COMBATING ATTACKS AGAINST INFORMATION SYSTEMS: EU LEGISLATION AND ITS DEVELOPMENT

by

LIBOR KLIMEK*

Cybercrime and attacks against information systems have a considerable cross-border dimension. Approximation of laws in the EU improves the judicial cooperation in criminal matters in the EU. This paper deals with a special legislative instrument – a Council Framework Decision 2005/222/JHA on Attacks against Information Systems. The objective of this instrument is to improve cooperation among judicial and other competent authorities of the Member States of the EU through approximating rules on criminal law in the Member States in the area of attacks against information systems. The paper analyses its background, key features and presents current legislative development in the field of combating attacks against information systems.

KEYWORDS:
Cybercrime, Attacks against information systems, Council Framework Decision 2005/222/JHA on Attacks against Information Systems, Proposal for a Directive on Attacks against Information Systems.

1. INTRODUCTION

It is trite, but nonetheless true, to say that we live in a digital age. The proliferation of digital technology and the convergence of computing and communication devices has transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to

* Ph.D. student (Criminal Law), Faculty of Law, Pan European University, Bratislava, Slovak Republic; libor.klimek(at)yahoo.com

these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes.[1]

In these days, electronic communication networks and information systems are an essential part of the daily. Networks and information systems are converging and becoming increasingly interconnected. Intentional attacks against information systems can take a wide variety of forms including illegal access, spread of malicious code and denial of service attacks. It is possible to launch an attack from anywhere in the world to anywhere in the world at any time.

Cybercrime and, more specifically, attacks against information systems have a considerable cross-border dimension which is most obvious in large scale attacks as the connecting elements of an attack are often situated in different locations and in different countries. Moreover, attacks of this kind could often be transnational in nature and would require international police and judicial cooperation in the EU. Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems.

Criminal laws relating to computers and the Internet have developed differently in various countries. At the level of the EU a number of legislative instruments have been adopted providing for mechanisms for Member States of the EU in order to enhance combating against cybercrime. This paper deals with a special legislative instrument of this area – a Council Framework Decision 2005/222/JHA on Attacks against Information Systems.[2] First, it focuses on its background and further it deals with its key features. Moreover, the paper presents the legislative development in this field.

2. GENERAL BACKGROUND

There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to

[1] Clough, J. 2010, Principles of Cybercrime, Cambridge University Press, New York, p. 3.

[2] Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems. OJ, L 69/67 of 16.3.2005.

the achievement of a safer information society and therefore requires a response at the level of the EU. Significant gaps and differences in Member States' laws may hamper the fight against organised crime and may complicate effective police and judicial cooperation in the area of attacks against information systems. The transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature.[3]

As pointed out by the European Commission, some of the most serious incidents of attacks against information systems are directed against electronic communications network operators and service providers or against electronic commerce companies. More traditional areas can also be severely affected given the ever-increasing amount of interconnectivity in the modern communications environment as manufacturing industries, service industries, hospitals, other public sector organisations and governments, themselves. However, victims of attacks are not only organisations. There can be very direct, serious and damaging effects on individuals, as well. Attacks are often carried out by individuals acting on their own, sometimes by minors who perhaps do not fully appreciate the seriousness of their actions.[4]

At the Tampere European Council[5] in October 1999, the need to approximate provisions concerning offences and sentencing in the area of cybercrime was recognised. Further, the Action Plan on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice[6] and the Santa Maria da Feira European Council in June 2000 indicated and called for legislative action against high technology crime, including common definitions, incriminations and sanctions.

In addition to that, there was also a need to supplement existing instruments at the EU level. Some legislative acts contain references to computer-related crime which need to be defined more precisely, for example

---

3 Recitals 2 and 5 of the preamble of the Council Framework Decision 2005/222/JHA on Attacks against Information Systems.

4 Explanatory Memorandum to the Proposal for a Council Framework Decision on Attacks against Information Systems. COM(2002) 173 final, p. 3.

5 See 'Presidency Conclusions, Tampere European Council of 15-16 October 1999', in Vermeulen, G. 2005, Essential Texts on International and European Criminal Law, 4th edition, Antwerpen – Apeldoorn, Maklu, pp. 327-341.

6 OJ, C 19/1 of 23.1.1999.

the Council Framework Decision on the European Arrest Warrant[7], the Council Framework Decision on the Execution in the EU of Orders Freezing Property or Evidence[8] or the Council Framework Decision on the European Evidence Warrant[9].

3. CURRENT EU LEGISLATION: FRAMEWORK DECISION ON ATTACKS AGAINST INFORMATION SYSTEMS

Network and information security belongs to the core of the European Commission's policy regarding the information society. Tackling cybercrime is also an issue under the cooperation among Member States of the EU in the field of Justice and Home Affairs (or Police and Judicial Cooperation in Criminal Matters; in the past known as the third pillar of the EU). A step in the in EU's fight against cybercrime is the Council Framework Decision 2005/222/JHA on Attacks against Information Systems (hereinafter 'Framework Decision'). It is a legal framework intended to close the gaps and differences in Member State's laws in this area and to tackle forms of crime, such as hacking, spreading computer viruses and other malicious code, and organizing denial of service attacks on web sites.[10]

The objective of the Framework Decision is to improve cooperation among judicial and other competent authorities including the police and other specialised law enforcement services of the Member States through approximating rules on criminal law in the Member States in the area of attacks against information systems.[11] In other words, the Framework Decision has two main objectives:[12]

---

7 See Article 2(2) of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures among Member States. OJ, L 190/1 of 18.7.2002.

8 See Article 3(2) of the Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the EU of Orders Freezing Property or Evidence. OJ, L 195/45 of 2.8.2003.

9 See Article 14(2) of the Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters. OJ, C 115/13 of 9.5.2008.

10 Janczewski, L. J. & Colarik, A. M, 2008, Cyber Warfare and Cyber Terrorism, IGI Global, London, p. 433.

11 Recital 1 of the preamble of the Framework Decision.

12 Raghavan, S. V. & Dawson, E. 2011, An Investigation Into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection, Springer, New Delhi – Dordrecht – Heidelberg – London – New York, p. 78.

- creating a common set of legal definitions and criminal offences across the EU and
- improving the effective prosecution of offenders by setting out minimum rules with regards to penalties as well as rules with regards to the judicial cooperation among Member States.

The Framework Decision is intended to supplement and build upon other EU and international instruments, in particular the Convention on Cybercrime.[13] However, it is not intended to require Member States to criminalize breaches of rules on access to or disclosure of personal data, secrecy of communications, security of processing of personal data, electronic signatures or intellectual property violations and it does not prejudice the Directive 98/84/EC on the Legal Protection of Services Based on, or Consisting of, Conditional Access[14].

The Framework Decision provides for a common set of legal definitions across the EU. Common definitions, particularly of information systems and computer data, are important to ensure a consistent approach to its application in the Member States. For the purposes of the Framework Decision, the term 'information system' shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.[15] This term is deliberately used here in its broadest sense in recognition of the convergence among electronic communication networks and the various systems they connect. Information systems therefore include "stand-alone" personal computers, personal digital organisers, mobile telephones, intranets, extranets and, of course, the networks, servers and other infrastructure of the Internet. Furthermore, the term 'computer data' shall mean any representation of facts, information or concepts in a form suitable for processing in an information system, includ-

[13] The Council of Europe Convention on Cybercrime was signed in 2001 and entered into force on 1 July 2004. In spite of the fact it has been signed by all Member States of the EU, it has been ratified by only 15 Member States. However, the EU is not a signatory to the Convention. It is regarded as the most complete international standard to date since it provides a comprehensive and coherent framework embracing the various aspects relating to cybercrime.

[14] OJ, L 320/54 of 28.11.1998.

[15] Article 1(a) of the Framework Decision.

ing a program suitable for causing an information system to perform a function.[16]

The Framework Decision covers common definitions of the offences involved in attacks against information systems at the level of the EU, namely:

- illegal access to information systems,
- illegal system interference, and
- illegal data interference.

Firstly, in relation to illegal access to information systems, each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor. This conduct is incriminated only where the offence is committed by infringing a security measure.[17]

Secondly, in relation to illegal system interference, each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.[18]

Thirdly, in relation to illegal data interference, each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.[19]

On top of that, each Member State shall ensure that the instigation of aiding and abetting aforementioned offences is punishable as a criminal offence. All the criminal offences need to be committed with intent. The term "intentional" is used explicitly in the Framework Decision. This should be interpreted in accordance with the criminal law principles in Member States governing intent. Thus, the Framework Decision does not require criminalisation of actions where there is gross negligence or other recklessness, but no intent as such. An intent to unlawfully access or interfere with informa-

[16] Article 1(b) of the Framework Decision.

[17] Article 2 of the Framework Decision.

[18] Article 3 of the Framework Decision.

[19] Article 4 of the Framework Decision.

tion systems in general should also be sufficient, rather than it being necessary to prove that the intent was directed at a specific information system.[20]

In line with the approach taken in a number of legal instruments adopted at the EU level to combat different types of criminality, it is necessary also to cover the situation in which legal persons are involved in attacks against information systems. Thus, the Framework Decision also contains provisions on legal persons. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for illegal access to information systems, illegal system interference, and illegal data interference, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on a power of representation of the legal person, or an authority to take decisions on behalf of the legal person, or an authority to exercise control within the legal person. Moreover, apart from these cases, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by aforementioned person has made possible the commission of the concerned offences for the benefit of that legal person by a person under its authority. Liability of a legal person shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of these offences.[21]

As far as penalties for legal persons are concerned, each Member State shall take the necessary measures to ensure that a legal person held liable is punishable by penalties which shall include criminal or non-criminal fines and may include other penalties, such as exclusion from entitlement to public benefits or aid, temporary or permanent disqualification from the practice of commercial activities, placing under judicial supervision, or a judicial winding-up order.[22]

The international nature of offences involving attacks against information systems means that an effective legal response requires procedural provisions on jurisdiction which should be clear and far-reaching at the EU level to ensure that offenders cannot escape prosecution. Each Member

---

[20] Explanatory Memorandum to the Proposal for a Council Framework Decision on Attacks against Information Systems. COM(2002) 173 final, p. 10.

[21] Article 8 of the Framework Decision.

[22] Article 9(1) of the Framework Decision.

State shall establish its jurisdiction with regard to aforementioned offences where the offence has been committed:

- in whole or in part within its territory, or
- by one of its nationals, or
- for the benefit of a legal person that has its head office in the territory of that Member State.

Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the EU in order to facilitate cooperation among their judicial authorities and the coordination of their action.[23]

In spite of the fact the Framework Decision made a step in the fight against cybercrime, its implementation in the national legislation of the Member States is not satisfactory. On the one hand, significant progress had been made in most Member States and that the level of implementation was relatively good but, on the other hand, implementation in some Member States was not yet complete.

Firstly, Member States shall take the necessary measures to comply with the provisions of this Framework Decision by 16 March 2007.[24] However, by that date, only one State – Sweden – had transmitted a national text to the European Commission for purposes of consideration and even that was incomplete. The Commission therefore sent a reminder to the Member States asking them to send the text of all the national provisions transposing the Framework Decision and any information relating to the implementation of this measure considered appropriate.[25]

Secondly, the Framework Decision has been implemented in very different ways. Its implementation faces the wide diversity in the ways the Member States have implemented penal legislation and the resulting difficulty with fully assessing the national legislation without looking into how it is

---

[23] Article 10(4) of the Framework Decision.

[24] Article 12(1) of the Framework Decision.

[25] Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against Information Systems. COM(2008) 448 final, p. 2.

applied in practice.[26] For example, as far as the liability of legal persons is concerned, only 16 Member States have clearly taken the necessary measures to ensure that legal persons can be held liable for aforementioned offences.

4. EXPECTED FUTURE DEVELOPMENT: DIRECTIVE ON ATTACKS AGAINST INFORMATION SYSTEMS

Since the Framework Decision was adopted, successive criminal attacks against information systems have repeatedly underlined the need for closer European coordination in response to attacks of this type. The importance of taking further action to step up the fight against cybercrime was underlined in 2009 in the Stockholm Programme.[27] It was pointed out that new and modern challenges have emerged in the form of cybercrime as criminal groups have taken effectively advantage of technologies. This in turn makes investigations more complicated for law enforcement authorities. The EU should therefore promote policies and legislation that ensure a very high level of network security and allow faster reactions in the event of cyber-disruptions or cyberattacks.[28] Furthermore, the recently presented Digital Agenda for Europe[29], the first flagship initiative adopted under the Europe 2020 strategy, recognised the need to address the rise of new forms of crime, in particular cybercrime, at the European level.

In 2010 the European Commission presented a Proposal for a Directive on Attacks against Information Systems and Repealing the Framework Decision on Attacks against Information Systems[30] (hereinafter 'Proposal'), which is now being discussed. Similarly to the Framework Decision, the objective is to approximate rules on criminal law in the Member States in

---

[26] Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on Attacks against Information Systems. COM(2008) 448 final, p. 9.

[27] Stockholm Programme – Open and Secure Europe Serving and Protecting the Citizens. OJ, C 115/1 of 4.5.2010.

[28] Point 4.4.4 of the Stockholm Programme.

[29] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : A Digital Agenda for Europe, COM(2010) 245 final/2.

[30] Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA. COM(2010) 517 final, p. 3.

the area of attacks against information systems and improve cooperation among judicial and other competent authorities including the police and other specialised law enforcement services of the Member States.[31] Further, as far as its subject-matter is concerned, the Directive should define criminal offences in the area of attacks against information systems and establish minimum rules concerning penalties for such offences. It also aims to introduce common provisions to prevent such attacks and improve European criminal justice cooperation in this field.[32]

As shown, the purpose of the Proposal is to replace Framework Decision. The main novelty is that the Proposal takes into account the new methods of committing cybercrimes, especially the use of botnets. The term 'botnet' indicates a network of computers that have been infected by a malicious software (a computer virus). Such a network of compromised computers – 'zombies' – may be activated to perform specific actions, such as attacking information systems. These 'zombies' can be controlled by another computer, often without the knowledge of the users of the compromised computers. This 'controlling' computer is also known as the 'command-and-control centre'. The persons who control this centre are among the offenders as they use the compromised computers to launch attacks against information systems.

On the one hand, it is urgently needed to update the definition of offences involved in attacks against information systems and to increase EU criminal justice coordination and cooperation to deal effectively with this critical problem.[33] On the other hand, the Proposal contains in the definitions of criminal offences a provision allowing to criminalize only 'cases which are not minor' in the process of transposition of the Directive into national law. This element of flexibility is intended to allow Member States not to cover cases that would *in abstracto* be covered by the basic definition but are considered not to harm the protected legal interest, e.g. in particular acts by young people who attempt to prove their expertise in information technology. This possibility to limit the scope of criminalisation should not, however, lead to the introduction of additional constitutive elements of of-

---

31 Recital 1 of the preamble of the Proposal.

32 Article 1 of the Proposal.

33 Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA'. OJ, C 218/130 of 23.7.2011.

fences beyond those that are already included in the Proposal, because this would lead to the situation that only offences committed with the presence of aggravating circumstances are covered.

In addition to that, similarly to the Framework Decision, the Proposal contains common definitions for its purposes. Further, *inter alia*, it deals with penalties, liability of legal persons as well as penalties on legal persons and jurisdiction.

5. CONCLUSION

Attacks against information systems have a considerable cross-border dimension, which is most obvious in large-scale attacks as the connecting elements of an attack are often situated in different locations and in different countries. Attacks of this kind could often be trans-national in nature and would require police and judicial cooperation in the EU. Network and information security belongs to the core of the European Commission's policy regarding the information society. Tackling cybercrime is also an issue under the cooperation among Member States of the EU in the field of Justice and Home Affairs.

The step in the in EU's fight against cybercrime is the Council Framework Decision 2005/222/JHA on Attacks against Information Systems. The objective of the Framework Decision is to improve cooperation among judicial and other competent authorities including the police and other specialised law enforcement services of the Member States through approximating rules on criminal law in the Member States in the area of attacks against information systems.

The Framework Decision covers common definitions of the offences involved in attacks against information systems at the level of the EU, namely illegal access to information systems, illegal system interference and illegal data interference. On top of that, the instigation of aiding and abetting aforementioned offences is punishable as a criminal offence. The Framework Decision also contains provisions on legal persons in relation to criminal liability and penalties. However, liability of a legal person does not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of these offences.

In spite of the fact the Framework Decision made a step in the fight against cybercrime, its implementation in the national legislation of the Member States is not satisfactory. Significant progress had been made in

most Member States and the level of implementation was relatively good, but implementation in some Member States was not yet complete. Its implementation faces the wide diversity in the ways the Member States have implemented penal legislation and the resulting difficulty with fully assessing the national legislation without looking into how it is applied in practice. Since the Framework Decision was adopted, successive criminal attacks against information systems have repeatedly revealed the need for closer European coordination in response to attacks of this type. The importance of taking further action to step up the fight against cybercrime was underlined.

In 2010, the European Commission presented a Proposal for a Directive on Attacks against Information Systems and Repealing the Framework Decision on Attacks against Information Systems which is now being discussed. Similarly to the Framework Decision, its objective is to approximate rules on criminal law in the Member States in the area of attacks against information systems and improve cooperation among judicial and other competent authorities including the police and other specialised law enforcement services of the Member States. The main novelty is that the Proposal takes into account the new methods of committing cybercrimes, especially the use of botnets.

REFERENCES

[1] Clough, J. 2010, Principles of Cybercrime, Cambridge University Press, New York.

[2] Ivor, J. et al. 2010, Trestné právo hmotné – Osobitná časť, 2. vydanie [Substantive Criminal Law – Special Part, 2nd edition], Iura edition, Bratislava.

[3] Janczewski, L. J. & Colarik, A. M, 2008, Cyber Warfare and Cyber Terrorism, IGI Global, London.

[4] Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA'. OJ, C 218/130 of 23.7.2011.

[5] Proposal for a Council Framework Decision on attacks against information systems. COM(2002) 173 final.

[6] Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA. COM(2010) 517 final.

[7] Raghavan, S. V. & Dawson, E. 2011, An Investigation Into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection, Springer, New Delhi – Dordrecht – Heidelberg – London – New York.

[8] Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. COM(2008) 448 final.

[9] Záhora, J. 2005 'Počítačová kriminalita v európskom kontexte' [Cybercrime in European Context] in Justičná revue, Vol. 57, No. 2 (2005), pp. 207-218.

[10] Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems. OJ, L 69/67 of 16.3.2005.

[11] Stockholm Programme. OJ, C 115/1 of 4.5.2010.