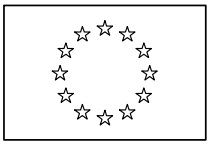

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 14.7.2008
COM(2008) 448 final

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

REPORT 1. INTRODUCTION

1.1. Background

The aim of this report is to assess whether the Member States have correctly implemented Council Framework Decision 2005/222/JHA on attacks against information system[1] (hereinafter "the FD") in their national law.

The main objective[2] of the FD, through an approximation of Member States' rules on criminal law in the area of attacks against information systems, is to improve cooperation between judicial and other competent authorities, including police and other Member States' specialised law enforcement services. Given this objective, the FD is intended to supplement and build upon other EU and international instruments (in particular the Council of Europe Convention on Cybercrime[3]).

Since the FD 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 massive denial of service attack against Estonia's information infrastructure in May 2007 served as a timely reminder of the disruptive and destructive effects of such attacks.

Consequently, the need for a complete and accurate implementation of the FD by every Member State has intensified since the FD was adopted. The timeliness of this report is further emphasised by explicit reference made to combating cybercrime in the conclusions of the recent meeting of the Justice and Home Affairs Council[4], which also said that it was looking forward to receiving the Commission report on the implementation.

1.2. Notifications and replies

Article 12(2) of the FD places an obligation on Member States to transmit, by 16 March 2007, the text of any provisions transposing the obligations imposed under the FD into their national law. By that date, only one State (Sweden) had transmitted a national text to the Commission and even that was incomplete. The Commission therefore sent a reminder to the Member States, asking them to send the Commission the text of all the national provisions transposing the Framework Decision and any information relating to the implementation of this measure considered appropriate.

By the 1 June 2008 the Commission had received notifications or replies to the reminder from 23 Member States. No replies have been received from *Malta*, *Poland*[5], *Slovakia* and *Spain*. In addition, the answers from *Ireland*, *Greece* and the

---

1 OJ L 69, 16.3.2005, p. 67.

2 Recital 1.

3 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

4 8 and 9 November 2007, see http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/en/jha/97023.pdf

5 While the Polish notification, submitted late on 1 July 2008, cannot be taken into consideration given strict publication deadlines, it will be considered latterly in actions following on from the publication of the report.

United Kingdom, as recognised by the respective governments, do not allow for any assessment of the implementation in these States, since the implementation has been delayed there.

The seven Member States mentioned have therefore not fulfilled their notification obligation under Article 12(2) of the FD. This report consequently gives an assessment of the law of only the other 20 Member States.

1.3. Method and evaluation criteria

This report is based on the information provided by the Member States. However, some of the data needed are missing. Consequently, the assessment and subsequent conclusions in this report are partly based on incomplete information.

Under Article 34(2)(b) of the Treaty on European Union, Framework Decisions shall be binding upon the Member States as to the result to be achieved, but shall leave to the national authorities the choice of form and methods. In order to evaluate objectively whether a Framework Decision has been fully implemented by a Member State, some general criteria have been developed with respect to Directives. These criteria can be applied *mutatis mutandis* to Framework Decisions. In particular, the rules implementing the FD must function effectively taking account of its aims, must satisfy the requirements of clarity and legal certainty, must assure full application of the text in a sufficiently clear and precise manner and must be implemented within the period prescribed.

This report focuses mainly on the formal level of implementation of the FD's criminal law provisions. However, actual *application* of those rules is beyond the scope of this report.

2. EVALUATION

2.1. General point on the implementation

The FD has been implemented in very different ways in the 20 Member States. In most States, the wording of the national law is close to that used in the FD. In others, a more indirect and general method of implementation has been applied. In many cases this means that the legal concepts and expressions used are not easily comparable. As far as possible, this report will take the general criminal law of the Member States into account and indicate any particular difficulties associated with this approach.

2.2. Definitions (Article 1)

The 20 Member States provided no clear or full information on how the definitions indicated in the FD have been applied in their national law. The general context, however, clearly shows that the definitions in their national law match the FD well.

2.3. Illegal access to information systems (Article 2)

The Commission considers that all the 20 Member States have incorporated the main obligation, i.e. to ensure that intentional access without right to the whole or any part of an information system is punishable as a criminal offence.

The final sentence of the first paragraph allows Member States the option to criminalise such conduct only 'for cases which are not minor'. The following Member States have, more or less explicitly, used this option on the basis that the models described below correspond to 'cases which are not minor':

– In *Austria*, the legal criterion for criminal responsibility is that intent to perpetrate data espionage and to use the data obtained in order to make a profit or to cause damage must be at hand;

– The *Czech Republic* has criminalised illegal access only in cases where the data are subsequently misused or damaged;

– In *Finland*, the requirement for criminal responsibility is that the data accessed must be 'endangered';

– In *Latvia*, illegal access is only criminalised only "if substantial injury is caused thereby".

A specific interpretation of 'cases which are not minor' is required in order to be able to assess whether these models are consistent with the FD. Such an interpretation is required to establish whether at least the core area of criminalisation intended by the FD is formally covered by the Member States. Article 2 aims at protecting the confidentiality of information systems. Accordingly, the Commission is of the opinion that the concept of 'minor case' must refer to cases where instances of illegal access are of minor importance or where an infringement of information system confidentiality is of a minor degree. However, the corresponding *Austrian*, *Czech*, *Finnish* and *Latvian* rules referred to above detail circumstances, e.g. where specific criminal intent or specific risks or damages have occurred, which cannot be considered as consistent with the aforementioned understanding. Thus the Commission has serious reservations that the *Austrian*, *Czech*, *Finnish* and *Latvian* provisions in question comply with the FD's conception of circumstances of 'cases which are not minor'.

More generally, such a divergence of interpretation and application of the option not to criminalise certain acts poses a serious risk to the objective to approximate Member State rules on criminal law in the area of attacks against information systems.

The Commission accordingly considers that only 16 of the 20 Member States have shown that they have properly implemented Article 2 of the FD.

Article 2(2) allows Member States to decide whether the conduct referred to in paragraph 1 is criminalised only where the offence is committed by infringing a security measure. This option has been applied in seven of the 20 Member States (*Austria, Finland, Germany, Hungary, Italy, Latvia and Lithuania*).

2.4. Illegal system interference (Article 3)

The Commission considers that all the 20 Member States cover the main obligation, i.e. 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.

However, further analysis of the practice in those Member States that have chosen relatively general provisions for implementation of this detailed Article of the FD may be needed to confirm this assessment. This is the case with *Denmark,* which claims that a very general legal provision regarding destruction of, damage to, or removal of all types of property covers all the criteria enumerated in this article. While such an approach is, in principle, acceptable, the extent to which such a provision is applicable to attacks on accessibility may be questioned, particularly in cases where the damage may be only temporary[6].

The last sentence of Article 3 allows Member States the option to criminalise such conduct only 'for cases which are not minor'. This option has been used by six Member States, which have, more or less explicitly, claimed that the following models cover such circumstances:

– *Austrian* law criminalises interference only in "severe" cases;

– *Czech* law requires intent to cause harm or loss[7];

– *German* law requires that the information system interfered with must be "of considerable importance for a third party";

– *Estonian* law makes criminal responsibility conditional on the criterion that "'significant damage is … caused";

– *Lithuanian* law criminalises only incidents "whereby … damage is caused";

– *Latvian* law criminalises interference only when "the protective systems are damaged or destroyed or large-scale loss is caused".

Again, closer definition of 'cases which are not minor' is required in order to be able to assess whether the above-mentioned models are consistent with the FD. This need has been previously discussed regarding Article 2 in section 2.3 above.

Article 3 aims at protecting the integrity of information systems. Accordingly, the Commission is of the opinion that the concept of 'minor case' must refer to cases where the system interference as such is of minor importance or where the integrity of the information system is only interfered with to a minor degree. The relevant *Austrian*, *Czech*, *Estonian* and *Lithuanian* rules referred to above seem to aim at

---

6 As underlined in the notification to the Commission from another Member States.

7 The Czech government has stated that this requirement will be dropped onadoption of the new criminal law.

exactly such circumstances and must be considered in line with the requirement that only minor cases of interference may be excluded from incrimination.

However, the relevant *German* rule refers to the importance for a third party and the *Latvian* rule to damages to protective systems or large-scale loss. The Commission considers these provisions' link to the integrity of information systems is insufficient in order to assess whether they are consistent with the FD option to exclude from incrimination 'cases which are not minor', and that this is inconsistent with the FD's objective to approximate Member State rules on criminal law in the area of attacks against information systems.

More generally, such a divergence of interpretation and application of the option not to incriminate certain acts poses a serious risk to the objective to approximate Member State rules on criminal law concerning attacks against information systems.

Accordingly, the Commission considers that only 18 of the 20 Member States have shown that they have properly implemented Article 3 of the FD..

2.5. Illegal data interference (article 4)

The Commission considers that all the 20 Member States cover the main obligation to ensure that the intentional deletion, damaging, deteriorating, alteration, suppression or rendering inaccessible computer data on an information system is punishable as a criminal offence. Many Member States have implemented both Articles 3 and 4 in a single national provision. Again, in the case of *Denmark*, the Commission is not convinced that a very generally held legal provision regarding destruction of, damage to, or removal of all types of property is assumed to cover the acts related to computer data enumerated in the article. For a brief discussion of this issue, refer back to the comments on Article 3 in section 2.4.

The final sentence of the article allows Member States the option to criminalise such conduct only 'for cases which are not minor'. This option has been used by three Member States, which have, more or less explicitly, claimed that the following models cover such circumstances:

– *Czech* law requires intent to cause harm or loss[8];

– *Estonian* law requires that "significant damage is … caused";

– *Latvian* law (Article 243 of the Criminal Law) applies the criterion that "the protective systems are damaged or destroyed or large-scale loss is caused".

As previously outlined in section 2.4 regarding the identical provisions implementing Article 3 of the FD, the Commission considers that the Czech law is, and the Estonian law must be presumed to be, consistent with the FD in this respect. As before, Latvia cannot be considered to have fulfilled its obligations under this point of the FD..

[8] The Czech government has stated that this requirement will be dropped with onadoption of the new criminal law.

The Commission considers that 19 of the 20 Member States have shown that they have properly implemented article 4 of the FD.

2.6. Instigation, aiding and abetting and attempt (article 5)

The Commission considers that the main obligation, i.e. to ensure that instigation of, aiding and abetting, as well as the attempt to commit, an offence is punishable is, in principle, met in 18 of the 20 Member States. *Finland* and *Portugal* have communicated national rules regarding attempt only and have therefore not demonstrated how the obligations regarding instigation, aiding and abetting are covered in their national law. *Sweden* does not provide for punishment in minor cases of instigation, aiding and abetting and attempt. This approach is not consistent with the requirements of the FD.

The Member States have the option of deciding not to apply the obligation to ensure that any attempt to commit the offence of illegal access to information systems is punishable. *Germany* and *Slovenia* have reported that they are making use of this possibility.

The Commission therefore considers that Article 5 has been properly implemented in 17 of the 20 Member States.

2.7. Penalties and aggravating circumstances (Articles 6-7)

The Commission considers that all 20 Member States have ensured that the offenses referred to in Articles 2 to 5 of the FD are punishable by reasonably effective, proportionate and dissuasive criminal penalties[9]. The penalties laid down for illegal system interference and illegal data interference also fulfil the specific requirements in Article 6(2) in the FD.

The situation regarding the obligation to take account of 'aggravating circumstances' for an offence committed within the framework of a criminal organisation (Article 7) is more varied.

- The provisions notified by *Austria* clearly do not fulfil this obligations under the FD;
- In *Danish* law makes no direct reference to criminal organisations;
- In *Finland*, no reference is made to criminal organisations in the relevant law;
- *Portugal* needs to make some adjustment to its law in order fully to comply with the FD.

Other Member States (*Bulgaria, Italy, Latvia and Sweden*) make no reference to the criterion 'criminal organisations' in the provisions notified to the Commission. However, the texts communicated however show that the obligation to apply more severe penalties for offences involving criminal organisations is already fully

[9] It should be noted that Austria seems to question whether its own penalties for illegal system interference are dissuasive enough.

covered – albeit indirectly – by national provisions in *Bulgaria, Italy* and *Latvia*. In these Member States the provisions in force for all cases of the offences in question lay down the more severe minimum penalties mentioned in Article 7 of the FD. The Swedish government claims that offences committed within the framework of criminal organisations are fully covered by the aggravating circumstance "serious crime" under Swedish law, and provided a detailed explanation in this regard.

Accordingly, the Commission considers that Article 6 has been properly implemented by all the 20 Member States and that 16 of them comply with the obligations under Article 7 of the FD.

2.8. Liability of legal persons and penalties for legal persons (Articles 8 and 9)

The Commission considers that 16 of the 20 Member States have clearly taken the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5 under the circumstances described in Article 8(1).

The *Czech Republic*[10]*, Latvia* and *Luxemburg*[11] have not fulfilled their obligation to notify the Commission of any such rules.

Estonia claims that its rules on civil liability cover all the cases described in Article 8(1), but has presented no details of these rules to the Commission. There is no obligation regarding the nature of the liability in question, and national rules on administrative or civil liability – when fully consistent with Article 8 – may in theory suffice. However, *Estonia* has not explained how its law on civil liability fully covers the obligations under the FD.

Article 8(2) places an obligation on the Member States to ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible commission of the offence for the benefit of that legal person by a person under its authority. The Commission considers that 10 of the 20 Member States have complied with this requirement. In addition to the *Czech Republic, Estonia*, *Latvia* and *Luxemburg*, where the conclusions drawn on Article 8(1) also apply to Article 8(2), *Denmark*, *Finland*, *France* and *Portugal* have presented no relevant rules on the liability of legal persons. *France* has stated that such liability follows from the rules on civil liability, but has provided no explanation of the exact content of this liability.

Under Article 9, Member States shall also take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) and Article 8(2) shall be punishable by effective, proportionate and dissuasive penalties. All the 14 Member States which presented measures correctly implementing Article 8(1) and the 10 Member States which have fulfilled their obligations pursuant to Article 8(2) have also fulfilled these obligations.

---

[10] The Czech government has stated that it has certain rules regarding civil liability in this context, but it has neither communicated the text of these rules nor described their content.

[11] A proposal for rules covering this obligation was presented to the Luxemburg Parliament in 2007, but the Commission is not aware that it has been adopted.

Accordingly, the Commission considers that only 12 of the 20 Member States have shown that they have fully implemented Articles 8 and 9 of the FD.

2.9. Jurisdiction (Article 10)

The Commission considers that 17 of the 20 Member States have fulfilled their obligation to establish their jurisdiction with regard to the offences referred to in Articles 2, 3, 4 and 5 of the FD (based on the specific criteria set out in Article 10). Although the different methods for legislating on jurisdiction issues across Member States make comparison more difficult, the Commission finds that the article has been implemented well. *Latvia* and *Portugal* have not fulfilled their obligation to inform the Commission of their national rules implementing Article 10.

The option provided for in paragraph 5, which gives Member States the possibility to decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c) has been used and notified by *France* (in the case of paragraph 1(b)) and *Austria, Finland*, *Germany*, *Hungary* and *Lithuania* (for paragraph 1(c)). *Italy* also seems to have made use of paragraphs 1(b) and 1(c) and *Estonia* and *Romania* of paragraph 1(c), although they have not formally acknowledged this. *Austria* has informed the Commission that it is still considering whether to continue to avail itself of this option.

Accordingly, the Commission considers that Article 10 has been properly implemented in 17 of the 20 Member States.

2.10. Exchange of information (Article 11)

Member States are under an obligation to ensure that they use the existing network of operational points of contact available 24 hours a day, seven days a week. The Commission has received no information which would enable it to assess whether this is the case regarding the FD in *Belgium*, *the Czech Republic*, *Germany*, *Italy, the Netherlands*, *Portugal* and *Slovenia*.

Regarding the obligation to inform the General Secretariat of the Council and the Commission of the appointed point of contact (Article 11(2)), the Commission has received no clear notification from *Austria*, *Bulgaria, Italy* and *Portugal.*

Accordingly, the Commission considers that only 11 of the 20 Member States have shown that they have fully met all the obligations set out in Article 11.

3. CONCLUSIONS

3.1. Level of implementation

This report provides a first insight into implementation of the FD by the Member States. It confirms 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.

The Commission notes that the FD is still being implemented in Member States. Significant progress has been made in practically all the 20 Member States assessed

in this report, where the level of implementation has been found to be relatively good.

Obviously the *major concern* for the Commission are the seven Member States that have yet to communicate any implementing measures. The Commission invites the Member States which have not yet implemented the FD in their national provisions to correct this situation as soon as possible. The Commission also invites Member States carefully to reconsider their legislation with a view to stepping up their efforts to counter attacks against information systems.

3.2. Future developments

Several emerging threats have been highlighted by recent attacks across Europe since adoption of the FD, in particular the emergence of massive simultaneous attacks against information systems and increased criminal use of so called botnets[12]. These attacks were not the centre of focus when the FD was adopted. In response to these developments, the Commission will consider actions aiming at finding better responses to the threat posed by botnets. These considerations may cover specific criminalisation of certain activities that facilitate criminal use of botnets plus tougher minimum penalties for offences committed in the form of massive and particularly dangerous attacks against information systems.

The Commission is also considering taking action to promote effective and timely use of the 24/7 contact points mentioned in Article 11. The need for rapid common actions – often including private operators – at international level to counter massive attacks against information systems was highlighted by serious incidents in 2007. In order to promote better coordination and consistency in such a response system, Member States should continue to consider whether the same contact points should be used as in the Council of Europe/G 8 networks[13]. The Commission will, in particular, consider establishment of EU guidelines on use of various international networks for high-tech crime issues.

---

[12] The term 'botnet' refers in brief to a collection of compromised machines running programs under a common command.

[13] Article 35 of the Convention.