Konwencja o cyberprzestępczości), regulacje Unii Europejskiej (Dyrektywa 2013/40/UE w sprawie ataków na systemy informatyczne) oraz regulacje polskie (kodeks karny) dotyczące podsłuchu sieciowego. Ostatnia część artykułu zawiera wnioski z porównania przepisów Konwencji o cyberprzestępczości, dyrektywy 2013/40 i polskiego kodeksu karnego.

Słowa kluczowe: inwigilacja sieciowa, podsłuch komputerowy, cyberprzestępczość, Konwencja o cyberprzestępczości, dyrektywa 2013/40