

**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'**

COM(2010) 517 final — 2010/0273 (COD)

(2011/C 218/27)

Rapporteur general: **Mr MORGAN**

On 20 January 2011 the Council decided to consult the European Economic and Social Committee, under Article 114 of the Treaty on the Functioning of the European Union, 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*

COM(2010) 517 final — 2010/0273 (COD).

On 15 February 2011, the Bureau of the European Economic and Social Committee instructed the Section for Transport, Energy, Infrastructure and the Information Society to prepare the Committee's work on the subject.

Given the urgent nature of the work (Rule 59 of the Rules of Procedure), the European Economic and Social Committee appointed Mr Morgan as rapporteur-general at its 471st plenary session, held on 4 and 5 May 2011 (meeting of 4 May), and adopted the following opinion by 173 votes to 1 with 7 abstentions.

## 1. Conclusions and Recommendations

1.1 The Committee welcomes the Communication from the Commission on the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems. The Committee shares the deep concern of the Commission regarding the scale of cybercrime in Europe and the actual and potential damage being done to the economy and the welfare of citizens by this growing menace.

1.2 The Committee also shares the Commission's disappointment that only 17 of the 27 Member States have to-date ratified the Council of Europe Convention on Cybercrime ('Cybercrime Convention')<sup>(1)</sup>. The Committee calls on the remaining Member States<sup>(2)</sup> - Austria, Belgium, Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Sweden, and United Kingdom - to ratify the Cybercrime Convention as soon as possible.

1.3 The Committee agrees with the Commission that a Directive 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.

1.4 Because of the urgent need for legislative action to deal specifically with attacks against information systems, the Committee agrees with Commission's decision to use the policy option of a Directive supported by non-legislative measures, targeted at this particular aspect of cybercrime.

1.5 However, as the EESC has called for in a previous opinion<sup>(3)</sup>, the Committee would like the Commission to proceed in parallel with work on the drafting of comprehensive EU legislation against cybercrime. The Committee believes that a comprehensive framework is essential to the success of the Digital Agenda and the Europe 2020 Strategy<sup>(4)</sup>. The framework should deal with prevention, detection and education issues in addition to law enforcement and punishment.

1.6 In due course, the EESC would like to consider proposals from the Commission for a comprehensive framework of action to tackle the general issue of Internet security. Looking forward 10 years, with most of the population using the Internet, with most economic and social activity depending on the Internet, it is inconceivable that we will still be able to rely on the present casual and unstructured approach to Internet usage, especially since the economic value of this activity will be incalculable. There will be manifold issues, involving other challenges such as personal data security and privacy, as well as cybercrime. Airline safety is controlled by a central authority that establishes standards for aircraft, airports and airline operations. It is time to create an analogous authority, establishing standards for foolproof terminal devices (PCs, Pads, 'Phones), Network security, website security and data security. The physical configuration of the Internet is a key element in the defence against cyber crime. The EU is going to need a regulator with power over the Internet.

1.7 The Directive will focus on the definition of crime and the threat of penalties. The EESC asks for a parallel focus on prevention through better security measures. Equipment manufacturers should meet standards for the delivery of foolproof

<sup>(1)</sup> Council of Europe Convention on Cybercrime, Budapest 23.11.2001, CETS n° 185.

<sup>(2)</sup> See: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

<sup>(3)</sup> EESC opinion on *Secure Information Society*, OJ C 97, 28.4.2007, p. 21.

<sup>(4)</sup> COM(2010) 245, COM(2010) 2020.

devices. It is unacceptable that the security of devices and therefore of the network depends on the whim of its owner. The introduction of a Europe-wide electronic ID scheme should be considered, but this would need to be carefully conceived to avoid infringement of personal privacy; the full exploitation of the security capabilities in IPv6 should be set in train, and the teaching of personal cyber security to citizens, including data security, should be a fundamental part of all digital literacy curriculum. The Commission should refer to previous opinions from the Committee that has dealt with these issues <sup>(5)</sup>.

1.8 The Committee is satisfied that the proposed Directive adequately covers attacks against information systems using botnets <sup>(6)</sup>, including Denial-of-Service (DoS) attacks <sup>(7)</sup>. The Committee also believes that the Directive will help authorities prosecute cybercrime which attempts to exploit the international inter-connectivity of networks, as well as prosecute perpetrators who attempt to hide behind the anonymity which sophisticated cybercrime tools can provide.

1.9 The Committee is also pleased with the list of criminal offences covered by the Directive, especially the inclusion of 'Illegal interception' and the clear exposition of 'Tools used for committing offences'.

1.10 However, considering the importance of trust and security to the Digital Economy, and the enormous annual cost of cybercrime <sup>(8)</sup>, the Committee proposes that in the Directive the severity of penalties should reflect the seriousness of the crime and also act as a realistic deterrent to criminals. The proposed Directive stipulates minimum penalties of 2 or 5 years imprisonment (5 years for aggravating circumstances). The EESC envisages a scale of penalties related to the seriousness of the crime.

<sup>(5)</sup> EESC opinion on *Secure Information Society*, OJ C 97, 28.4.2007, p. 21; EESC opinion on *Advancing the Internet*, OJ C 175, 28.7.2009, p. 92; EESC opinion on *Critical Information Infrastructure Protection*, OJ C 255, 22.9.2010, p. 98; EESC opinion on *A Digital Agenda for Europe*, OJ C 54, 19.2.2011, p. 58; EESC opinion on 'New' ENISA Regulation, not yet published in OJ; EESC opinion on *Enhancing digital literacy, e-skills and e-inclusion*, not yet published in OJ.

<sup>(6)</sup> The term 'botnet' indicates a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. It is difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack may be in a different location from the offender himself.

<sup>(7)</sup> Denial-of-Service (DoS) attack – a denial of service attack is an act to make a computer resource (for example a website or Internet service) unavailable to its intended users. The contacted server or webpage will show itself as 'unavailable' to its users. The result of such an attack could, for example, render online payment systems non-operational, causing losses for its users.

<sup>(8)</sup> According to a 2009 study presented to the World Economic Forum, the global cost of cybercrime is \$1 trillion and growing rapidly. See paragraphs 2.5 and 2.7 below.

1.11 The EESC proposes that the opportunity should now be taken to send out a strong message to criminals and to citizens seeking reassurance, by stipulating more stringent penalties. For example, the UK <sup>(9)</sup> has penalties of up to 10 years for large-scale attacks on information systems, and Estonia has increased its penalties whereby terrorist use of large-scale attacks can be punishable up to 25 years imprisonment <sup>(10)</sup>.

1.12 The Committee welcomes the Commission's proposal to support the Directive with non-legislative measures to promote further coordinated action at EU level and more effective enforcement. The EESC would also stress the need to extend coordination to include close cooperation with all of the EFTA countries and NATO.

1.13 The Committee strongly supports the training programmes and best practice recommendations proposed to enhance the effectiveness of the existing 24/7 contact points for law enforcement authorities.

1.14 In addition to the non-legislative measures mentioned in the proposal, the Committee calls on the Commission to especially target R&D funds at the development of early detection and response systems to deal with attacks on information systems. The state-of-the-art in cloud computing <sup>(11)</sup> and grid computing <sup>(12)</sup> technologies have the potential to provide Europe with greater protection from many threats.

1.15 The Committee suggests that ENISA sponsor a targeted skills development programme to strengthen Europe's ICT security industry beyond law enforcement <sup>(13)</sup>.

1.16 To strengthen Europe's defences against cyber attacks, the Committee wants to reiterate the importance of developing the European Public Private Partnership for Resilience (EP3R) and integrate it with the work of the European Network and Information Security Agency (ENISA) and the European Governmental Group of CERTs (EGC).

<sup>(9)</sup> <http://www.legislation.gov.uk/ukpga/2006/48/contents>.

<sup>(10)</sup> SEC(2010) 1122 final - Commission Staff Working Document and Impact Assessment, accompanying document to the Proposal for a Directive on attacks against information systems.

<sup>(11)</sup> **Cloud computing** refers to the provision of computational resources on demand, or automatically, over the Internet. Cloud services are presented to users in a simple way that is easy to understand without the users needing to know how the services are provided. State-of-the-art end-user antivirus and Internet security software could be provided through a cloud platform to every connected user in Europe, reducing the need for users to protect themselves.

<sup>(12)</sup> **Grids** are a form of distributed computing whereby a 'super virtual computer' is composed of many networked loosely coupled computers acting together to perform very large tasks. Grid computing technologies might provide a platform for real-time cyber-attack analysis and response systems.

<sup>(13)</sup> EESC opinion on 'New' ENISA Regulation, (OJ C 107, 6.4.2011, p. 58.).

1.17 A strong information security industry should be fostered in Europe to match the competency of the very well financed industry in the US <sup>(14)</sup>. Investment in cyber security R&D and education should be increased significantly.

1.18 The Committee notes the exemptions under Treaty Protocols granted to the United Kingdom, Ireland and Denmark from enacting the proposed Directive. Notwithstanding the exemptions, the Committee calls on these Member States to cooperate to the greatest extent possible with the provisions of the Directive to prevent criminals from exploiting policy gaps across the Union.

## 2. Introduction

2.1 Europe today depends heavily on information systems for the creation of wealth and our quality of life. It is important that our growing dependence is matched by an increasing sophistication of security measures and strong laws to protect information systems from attack.

2.2 The Internet is the core platform of the digital society. Tackling threats to the security of information systems is critically important to the development of the digital society and the digital economy. The Internet supports most of Europe's Critical Information Infrastructure: underpinning information and communications platforms for the provision of essential goods and services. Attacks against information systems – government systems, financial systems, social services and critical infrastructure systems vital such as power supply, water, transport, health and emergency services – has become a major problem.

2.3 The architecture of the Internet is based on the inter-connection of millions of computers with processing, communications and control distributed globally. This distributed architecture is the key to making the Internet stable and resilient, with fast recovery of traffic flows whenever a problem arises. However, it also means that large-scale cyber attacks can be launched from the edge of the network, using botnets for example, by anyone with the intent and basic knowledge.

2.4 Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' <sup>(15)</sup> and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions. Given the difficulties of bringing a prosecution, organised crime is able to make considerable profits with little risk.

2.5 According to a 2009 study <sup>(16)</sup> presented to the World Economic Forum, the global cost of cybercrime is \$1 trillion and growing rapidly. And a recent government report <sup>(17)</sup> in the UK puts the annual cost in the United Kingdom alone at £27 billion. The high cost of cybercrime warrants tough action, strong enforcement and high penalties for offenders.

2.6 As detailed in the Commission's staff working document which accompanies the proposal for a Directive <sup>(18)</sup>, organised crime and hostile governments exploit the destructive potential of attacks on information systems across the Union. Attacks from such botnets can be very dangerous for the affected country as a whole, and can also be used by terrorists or others as a tool to put political pressure on a state.

2.7 The attack on Estonia in April-May 2007 highlighted the problem. That attack brought down important parts of the critical information infrastructure in government and the private sector for days due to large scale attacks against them – at a cost of EUR 19 million - EUR 28 million and significant political cost. Similar destructive attacks were also launched against Lithuania and Georgia.

2.8 Global communications networks involve a high degree of cross-border interconnectivity. It is vital that there is collective and uniform action by all 27 Member States to combat cybercrime, and specifically attacks against information systems. This international interdependency puts the onus on the EU to have an integrated policy for protecting information systems from attack and punishing perpetrators.

2.9 In its 2007 Opinion on 'A Strategy for a Secure Information Society' <sup>(19)</sup>, the Committee stated that it would like to see comprehensive EU legislation against cybercrime. In addition to attacks against information systems, a comprehensive framework should cover financial cybercrime, illegal Internet content, the collection/storage/transfer of electronic evidence, and more detailed jurisdiction rules.

2.10 The Committee recognises that formulating a comprehensive framework is a very difficult task, made even more difficult by the lack of political consensus <sup>(20)</sup> and by problems with significant differences between Member States on the admissibility of electronic evidence in courts. However, such a comprehensive framework would maximise the benefits

<sup>(14)</sup> The official figures from the Whitehouse show that the US government spent \$407m on cyber security research and development and education in 2010 and is proposing to spend \$548 million in FY 2012. <http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf>.

<sup>(15)</sup> 'Malware', short for *malicious software*, is software designed to secretly access a computer system without the owner's informed consent.

<sup>(16)</sup> 'Unsecured Economies: Protecting Vital Information', carried-out by researchers from Purdue University's Centre for Education and Research in Information Assurance and Security for McAfee (2009), [http://www.cerias.purdue.edu/assets/pdf/mfe\\_unsec\\_econ\\_pr\\_rpt\\_fnl\\_online\\_012109.pdf](http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf).

<sup>(17)</sup> <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>.

<sup>(18)</sup> SEC(2010)1122.

<sup>(19)</sup> EESC opinion on *Secure Information Society*, OJ C 97, 28.4.2007, p. 21 (TEN/254).

<sup>(20)</sup> SEC(2010) 1122, Impact Assessment of COM(2010) 517.

of both the legislative and non-legislative instruments to tackle the broad spectrum of cybercrime problems. It also would deal with the criminal law framework and at the same time improve law enforcement cooperation within the Union. The Committee would urge the Commission to continue working towards the goal of a comprehensive legal framework for cybercrime.

2.11 Fighting cybercrime requires special skills. The Committee's opinion on the proposed Regulation concerning ENISA <sup>(21)</sup> highlighted the importance of training of law enforcement personnel. The Committee is pleased that the Commission is progressing with the establishment of the cybercrime training platform involving law enforcement and the private sector, as proposed in COM(2007) 267 <sup>(22)</sup>.

2.12 Stakeholders in EU cyber security include every citizen whose life, might depend on vital services. The same citizens have a responsibility to protect their connection to the Internet from attack to the best of their ability. Even more responsible are the technology and services providers of the ICTs that deliver information systems.

2.13 It is critical that all stakeholders are appropriately informed about cyber security. It is also important for Europe to have a large number of skilled experts in the field of cyber security.

2.14 A strong information security industry should be fostered in Europe to match the competency of the very well financed industry in the US <sup>(23)</sup>. Investment in cyber security R&D and education should be increased significantly.

### 3. Gist of the draft Directive

3.1 The purpose of the proposal is to replace Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems <sup>(24)</sup>. The Framework Decision responded, as stated in its recitals, to the objective of improving cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, by approximating the rules of the criminal law in the Member States in relation to attacks against information systems. It introduced EU legislation to deal with offences such as illegal access to information systems, illegal system interference and illegal data interference, as well as specific rules on the liability of

legal persons, jurisdiction and exchange of information. Member States were required to take the necessary measures to comply with the provisions of the Framework Decision by 16 March 2007.

3.2 On 14 July 2008, the Commission published a report on the implementation of the Framework Decision <sup>(25)</sup>. In the conclusions it was stated that several 'emerging threats have been highlighted by recent attacks across Europe since adoption of the Framework Decision, in particular the emergence of large-scale simultaneous attacks against information systems and increased criminal use of so-called "botnets". These attacks were not the centre of attention when the Framework Decision was adopted.

3.3 This proposal takes into account the new methods of committing cybercrimes, especially the use of botnets <sup>(26)</sup>. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack may be in a different location from the offender himself.

3.4 Attacks carried out by a botnet are often executed on a large scale. Large-scale attacks are those attacks that can either be carried out with the use of tools affecting significant numbers of information systems (computers), or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc. The damage caused by large-scale attacks has a major impact on the functioning of the target itself, and/or affects its working environment. In this context, a 'big botnet' is understood to have the capacity to cause serious damage. It is difficult to define botnets in terms of size, but the biggest botnets witnessed have been estimated to have between 40 000 and 100 000 connections (i.e. infected computers) per period of 24 hours <sup>(27)</sup>.

3.5 The Framework Decision has a number of shortcomings due to the trend in the size and number of the offences (cyber attacks). It approximates legislation only on a limited number of offences, but does not fully address the potential threat posed to society by large scale attacks. Nor does it take sufficient account of the gravity of the crimes and sanctions against them.

3.6 The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States.

<sup>(21)</sup> EESC opinion on 'New' ENISA Regulation, OJ C 107, 6.4.2011, p. 58.

<sup>(22)</sup> COM(2007) 267 *Towards a general policy on the fight against cybercrime*.

<sup>(23)</sup> The official figures from the Whitehouse show that the US government spent \$407m on cyber security research and development and education in 2010 and is proposing to spend \$548 million in FY 2012.  
<http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf>.

<sup>(24)</sup> OJ L 69, 16.3.2005, p. 68.

<sup>(25)</sup> 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.

<sup>(26)</sup> See footnote 6 above.

<sup>(27)</sup> Number of connections per 24 hours is the commonly used measuring unit to estimate the size of botnets.



3.7 Attacks against information systems, in particular as a result of the threat from organised crime, are a growing menace, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.

3.8 There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types.

3.9 Common definitions in this area, particularly of information systems and computer data, are important in order to ensure a consistent approach in the Member States to the application of this Directive.

3.10 There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

3.11 Member States should provide for penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive.

3.12 The Directive, while repealing Framework Decision 2005/222/JHA, will retain its current provisions and include the following new elements:

- (a) It penalises the production, sale, procurement for use, import, distribution or otherwise making available of devices/tools used for committing the offences.
- (b) It includes aggravating circumstances:
  - the large-scale aspect of the attacks - botnets or similar tools would be addressed by introducing a new aggravating circumstance, in the sense that the act of putting in place a botnet or a similar tool would be an aggravating factor when crimes listed in the existing Framework Decision are committed;
  - when such attacks are committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.
- (c) It introduces 'illegal interception' as a criminal offence.
- (d) It introduces measures to improve European criminal justice cooperation by strengthening the existing structure of 24/7 contact points <sup>(28)</sup>.
- (e) It addresses the need to provide statistical data on cyber-crimes including the offences referred to in the existing Framework Decision and the newly added 'illegal interception'.
- (f) It contains in the definitions of criminal offences listed in articles 3, 4, 5 (illegal access to information systems, illegal systems interference and illegal interference) a provision allowing to criminalise only 'cases which are not minor' in the process of transposition of the directive into national law.

Brussels, 4 May 2011.

*The President*  
*of the European Economic and Social Committee*  
Staffan NILSSON

---

<sup>(28)</sup> Introduced by the Convention, and FD 2005/222/JHA on Attacks against Information Systems.