time.lex

Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software

SMART 2008/ 0013

Disclaimer

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

time.lex CVBA

Advocaten – Avocats – Attorneys at law

Rue du Congrès 35, 1000 Brussels, Belgium

On behalf of the Management Board of time.lex CVBA:

Jos Dumortier and Geert Somers
Partners – Managing Directors

Executive summary

The current document is drafted in response to the European Commission's decision to award time.lex the procurement study "*Study on activities undertaken to address threats that undermine the confidence in the Information Society, such as spam, spyware and malicious software*" (SMART 2008/0013, hereinafter referred to as the ***Study***).

The original purpose of the Study was as follows:

- collect up-to-date information on the actions taken by competent national authorities against spam, spyware and malicious software;
- collect up-to-date information on the security measures taken by electronic communication network and service providers against spam, spyware and malicious software;
- collect up-to-date information on (actions taken by vendors against) the illegal spread of spyware and malicious software through software products delivered to end-users;
- provide information on the compliance of on-line distribution practices with European data protection legislation, notably the standard of information provided to end-users (Directives 2002/58 and 95/46/EC).

To carry out the Study, time.lex collected the above described up-to-date information from Member States' public authorities and industry, where possible and available. On the basis of the information provided the current document contains the main findings per Member State. For each Member State:

- on the one hand, measures undertaken by competent national authorities, by the service provider industry and by the vendor industry;

- on the other hand, cooperation activities between governmental bodies, between the government and the industry and in general at international level.

On the basis of this information, the European Commission wishes to assess the evolutions since its Communication (COM(2006) 688 final) of 15 November 2006 on this subject.

Jos Dumortier/Geert Somers
Brussels, 27 April 2009

Table of Contents

Section One: General introduction

1.1 Background

In its Communication (COM(2006) 688 final) of 15 November 2006 on Fighting spam, spyware and malicious software, the European Commission came to the following conclusions:

a) Member States didn't put in place the necessary internal cooperation procedures, bringing together the technical and investigative expertise of different government agencies and establishing close cooperation with network operators and ISPs;
b) substantial resources must be dedicated to gather evidence, pursue investigations and mount prosecution in this field;
c) all Member States must subscribe to international cooperation procedures to be able to immediately act on requests for cross-border assistance.

The European Commission proposes a series of actions to combat spam, illegal spyware and malware. The proposed actions target at

a) the Member States level;
b) the (software) industry level; and
c) the European level.

The actions to be taken at the level of governments and national authorities relate in particular to enforcement and cooperation. The Commission calls for greater involvement and prioritisation by the Member States, stating that the three main success factors of an effective policy in this area are

a) a strong commitment by central government to fight online malpractices;
b) clear organisational responsibility for enforcement activities; and
c) adequate resources for the enforcement authority.

In the view of the Commission, these three factors are not present in all Member States. Under the European Directives 95/46/EC and 2002/58/EC national authorities are requested to act against a number of illegal practices such as

a) unsolicited direct marketing communications (art. 13, Dir. 2002/58/EC);
b) unlawful access to terminal equipment (art. 5(3) Dir. 2002/58/EC);
c) phishing (art. 6 (a) Dir. 95/46/EC).

Under the Framework Decision 2005/222/JHA the Member States have to provide for criminal penalties for some of these practices. One of the tasks to be taken by Member States is to define clearly the responsibilities of different authorities and the necessary administrative processes for prevention, investigation and prosecution of these illegal activities. One of the main conclusions of the Commission's Communication of 2006 is that Member States didn't put in place the necessary internal cooperation procedures, bringing together the technical and investigative expertise of

different government agencies and establishing close cooperation with network operators and ISPs. The Commission further stresses the need to dedicate substantial resources to gather evidence, pursue investigations and mount prosecution in this field. It is, finally, also important that all Member States subscribe to international cooperation procedures and are able to immediately act on requests for cross-border assistance.

As far as the role of industry is concerned the Communication of 2006 mentions three kinds of possible actions that could be taken in this field: 1) adequate information to the users of software products about the processing of personal data via the installation of software or data on the user's device, 2) companies that have their products advertised online should contractually prohibit and monitor against the illegal use of software when these advertisements are served to consumers. Illegal use of software by advertising companies or their contract partners should lead to termination of the agreement. and 3) more emphasis should be placed by service providers on egress filtering.

The Commission announced in its Communication of 2006 that it would monitor the implementation of these actions and assess by 2008 whether additional action is needed. The Study should underpin this task of the Commission by providing information on the take up of the actions proposed in the Communication by 1) Member States, 2) (software) industry and 3) network operators and e-communications service providers.

1.2 **Content of this document**

The Study was drafted on the basis of answers obtained from national correspondents to a questionnaire containing the Commission's questions on the take up in and by Member States of actions proposed in the Commission's Communication of 2006.

In particular, this document contains up-to-date information

a) on the actions taken by competent national authorities against spam, spyware and malicious software
b) on the security measures taken by electronic communication network and service providers against spam, spyware and malicious software;
c) on (actions taken by vendors against) the illegal spread of spyware and malicious software through software products delivered to end-users;
d) on the compliance of on-line distribution practices with European data protection legislation, notably the standard of information provided to end-users (Directives 2002/58 and 95/46/EC).

For each of these four sections, the Study tries to identify tangible results (output) and good practices resulting from initiatives taken by Member States, industry and network operators or service providers.

1.3 **Purpose of the Study**

The outcome of this Study will be used by the European Commission in the context of monitoring progress made on the issues at stake and the analyses of the need for further policy initiatives relating to privacy and electronic communications.

1.4 **Terminology**

In this Study, the terms and acronyms below will have the following meaning:

APWG	Anti-phishing working group
CERT	Computer emergency response team, expert groups at national level that handle computer security incidents
CNSA	EU Contact network of spam authorities. The CNSA brings together the national authorities in the EU Member States that are competent for spam enforcement
DPA	The competent national data protection authority
Egress filtering	Filtering electronic communication that leaves a service provider's network
ENISA	European Network and Information Security Agency
ISP	Internet service provider
ISPA	Internet service provider association
LAP	London Action Plan
LEA	Law enforcement authority
MAAWG	Messaging Anti-Abuse Working Group
Malware (malicious software)	Software designed to infiltrate or damage a computer system without the owner's informed consent, e.g. worms and viruses as envisaged by article 5 of Directive 2002/58/EC
Phishing	Unsolicited communication to mislead users into giving away sensitive information
Spam	Unsolicited commercial communication as envisaged by article 13

	of Directive 2002/58/EC
Stopspamalliance.org	Umbrella group of worldwide anti-spam groups, public private partnership.
Spyware	Software installed on a computer without the user's knowledge in order to gain access to information, to store hidden information or to trace the activities of the user as envisaged by article 5 of Directive 2002/58/EC

1.5 **Reference documents at European level**

The legislative and other official documents adopted at European level are the most important reference documents for this Study.

Directive 95/46/EC of 24 October 1995	Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1]
Directive 2000/31/EC of 8 June 2000	Directive on certain legal aspects of information society services, in particular e-commerce, in the internal market. [2]
Directive 2002/58/EC of 12 July 2002	Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector. [3]
Communication (COM (2006) final) of 15 November 2006	Communication on Fighting spam, spyware and malicious software. [4]
Directive 2005/29/EC of 11 May 2005	Directive concerning unfair business-to-consumer commercial practices in the internal market. [5]
Regulation 2006/2004 EC of October 2004	Regulation on cooperation between national authorities responsible for the enforcement of consumer protection laws

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.
[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:EN:PDF.
[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF.

CNSA Cooperation procedure of 1 December 2004	Cooperation procedure concerning the transmission of complaint information and intelligence relevant to the enforcement of article 13 of the privacy and electronic communication directive 2002/58/EC, or any other applicable national law pertaining to the use of unsolicited electronic communications.[6]
Opinion 5/2004 of the article 29 WG	Opinion on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC.
LAP/CNSA spam referral, pro forma, December 2005	Cooperation procedure to standardize the exchange of information, requests for investigative assistance and the referral of cases between agencies responsible for enforcing the ban on spam.

1.6 **Reference documents at international level**

The legislative and other official documents adopted at European level are the most important reference documents for this Study.

Mobile spam code of practice[7]	A voluntary non-legally binding document of the GSM Association (GSMA) reflecting a commitment by operators and the GSMA to act against mobile spam and minimise the impact it has on customers.

[6] http://ec.europa.eu/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf
[7] http://gsmworld.com/documents/code_of_practice.pdf

Section Two: Main findings of the Study

1.1 General findings

1.1.1 Available information

It is clear that in recent years Member States have become more active in the fight against spam, spyware and online malware although the overall level of activity could still be improved[8]. More active Member States usually also make more information publicly available. As a result, some country profiles are much more detailed than others. In most Member States, it seems to be easier to obtain detailed information on action and measures taken by competent authorities than information about the industry, in particular the internet access providers and more even the vendor industry. Also, when spam is combined with organised crime, information relating to its prosecution will usually not be available to the general public.

1.1.2 Activity level of Member States

In the context of this study not all Member States have been able to demonstrate the same level of activity and commitment to combat online malware practices.

Member States with a low activity level – Some Member States could improve the level of attention that is paid to the fight against spam, spyware and malicious software. Currently this is clearly not a point of focus of the central government in such States, where the focus lays with other economic or political priorities. In some cases, the impact of spam is just lower due to language barriers[9].

Even where certain governmental departments are competent and dedicated to combat online malpractices, their actions could be considered insufficient due to a lack of budget and staff.

Member States with a high activity level – Member States with a strong commitment of the central government to fight online malpractices, often adopt legislative instruments and free budgets to increase the investigation and prosecution powers of their governmental departments.

Even in Member States where central government is investing considerable financial resources and efforts to improve the fight against online malpractices[10], the available budget though will usually not be sufficient to combat all kinds of such practices.

[8] Typical examples of active Member States are the Netherlands, Austria, Cyprus, France, Germany and Italy. Examples of less active Member States are the Czech Republic, Finland, Hungary, Lithuania and Slovakia.
[9] For example Finland and Hungary.
[10] For example Cyprus and the Netherlands.

Even in Member States with a reinforced police cybercrime department, priorities need to be given to serious offences, such as online child pornography and financial crime. Spam will get similar attention from the police when it comes in serious forms.

Although the situation has improved over the recent years, in general not enough deterring measures, in particular through imposing fines, have been undertaken at Member State level. Member States do seem to realise that the problem of online malpractices needs to be addressed at the international level. Therefore, many Member States participate in one or more international initiatives to address the problem of spam, spyware, malicious software and other online malpractices (see under 1.5.3).

1.2 Malware: applicable legislation and competent authorities

1.2.1 Malware and applicable legislation

Relevant provisions on information security or spam are encompassed in several laws and decrees.

Data protection and e-commerce legislation – Pursuant to applicable European legislation, all Member States have provisions in place relating to the prohibition of unsolicited commercial communication, as such implementing applicable European data protection and e-commerce legislation, in particular Directive 2002/58 EC and Directive 2000/31/EC.

Cybercrime legislation – Also, many Member States indicate the existence of specific cybercrime provisions, generally resulting from ratification of the Cybercrime Convention of 2001. Some criminal provisions explicitly refer to the dissemination of spyware and malware.

1.2.2 Malware and competent authorities

In most Member States, effective competences for the fight against spam and online malware are with the national telecom regulator and/or the national data protection authority (DPA), who usually both have investigation powers.

The national DPA – The DPA often has the power to request and demand information that its deems relevant for its investigation and to impose fines when a company or individual fails to supply requested information. Typically, the role and powers of the national DPA are limited to spam and spyware, in particular enforcing the legal provisions relating thereto. The powers of the DPA may be less or more ambitious, e.g. where the DPA has the specific competence to impose financial sanctions, carry out on-site inspections or issue public warnings. Usually however, the DPA takes up a less active role, e.g. when it comes to investigating or imposing fines. Sometimes, it can also order controllers to cease the sending of spam and if necessary impose a financial penalty or an injunction to stop the sending of spam.

The telecom regulator – The telecom regulator also often has the power to request and demand information that it deems relevant for its investigation and to impose fines when a company or individual fails to supply requested information. Frequently, it operates an informative website and spam complaint channel. Typically, it cooperates at the international level and nationally with the police and/or governmental organisations and/or the DPA. Nevertheless, the division of competences between the telecom regulator and the DPA is not always very clear with shared competences for data protection in electronic commerce but not in relation to spam in specific.

Other competent authorities – In some countries, the responsibility to fight online malware is (also) given to another governmental body, such as the ministry of economics and, to a lesser extent, the consumer protection authority[11].

No centralisation of competences – In none of the States, one governmental authority has competence over all matters pertaining to online malpractices. Nevertheless, some Member States have a clear organisational responsibility for enforcement activities and have therefore given increased powers to a number of governmental departments to fight online malpractices. Also, some governmental departments have stronger powers than others. Some Member States also give certain competence to the ombudsman.

Police competences – In several Member States, the police has specific task forces to deal with computer crime. In any case, the public prosecutor will have criminal enforcement powers when spam contains illegal content.

1.3 Malware: measures taken by stakeholders

1.3.1 Malware and measures taken by competent authorities

Awareness measures – Competent national authorities often adopt a proactive approach and provide information to users on how to adequately protect themselves against malware and internet fraud (awareness raising). Often, the national CERT also provides information to internet providers on security incidents and measures to prevent them.

Complaint channels – Communication channels are usually provided to users and subscribers to formulate their complaints against unsolicited commercial communication or, more generally, illicit content and behaviour on internet. When they have investigative powers, the relevant authorities may request and demand information that they deem relevant for their investigation.

Organisation – In practice it can be seen that sufficient staff is needed to deal with the millions of spam messages received via the complaint channel. Some Member States have therefore transferred this competence to a bigger structure, such as the telecom regulator.

[11] In Denmark for instance, the authority responsible for enforcing the ban on spam is the Danish Consumer Ombudsman. In Belgium, officials of the ministry of economics have investigative powers, can make legally binding protocols and can act as witness in court.

Sanctions – In a number of cases, administrative or judicial sanctions have been imposed specifically in the context of spam (see below under chapter 1.4).

1.3.2 Malware and measures taken by the service provider industry

Amount of providers – Some countries have only a very limited number of internet access providers, while others have (way) over a hundred providers[12]. Most countries have a national ISPA[13].

Filters – Mostly, the service provider industry has implemented technical measures, such as (effective) spam filters, which compensate to a certain extent for the weaker legal enforcement of legal anti-spam provisions[14]. However, it remains to be seen whether such spam filters will keep on functioning at their present performance level in the future. In some Member States, the government clearly emphasises the role of service providers as responsible actors who should implement high information security standards. Very few Member States indicate actions undertaken by mobile service providers[15]. A good example of action by mobile providers is France, where the associations of telecom and mobile operators launched a website specifically dedicated to mobile spam. It provides information on what is mobile spam and what the user can do about it.

Black and white lists – Often internet access providers also use black lists. Because black lists bear the risk of banning legitimate e-mail, Germany is experimenting with a centralised white list of legitimate mass mailers. This ensures that genuinely desired mailings (on both parts) from legitimate originators reach their destination without the mailer needing to worry about their mail being black listed. It also happens that a service provider offers a personalised anti-spam service, allowing for the creation of personal white and black lists.

Awareness measures – Regularly, ISPs also provide users with tips on how to combat spam.

Spam policy – Often, ISPs have an explicit spam policy in the contracts with users, prohibiting users from sending spam or malicious software, thereby reserving the right to interrupt the service and to terminate the contract with the user.

Code of conduct – Sometimes, service providers have a code of conduct with spam related measures.

[12] For example Cyprus only has a bit over 10 access providers, Luxembourg a bit over 20, Latvia over 40, Romania and the Netherlands over 50. Other relatively small Member States on the other hand, such as Austria, Denmark or Lithuania, have well over a 100 providers. Hungary indicates a presence of almost 300 providers. In Italy, the amount of providers is said to be 'very high'. In the UK, there are over 150 providers.

[13] In Luxembourg for instance, the national ISPA ceased to exist in 2002. In some Member States, such as the Netherlands or Romania, some major ISPs are not represented in the national ISPA.

[14] Often such filers appear to be offered for free. In some cases, a small monthly compensation is charged.

[15] Mobile spam is however considered the biggest problem in Cyprus.

1.3.3 Malware and measures taken by the vendor industry

Actions at national level – Information on actions undertaken by software vendors at national level appears to be difficult to obtain. Even Member States with a high activity level and proactive approach in the fight against online malpractices do not produce a lot of information in this respect. This may in part be due to the fact that vendors usually don't limit their territory to one Member State.

Nevertheless, it appears that the vendor industry sometimes contributes to awareness campaigns and publishes information and warnings on information security risks to both consumers and professional organizations. For example, vendors may sponsor awareness campaigns on safer internet use in the context of the yearly "Safer Internet Day" activities.

Actions at international level – Vendors are sometimes seen to participate in international cooperation activities (see below under chapter 1.5.3[16]).

1.3.4 Malware and measures taken by private parties

In some Member States, there are one or more personal websites which provide up-to-date information on all kinds of online malware.

1.3.5 Overview of main informative websites and complaint channels

Abbreviations used in the table below:

- DPA = data protection authority
- PPP = public private partnership
- TA = telecom and media authority
- CA = consumer authority
- CERT = computer emergency response team
- CSIRT = computer security incident response team
- ISPA = internet service providers' association

Country	Informative website	Complaint channel
Austria	www.help.gv.at	*No information available*
	www.rtr.at	

[16] For example vendor participation in the MAAWG and the APWG.

Belgium	www.spamsquad.be (PPP) http://economie.fgov.be (government) www.privacycommission.be (DPA)	www.ecops.be (police) www.privacycommission.be (DPA)
Bulgaria	www.cybercrime.bg (police)	www.cybercrime.bg (police)
Cyprus	www.cyberethics.info (PPP) www.dataprotection.gov.cy (DPA)	www.dataprotection.gov.cy (DPA) www.cyberethics.info (PPP) www.mtn.com.cy (website of a private ISP)
Czech Republic	www.uoou.cz (DPA)	www.uoou.cz (DPA)
Denmark	www.it-borger.dk (TA) www.itst.dk (TA) www.cert.dk (national CERT) www.forbrug.dk (CA) www.spyware.dk (private) www.pc.sikkerhed.dk (private)	Email: spam@forbrugerombudsmanden.dk (ombudsman – for spam) Email: itst@itst.dk (TA – for spyware and malicious software)
Estonia	www.arvutikaitse.ee www.ria.ee (CERT) www.nupukas.ee (CA) www.tka.riik.ee (CA) www.dp.gov.ee (DPA)	www.dp.gov.ee (DPA) www.tka.riik.ee (CA)
Finland	www.ficora.fi (TA) www.tietosuoja.fi (DPA)	www.cert.fi (CERT)
France	www.signalspam.fr (PPP) www.cnil.fr (DPA)	www.signalspam.fr (PPP) www.internet-signalement.gouv.fr (government) www.cnil.fr (DPA)
Germany	www.internet-beschwerdestelle.de (ISPA) www.eco.de (ISPA) www.bsi-fuer-buerger.de (IT security agency)	www.internet-beschwerdestelle.de (ISPA) Email: whitelist-complaints@eco.de Email: rufnummernspam@bnetza.de (federal

	www.klicksafe.de (TA)	network agency – cold calls and SMS)
Greece	www.dpa.gr (DPA)	www.dpa.gr (DPA)
	www.1020.gr (government)	www.synigoroskatanaloti.gr (ombudsman)
Hungary	www.baratsagosinternet.hu (PPP)	Email: spam-bejelentes@nhh.hu (TA)
	www.50plusz.net (private)	Email: cert@cert-hungary.hu (CERT)
	www.virushirado.hu (PPP)	www.megelozes.eu (police)
	www.biztonsagosinternet.hu (CERT)	
Ireland	www.dataprotection.ie (DPA)	www.dataprotection.ie (DPA)
		www.regtel.ie (industry)
Italy	www.garanteprivacy.it (DPA)	www.denunceviaweb.poliziadistato.it (police)
	www.commissariatodips.it (police)	Toll free telephone: +39 800 16 66 61
Latvia	www.netsafe.lv (PPP)	www.ddirv.lv (CSIRT)
		www.netsafe.lv (PPP)
		www.dvi.gov.lv (DPA)
		www.ptac.gov.lv (CA)
Lithuania	www.esaugumas.lt (TA)	www.cert.lt (CERT)
	www.ada.lt (DPA)	www.ada.lt (DPA)
	www.cert.lt (CERT)	www.vartotojoteises.lt (CA)
Luxembourg	www.cases.lu (government)	www.police.public.lu (police)
Malta	www.mca.org.mt (TA)	www.mca.org.mt (TA)
	www.police.gov.mt (police)	www.dataprotection.gov.mt (DPA)
	www.mtcert.gov.mt (CERT)	www.dataprotection.gov.mt (DPA)
		police.gov.mt (police)
Poland[17]	www.uokik.gov.pl (CA)	www.federacja-konsumentow.org.pl (consumer federation)
		www.giodo.gov.pl (DPA)
		www.uokik.gov.pl (CA)

[17] See: http://www.uokik.gov.pl/en/consumer_protection/consumer_on_the_internet/spam/#pytanie9.

Portugal	www.anacom.pt (TA) www.cert.pt (CERT)	www.anacom.pt (TA) Email: geral@cnpd.pt (DPA)
Romania	www.anrcti.ro (government)	www.anrcti.ro (government) Email: relatii_cu_publicul@anrcti.ro (TA)
Slovakia	*No information available*	www.teleoff.gov.sk (TA)
Slovenia	www.arnes.si (CERT) www.ti.gov.si (government)	*No information available*
Spain	www.agpd.es (DPA) www.inteco.es (national institute of communication technologies)	www.agpd.es (DPA) www.inteco.es (national institute of communication technologies)
Sweden	www.sitic.se (Swedish IT incident centre) www.pts.se (TA) www.surfalugnt.se (PPP)	www.sitic.se (Swedish IT incident centre) www.epostreklam.konsumentverket.se (CA)
The Netherlands	www.spamklacht.nl (TA) www.consuwijzer.nl (CA, TA and completion authority) www.waarschuwingsdienst.nl (CERT)	www.spamklacht.nl (TA) www.meldpuntcybercrime.nl (police)
United Kingdom	www.ico.gov.uk (DPA) www.ukcert.org.uk (CERT)	forms.ico.gov.uk (DPA)

1.4 Malware: administrative and judicial sanctions

Administrative sanctions – In a number of Member States, administrative sanctions in the form of fines have been imposed by competent authorities[18]. Mostly they relate to spam (i.e. the fact of sending spam, not the content of the spam messages). Nevertheless, the amounts imposed are usually not very high, so that their deterring effect may be rather limited. The advantage a spam-ban upon action undertaken by authorities in comparison to action by individuals is that such ban goes for spam sent to anybody, not only the claimant himself.

Judicial sanctions – There are only a few effective judicial sanctions against online malpractices in Member States. This may in part be due to the fact that end users do not usually have the know-how and means to start proceedings. A right for network operators to sue spammers may be helpful in

[18] A very good example in this respect is Italy.

this respect.. Two cases have been reported where the infringer was sentenced to imprisonment, be it that the imprisonment was commuted to a fine[19].

Overview – Below is an overview of examples of sanctions imposed at national level in the past years.

Czech Republic	• the DPA imposed fines in total of around 15.000 EUR in 2007
Denmark	• a Danish commercial court imposed a fine of around 270.000 EUR for mobile spam • as a result of legal action undertaken by the Danish Consumer Ombudsman, Danish companies were fined respectively around 13.330 EUR, 2.670 EUR, 1.330 EUR, 670 EUR and 1.330 EUR in 2008 • in 2009, a fine of around 3.330 EUR has been metered out by the court to a Copenhagen nightclub for unsolicited text messages containing information about events etc. taking place at the nightclub
Finland	• conviction for writing malicious software, including use of spyware and spam • sentenced to 7 months in prison, later commuted to 162 hours of community work
Germany	• numerous cease and desists orders of district courts and higher courts threatening the defendant with administrative fines not exceeding 250.000,00 €, alternatively arrest for contempt not exceeding 6 months; often also conviction to pay fine of 2.500,00 € for each violation of the cease and desist order • court orders actually *imposing* these fines are not publicized
Greece	• imposition of a fine of 20.000 EUR for

[19] Decision of an Italian court of appeal of 2008 and decision of a Finnish first instance court of June 2008.

	sending spam to random mobile numbers
Hungary	• in 2007, a total sum of around 6.400 EUR was imposed • in 2008, this amount was 10 times higher (the maximum fine is 500.000 HUF): one spammer was fined seven times with a total sum of fines amounting to 1.6 million HUF (around 5.333 EUR at the time of this Study)
Ireland	• the DPA applied two fines for mobile spam (one of 2.000 EUR in 2008 for sending 6 text messages)
Romania	• in 2008, the telecom regulator applied fines in 20 cases, ranging from 250 EUR to 500 EUR • the DPA applied two fines for mobile spam (via SMS)
Italy	• in 2008, the DPA imposed a fine of 570.000 EUR on an SMS spammer • in 2004, the Naples court of peace sentenced a spammer to a fine of 1.000 EUR • in 2002-2003, the DPA issued a number of decisions ordering to stop the sending of spam • an Italian court of appeal sentenced a sender of malware and spyware infected e-mail to a fine of 4.280 EUR
Latvia	• the DPA imposed fines in two cases for a total amount of 4.300 EUR
Lithuania	• in 2008, the DPA applied administrative sanctions in 3cases; 2 of them were confirmed by the administrative court; 1 case is still pending
Poland	• the consumer policy department ordered to

	cease infringement of consumer interests through spam
Spain	• in 2008, the DPA imposed 39 fines for sending spam with a total of 85.500 EUR as follows: 81.100 EUR for 34 e-mail spam cases (of which 30.000 EUR for two serious e-mail spam cases), 3.800 EUR for 4 SMS spam cases and 600 EUR for one fax spam case.
Netherlands	• in 2006, the telecom regulator imposed a fine of 75.000 EUR for sending spam • in 2007, three Dutch companies were fined 1.000.000 EUR for placing adware and spyware • in 2008, a spammer was fined 510.000 EUR

1.5 **Malware: cooperation activities**

1.5.1 Cooperation between governmental bodies

In many Member States, efforts are being made to coordinate actions efficiently between competent authorities. The level of coordination is however quite different.

Loose cooperation –In several Member States, coordination stops at the level of general informal contacts and, as the case may be, (obligatory) administrative assistance[20]. Such preventive cooperation rarely leads to actual joint case resolution. As a result, working groups may be set up or memoranda may be drafted to try to clarify the different responsibilities[21]. Also, cooperation may exist on a more general level, e.g. in relation to information security and computer crime, without actual focus on spam or spyware[22].

[20] For example in Slovenia, Slovakia, Portugal, Poland, Estonia, Denmark and Bulgaria. In Germany, the federation of consumer organisations and the agency against unfair competition periodically exchange information on spam cases.
[21] For example in Greece and Finland.
[22] For example in Luxembourg and Malta. In Hungary, the competition authority cooperates with the telecom regulator for the protection of the electronic communications market and with the consumer protection and financial supervisory authorities on the prohibition of unfair commercial practices against consumers.

Tighter cooperation – In other Member States, competent authorities jointly developed strategies for awareness raising, cooperation with the private sector and international cooperation. Typically, coordination and/or cooperation takes place between the national telecom regulator and the national DPA. Sometimes, other authorities are involved as well[23].

1.5.2 Cooperation between government and industry

Formal cooperation – In some Member States[24], the competent authorities have actually concluded formal collaboration agreements with the industry and/or jointly organise awareness campaigns. Such information is therefore readily available. Another option may be that a working group within the national DPA is obliged to collaborate with the industry.

Informal cooperation – In other Member States however, such cooperation may be of a less formal nature and therefore less accessible. Also, it may not go further than joint awareness raising.

1.5.3 Cooperation at international level

Certain Member States are more actively involved at the international level than others and even see it as their responsibility to share their expertise and experience in the area of cyber security in an international context[25]. Mostly, international cooperation takes place in the context of the following formalised schemes:

Contact network of spam authorities (CNSA) – At EU level, the European Commission has set up a contact network of anti-spam' enforcement authorities in 2004 to share information and pursue complaints across borders in a pan-European drive to combat spam. The authorities include data protection authorities, IT and telecom authorities and a few consumer protection authorities. They agreed to cooperate in investigating complaints about cross-border spam from anywhere within the EU. The contact network of spam authorities facilitates the sharing of information and best practices in enforcing anti-spam laws so as to make it easier to identify and prosecute spammers anywhere in Europe[26].

Operation Spam Zombies – Some Member State agencies also extend their cooperation beyond the European Union by joining 'Operation Spam Zombies', an initiative of the United States Federal Trade

[23] For example in the UK, the DPA and Office of Communications signed a letter of understanding on the enforcement modalities of privacy and electronic communications. In the Netherlands, the telecom regulator concluded formal cooperation agreements with the high tech crime unit of the police, the consumer protection agency and the DPA. In Romania, the telecom regulator is said to have concluded cooperation protocols with the DPA and the police, such protocols are however not public. In Latvia and Lithuania, the telecom regulator and the DPA cooperate for the fight against spam. In Italy, the DPA closely cooperates with the police. In France, the DPA and SignalSpam have an anti-spam partnership in place.

[24] For example Belgium, Cyprus, Estonia, Romania and the Netherlands.

[25] Most Member States participate in at least one of the initiatives. Member States with no participation are Luxembourg, Finland, Romania, Slovakia, Slovenia and Sweden.

[26] The Member States that joined the CNSA project from the beginning are Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, France, Greece, Ireland, Italy, Lithuania, Malta, the Netherlands and Spain.

Commission, members of the London Action Plan and other governmental agencies to target so-called spam zombies, i.e. the technology trick used by illegal spammers to tap into consumers' home computers and use them to send millions of pieces of illegal spam. By routing their e-mails through "zombie" computers, the spammers are able to hide the true origin of the spam from consumers and make it more difficult for law enforcement to find them. Consumers often do not discover that they, themselves, have been sending spam[27].

SpotSpam – SpotSpam is a project supported by the European Commission's Safer Internet Programme and Microsoft, which aims at facilitating the cross-border fight against spam, phishing and other forms or illegal electronic communication, in particular legal action against spammers at the international level[28]. In these countries, spam complaints can be submitted to the SpotSpam database via national Spamboxes. The information stored in the database enables appropriate authorities to take action against spammers: LEAs and registered companies taking court-action against spammers can retrieve information from and add new cognitions to the database. Co-operation with more partners was planned to enhance the capabilities of the database and make it an even more efficient tool at a later stage. Due to a lack of funding for technical adaptations towards the finalization of the project, the database did not go live, yet. Due to the still large interest of authorities and the huge potential of the database, the German ISPA is currently looking for further funding to finally kick off the project and to maintain its operation.

London Action Plan (LAP) – The purpose of this Action Plan is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing and dissemination of viruses. The participants also open the Action Plan for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement cooperation[29]. In October 2008, a conference was organized together with the CNSA, ENISA and the German host (Hessen IT). This event was sponsored by several IT vendors.

MAAWG – The Messaging Anti-Abuse Working Group (MAAWG) is a global organization of Internet Service Providers (ISPs), network operators, anti-spam technology vendors, e-mail service providers and other forms of senders as well as other interested parties. MAAWG originated in 2004 and represents almost one billion mailboxes, key technology providers and senders. It focuses on preserving electronic messaging from online exploits and abuse (e.g. spam, virus attacks, denial-of-service attacks, etc.) with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives. The MAAWG holds three members-

[27] The Member States that joined Operation Spam Zombies from the start are Belgium, Bulgaria, Cyprus, Denmark, Germany, Greece, Ireland, Lithuania, the Netherlands, Norway, Poland, Spain and the UK.
[28] Two Member States participate in this project: Germany and Poland.
[29] The Member States that joined the LAP are Belgium, Denmark, Finland, Hungary, Ireland, Latvia, Lithuania, Spain, Sweden, the Netherlands and the UK.

only meetings per year: two in North America, and one in Europe[30]. In October 2007 a joint MAAWG/LAP/CNSA conference was organised in Washington DC.

APWG – The Anti-Phishing Working Group (APWG) is a global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and e-mail spoofing of all types. The stakeholders exchange information and compile good practices between them.

The NATO Cooperative Cyber Defence Center of Excellence – This international center conducts research and training on cyber warfare and is located in Tallinn, Estonia[31].

IWGDPT (International Working Group on Data Protection in Telecommunications) – The Working Group was founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners at the initiative of the Berlin Commissioner for Data Protection, who has since then been chairing the Group. The Group has since 1983 adopted numerous recommendations ("Common Positions" and "Working Papers") aimed at improving the protection of privacy in telecommunications, including spam. Membership of the Group includes representatives from Data Protection Authorities and other bodies of national public administrations, international organisations and scientists from all over the world. Since the beginning of the 90s the Group has in particular focused on the protection of privacy on the Internet.

OECD Task force on spam – The OECD has launched an anti-spam toolkit as the first step in a broader initiative to help policy makers, regulators and industry players orient their policies relating to spam solutions and restore trust in the internet and e-mail[32].

Bilateral initiatives – Apart from these multilateral cooperation structures, there seems to be also room for bilateral arrangements. An example hereof is the collaboration agreement between France and Japan for coordinated international action in the fight against spam. Both countries especially consider to exchange information and good practices regarding the field of anti-spam policies and strategies.

[30] As of May 2008, MAAWG Sponsor members included AOL, AT&T, Bell Canada, Charter Communications, Cloudmark, Comcast, Cox Communications, EarthLink, FT Group, Goodmail Systems, OpenWave, Yahoo!, Time Warner Cable, and Verizon. Full members elected to the Board of Directors were Cablevision and Return Path Inc.

[31] It currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain.

[32] The Member States that participate in the OECD project are Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Poland, Portugal, the Slovak Republic, Spain, Sweden and the UK.

Section Three: Conclusions of the Study

In the below tables, a summary overview of the main findings from the Study is provided. It results, amongst others, from the Study that

- several Member States have internal cooperation procedures in place, bringing together the technical and investigative expertise of different government agencies and establishing close cooperation with network operators and ISPs;
- in general, Member States should invest more substantial resources to gather evidence, pursue investigations and mount prosecution in this field;
- not all Member States subscribe to the available international cooperation procedures and are therefore not able to immediately act on requests for cross-border assistance;
- almost all Member States have one or more informative website and one or more complaint channel to deal with on spam and spyware.

The Study did not result in substantial information on actions taken by the industry (software vendors, etc.) such as adequate privacy information to the users of software products or emphasis on egress filtering.

1.6.1 Awareness raising

In most Member States, awareness raising measures are undertaken by competent authorities as well as by private companies. Usually, one or more websites are made available with comprehensive information on spam and/or malware, including advice on how to best protect against them.

1.6.2 Enforcement

A number of Member States can be considered as forerunners in the fight against spam and online malware. These are usually the Member States in which administrative fines and/or judicial sanctions have been imposed or where the service provider industry is very proactive. In other Member States, actual enforcement of the legal anti-spam framework through sanctions is rarely seen. Often, this is due to insufficient or ambiguous competences, a lack of appropriate resources or simply because of other priorities.

1.6.3 Cooperation

In most Member States, government authorities work together in one way or the other. Sometimes, such cooperation is loose and informal. At other times, it is tighter and more efficient. Also, most

Member States are involved in one or more international anti-spam related projects .

1.6.4 Reflections

Role of the government – Based on the results of the Study, it can be concluded that in general, a stronger commitment by central government to fight online malpractices is necessary in Member States. The same is true for a clearer organisational responsibility for enforcement activities and adequate resources for the enforcement authority. It may be questioned whether enforcement of the anti-spam ban could not be more effective if centralised and assigned to one single authority.

Role of the service provider industry – One may question whether the degree to which the handling of IT security today is left with the individual and often inadequately informed user, is not too high. As a matter of fact, such situation may be considered neither fair nor reasonable and leads to the question whether not more responsibility should be shifted to those players that have a real possibility to improve the level of security. Incentivising the internet industry to provide a more appropriate technical architecture response (security measures and e-mail authentication technologies) to practices hindering internet traffic and limiting satisfaction of the internet users may indeed be more efficient than enforcement policies targeting at individual perpetrators. As ISPs are not directly affected themselves, they may not have the economic incentive. On the other hand, ISPs should have their own right to sue spammers. For the purpose thereof, existing legislation may have to be reviewed in view of changes to facilitate such action by ISPs. Finally, there should be sufficient cooperation between the service providers themselves.

Internal cooperation – The nature of cybercrime demands strong inter-agency cooperation for the purpose of sharing knowledge and experience. Legal means to exchange information should be in place. Spam cannot be adequately addressed on the basis of administrative assistance only.

International cooperation – More international cooperation, both within the European Union as on a global level, appears necessary to adequately deal with the problem of online malpractices. Competent government agencies should have sufficient manpower and budget to travel and meet international partners. They also should have the legal means to investigate, to assist each other and to exchange information cross-border.

Public-private partnerships – Government agencies should not hesitate to seek cooperation with private companies, which often have a vast amount of knowledge and information about internet security. Moreover, they also have a clear interest in keeping the net safe. A successful approach to fight online threats requires a combination of prevention, enforcement and raising public awareness by the relevant public and private stakeholders.

Efficient combat – Even in countries with effective legislation, the anonymity of spam senders remains a difficult hurdle in the fight against online malpractices. The biggest problem in all Member States seems to be the technical means and the fact that most spam are received from abroad.

Future – The core problems must be strongly addressed to encounter better the new development and speed of innovation in targeted spam and spyware tools and methods. It will be of particular importance to address the problems simultaneously at all appropriate levels, in particular through enforcement, cooperation, self-regulation and technical means. All kinds of electronic communication should be envisaged. Particular attention should go to mobile communication and social networks.

Section Four: Main findings per Member State

The tables in this section contain the main findings per Member State relating to:

- on the one hand, measures undertaken by competent national authorities, by the service provider industry and by the vendor industry;
- on the other hand, cooperation activities between governmental bodies, between the government and the industry and in general at international level.

Also, for every country a short assessment of the activity level in combating online malware is given.

1. Austria

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The national telecom regulator already imposed fines. *Judicial decisions* – No criminal cases have been reported so far. *Awareness measures* – Competent authorities have published information on spam but there is no official website to warn users about online malware. *Complaint channels* – There is no online complaint form provided to end-users. Complaints must be submitted to the telecom regulator by e-mail or letter. Under article 7 of the Austrian E-Commerce Act (ECG), the telecom regulator is required to maintain a registry of persons and companies who do not wish to receive promotional e-mail (the so-called "ECG list", a kind of public Robinson list). Such parties can have their names entered in this registry free of charge via the e-mail eintragen@ecg.rtr.at.
Measures undertaken by the service provider industry	Mobile network and service providers as well as internet service providers have implemented (web-based) spam filters, use blacklists, etc. The effectiveness of these filters compensates to a certain extent for the weaker legal enforcement of strict legal anti-spam provisions. Internet service providers also established a Code of Conduct. ISPA has established an anti-spam working group. Also, the industry has taken the major burden in developing appropriate spam filters. Through ACOnet, an organisation of universities, academic hospitals, research institutes and other scientific institutes effective spam filters of ISPs

	were developed.
Measures undertaken by the vendor industry	There are several ICT enterprise associations and other platforms that are in some way or another involved in combating online malpractices. The vendor industry allows everybody to be included on a Robinson list against unsolicited commercial communications.

Cooperation activities to combat malware	
Cooperation between governmental bodies	Internal coordination between the competent authorities is based on informal contacts and the principle of administrative assistance.
Cooperation between government and industry	Cooperation between public authorities and industry actors exists but it is mostly informal.
Cooperation at international level	The telecom regulator participates in the CNSA on behalf of Austria. It also participated in the anti-spam working group of the OECD.

General assessment
Austria can be considered as a Member State where appropriate actions and measures have been undertaken related to the combat against online malpractices such as spam, spyware or malicious software. Action is focused on strict laws and technical enforcement, e.g. industry actors have taken the major burden in developing appropriate spam filters. Co-operation between public authorities and industry actors exists at a sufficient level but mostly informal. Cooperation between public authorities is based on the principle of administrative assistance. It appears that spam is not considered a real problem at the moment. For the future, this observation is subject to spam filters functioning at the present level. Supervisory authorities seem to lack resources for more effective sanctioning and national and international co-operation. Internet providers, in particular the Austrian Science Network, claim to invest considerable financial resources. Finally, efforts are being made to co-ordinate actions efficiently.

2. Belgium

Measures undertaken to combat malware	
Measures undertaken by competent national	*Administrative decisions* – Unfortunately, competent administrative authorities cannot impose fines.

authorities	*Judicial decisions* – So far, no convictions for spam and spyware took place because the Federal Public Service Economy, SMEs, Middle class and Energy and of the national DPA do not have the power to impose sanctions. The actual power to prosecute lies with the Public Prosecutor. *Awareness measures* – The competent authorities try to keep citizens well informed through websites and brochures. *Complaint channels* – Citizens can file a complaint on the website ecops.be (see below).
Measures undertaken by the service provider industry	ISPs collaborate with the government to fight spam through the eCops portal. Also, most ISPs offer their clients spam filters, tools to detect spyware and protection against viruses and use black lists.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	- Ecops.be The federal computer crime unit of the police and the ministry of economics have jointly set up this website, which is an online reporting service to which the Internet user can report crimes committed on or through Internet (misleading information, spam, etc.). eCops makes sure that a report is being investigated by the appropriate service. - Spamsquad.be This is the Belgian portal site in the fight against spam, set up by a number of stakeholders, including the ministry of economics, the DPA, the federal computer crime unit of the police, the direct marketing association, the internet service providers association, etc.
Cooperation between government and industry	- Cooperation protocol The internet service providers association and the ministries of justice, interior and telecom affairs concluded a cooperation agreement for the

	fight against illegal behaviour on internet. This protocol has become less important since the launch of the eCops portal (see infra) by the internet service providers association, the ministry of economic affairs and the police. - Spamsquad.be This is the Belgian portal site in the fight against spam, set up by a number of stakeholders, including the ministry of economics, the DPA, the federal computer crime unit of the police, the direct marketing association, the internet service providers association, etc.
Cooperation at international level	Belgium actively participates in international campaigns and actions (LAP, CNSA and OECD).

General assessment
Belgium can be considered as a Member State where appropriate actions and measures have been undertaken related to the combat against online malpractices such as spam, spyware or malicious software. Various authorities have been made competent in order to make the fight against spam and spyware a success. There is awareness that these are important problems and campaigns to inform civilians have been worked out. Also, commitment can be demonstrated by a relatively quick implementation of European legislation. Unfortunately, the DPA has no real sanctioning power. Also, a collaboration scheme between international authorities and private partners such as ISPs has been set up and Belgium participates actively in international action plans and think thanks. The various competences however are not always clearly defined but this does not seem to cause a lot of problems. The biggest problem however is that no administrative decisions are being imposed due to a lack of sanctioning power of the competent authorities and that makes it very difficult to act fast and efficiently when faced with spam and spyware.

3. Bulgaria

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No information available. *Judicial decisions* – No information available. *Awareness measures* – A lot of information about online malware is available via the internet. In particular the website of the Department

	for combat against organized and heavy crime (cybercrime.bg) contains essential cybercrime terminology, explained in a clear and understandable manner and advice on how to protect against online malware *Complaint channels* – Cybercrime.bg (see above) contains an on-line form for submitting particular warnings about online malpractices.
Measures undertaken by the service provider industry	The Bulgarian direct marketing association adopted a code of conduct, including rules on commercial electronic communications. This code corresponds to the requirements of applicable Bulgarian and European legislation. Financial institutions sometimes warn on their website about the most important internet threats, in particular phishing. Some ISPs offer their clients spam filters and use black lists.
Measures undertaken by the vendor industry	No information available.
Cooperation activities to combat malware	
Cooperation between governmental bodies	Generally speaking, competent governmental bodies do not exchange information. Also, there are no co-operation procedures or initiatives in place between them, except for some co-ordination procedures in respect to the adoption of new legislation in this area.
Cooperation between government and industry	No information available.
Cooperation at international level	Bulgaria participates in Operation Spam Zombies but does not yet participate in the CNSA.

General assessment
In Bulgaria, actions against online malpractices such as spam, spyware or malicious software are mainly concentrated on such malpractices which are considered as crimes. The competences for combating on-line malpractices are scattered between different institutions. In practice, some authorities lack competences, whereas others have large competences but not those needed to combat against on-line malpractices. Consequently, the necessary experience may not be available. In this regard revision of the legal framework is needed and when doing so, sufficient attention should be given to cooperation between governmental bodies, which cooperation is currently not

existent. Also, more financial resources and efforts are necessary to co-ordinate the actions of the different authorities efficiently.

4. Cyprus

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Both the telecom regulator and the national DPA can impose fines. So far, the DPA imposed twice a fine between EUR 2.500 and 3.500 EUR, i.e. relatively limited amounts. *Judicial decisions* – The reported court cases relate to possession of child pornography, not to online malware practices. *Awareness measures* – 1) The CyberEthics website (www.cyberethics.info) serves as a general hotline for cyber crime activities. It is co-funded by the EC Safer Internet Programme. 2) The Cyprus police has its own website (www.police.gov.cy) where it provides advice on the prevention of fraud through online malware. 3) The national DPA issued guidelines for the public on the protection against spam (www.dataprotection.gov.cy). *Complaint channels* – There is no online complaint channel in Cyprus. The DPA receives some complaints relating to spam and usually does not act prior to receiving such a complaint, mainly due to a lack of sufficient personnel.
Measures undertaken by the service provider industry	At least one service provider offers the possibility to users to report spam messages via an online form (www.mtn.com.cy/index.cfm/id/79/lang/english). Several ISPs offer their clients (web based) spam filters, use blacklists and have an explicit spam policy in place.
Measures undertaken by the vendor industry	No specific information available. Some service providers profile themselves as specialists to advice organizations and institutions on the security of their computer systems. IT enterprises founded their own association.

Cooperation activities to combat malware	
Cooperation between	The telecom regulator and the national DPA commonly supervise data protection compliance in the area of IT and spam in particular.

governmental bodies	Therefore, they also coordinate in order to fight spam. The telecom regulator also works closely together with the Cyprus police for the investigation and prosecution of cybercrime.
Cooperation between government and industry	The Cyberethics project results from a partnership between government agencies, press, media groups and ISP associations. The police cybercrime department collaborates with private companies such as Microsoft for the purpose of conducting its investigations, receiving specialist training and using specialist resources.
Cooperation at international level	Cyprus participates in the CNSA and Operation Spam Zombies. The police cybercrime department also collaborates with the FBI.

General assessment
Cyprus can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. In comparison to other Member States with a strong enforcement profile, Cyprus is steadily improving its strategy in combating online malpractices. A number of legislative instruments exist and several governmental bodies have been granted increased powers. The supervisory authority (in particular the national DPA) appears not to be using its investigatory powers to the fullest extent. On the other hand, credit can be given to the Cyprus Police. According to general press announcements, the government has invested considerable financial resources and efforts are being made to improve its specialist electronic crime department. The telecom regulator closely cooperates with the DPA and the police. The government and the private industry set up a partnership for all cybercrime issues. Cooperation at international level takes place through the CNSA and Operation Spam Zombies.

5. Czech Republic

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The DPA can impose fines of up to 10 million crowns on Czech spammers. In 2007, the national DPA imposed fines in total of around 15.000 EUR. The highest sanction ever imposed by the DPA amounted to 8.500 EUR. *Judicial decisions* – No information available.

	Awareness measures – The website of the national DPA contains general information about spam and phishing. There is no official resource for information about spyware and malicious software. *Complaint channels* – The website of the national DPA contains an online form to file a complaint concerning the sending of spam.
Measures undertaken by the service provider industry	None of the industry associations have a project to fight online malpractices, but internet service providers mostly block spam messages through spam filters. Financial institutions sometimes warn on their website about phishing attempts.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The national DPA and telecom regulator merely cooperate at the level of passing on cases of jurisdiction. There is no information available that would indicate cooperation on actual case resolution.
Cooperation between government and industry	Upon request of the national DPA, the national DNS provider must suspend access to problematic domains. The DPA also cooperates with internet service providers: it informs them which of their clients infringe applicable legislation for the information society and requests suspension of e-mail accounts or hosting services based on the general terms and conditions of the service provider. Internet service providers are however not entitled to provide information about their clients to the DPA.
Cooperation at international level	The Czech Republic participates in the CNSA but Czech law does not set out the conditions necessary for transferring data to another country. This means that international cooperation is more theoretical.

General assessment
The Czech Republic appears not to have a developed and organized system for fighting online malpractices. However, a solid legal framework regulating spam is in place, which can be enforced.

The national DPA has already imposed several fines on Czech spammers. Cooperation between public authorities is based on the principle of administrative assistance. The DPA cooperates with internet service providers by sending them information on clients infringing anti-spam legislation. Cooperation at international level remains rather theoretical because of missing legal conditions for the transfer of data to another country. None of the industry associations have a project to fight online malpractices.

6. Denmark

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The Danish consumer ombudsman has taken legal action in a number of cases concerning spam from Danish business. The Danish Consumer Ombudsman (DCO) has taken legal action in a number of cases concerning spam from Danish businesses. - A major clothing chain store failed to observe the ban on unsolicited commercial enquiries when making automated voice message calls. After being reported to the police in 2007, the company agreed to pay a penalty of DKK 100,000 (€ 13,330) for infringing section 6(1). http://www.forbrug.dk/nyheder/pressemeddelelser/bode-hm/ (in Danish) - A business was in 2008 fined DKK 20,000 (€ 2, 670) for failing to prove that the business has obtained consent from app. 375 of its customers prior to sending out commercial emails, thereby breaching section 6(1). http://www.forbrug.dk/nyheder/pressemeddelelser/spam0/ (in Danish) - A publisher distributed not less than 50 fax messages to potential customers without having obtained consent. A fine of DKK 10,000 (€ 1,330) was metered out to the business in 2008 for its violation of section 6(1). http://www.forbrug.dk/nyheder/pressemeddelelser/kraks-spam/ (in Danish) - Two real estate agencies were in 2008 reported to the police for failing to observe the Danish 'Robinson list' (section 6(3) of the Danish Marketing Practices Act). The Robinson list is a register of citizens who do not wish commercial material and therefore has signed up to avoid being contacted in writing. The cases were closed upon the real estate agents accepting to pay penalties of DKK 5,000 (€ 670) and 10,000 (€ 1,330) respectively. http://www.forbrug.dk/nyheder/pressemeddelelser/reklame-robinson/ (in Danish) - A fine of DKK 25,000 (€ 3,330) has recently been metered out by the

	court to a Copenhagen nightclub for unsolicited text messages containing information about events etc. taking place at the nightclub. No material or media release is yet available. There have also been the following police notifications: - Nightclub reported to the police in January 2008 for distributing invitations without prior consent via SMS http://www.forbrug.dk/nyheder/pressemeddelelser/uanmodetsms/ (in Danish) - An organizer of Christmas events was reported to the police in August 2008 for conceding to having set out app 500 emails to recipients from whom they had not obtained consent. http://www.forbrug.dk/nyheder/pressemeddelelser/julegalla-spam/ (in Danish) - A computer business was in February 2008 reported to the police for sending targeted physical commercial material by ordinary mail in contravention of section 6(3) – the Robinson list. http://www.forbrug.dk/nyheder/pressemeddelelser/robinson/ (in Danish) *Judicial decisions* – In 2005, a Danish commercial court fined the German mobile telephone operator Debitel the record sum of two million kroner (approximately 270.000 EUR) by for sending unsolicited text and e-mail messages to phone users (http://www.smh.com.au/news/Breaking/Mobile-operator-fined-for-SMS-spam/2005/03/15/1110649167892.html?oneclick=true) On calculating the size of the fine, the Court took into consideration the number of messages and the number of recipients (app. 50, each of whom had received more than one message); the nuisance caused and the financial damage inflicted on the recipients, the majority of whom were small businesses wasting time and resources on processing the messages, and; the fact that the company continued to act contrary to section 6, even after having received guidance by the public authorities. On 21 January 2004 the Maritime and Commercial Court rendered another anti-spam judgment, this time in relation to a dealer in telecommunications solutions for businesses, whose marketing activities conflicted with section 6(1). The company was found guilty of violating section 6 due to its distribution of somewhere between 7,650-15,300 unsolicited advertising letters via fax. The company was fined

	DKK 400,000. In connection with the case, the DCO suggested the following fine calculation model to be applied to any violation of section 6 of the Marketing Practices Act, regardless of the manner in which the unsolicited commercial message was distributed: *A minimum fine of DKK 10,000 (€ 1,500) should be given for 100 instances of violation or less. A DKK 100 penalty for each instance of violation should be given in excess of 100 violations. Hence, the fine for 60 instances of violation would amount to DKK 10,000, and 140 instances of violation would amount to a penalty of DKK 14,000 (€ 1,900).* In the case in question, the Court also stressed the number of unsolicited commercial messages; the nuisance and financial damage inflicted on the recipients; information presented to the Court about the company's affairs; and, the number of complaints submitted to the DCO. This and other spam cases have served as trials against which the spam penalty calculation model as a standard has been tried and tested; those other cases include http://www.forbrug.dk/english/dco/actions/selected-court-case-abstracts/dmpa/section3/spam/ and http://www.forbrug.dk/english/dco/actions/selected-court-case-abstracts/dmpa/section6a/uccf/. In May 2003, the Maritime and Commercial Court in Copenhagen rendered its first decision in a case concerning bulk spam mail – in this case unsolicited commercial messages via fax and email. The spammer in question was fined DKK 15,000 (€ 2,000) for distributing 156 commercial messages. The spammer, a small company, sold software, leaflets and books to, presumably, other small businesses. The company was found guilty of violating section 6(1) of the MPA for distribution of unsolicited commercial messages via fax and email. *Awareness measures* – Various websites (ombudsman, consumer agency, IT and telecom agency, national CERT, some private websites contain information for end users regarding online malware and security. *Complaint channels* – The Danish consumer ombudsman provides

	information on how to file spam complaints.
Measures undertaken by the service provider industry	A trustmark scheme has been developed for safe and ethically responsible conduct on internet. It includes adherence to the ban on spam. The ISP security forum also adopted a binding code of practice to reduce spam. The internet access providers also agreed to carry out a central filtering of e-mails, whereby users may choose the degree of filtering.
Measures undertaken by the vendor industry	The Danish IT industry association discusses developments in IT security with software vendors in view of strengthening the overall IT security level. The Danish Board of Technology carried out a project concerning user IT security and came to the conclusion that the degree to which the handling of IT security today is left with the individual user, is too high. This situation is considered neither fair nor reasonable.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information available.
Cooperation between government and industry	An IT security committee has been established by the national IT and telecom agency with representatives from relevant private and public bodies. This committee has discussed but not really dealt with online malware.
Cooperation at international level	Denmark participates in the CNSA, Operation Spam Zombies and the OECD anti-spam task force.

General assessment
Denmark can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. The information is provided in a comprehensible manner and with a view to provide the public with information about how businesses and private persons may avoid harm deriving from spam, spyware and malware. On the other hand, no information is available that would indicate cooperation between governmental bodies. At the international level, Denmark participates in the

CNSA, Operation Spam Zombies and the OECD anti-spam task force. Generally speaking, a lot of actions have been taken in relation to the fight against spam deriving from Danish businesses. There is a greater focus on spam (actual enforcement) than on spyware and malware (limited to informing the public). This is in particular due to the high priority this issue has been given by the Danish Consumer Ombudsman, who has taken legal action in a number of cases.

7. Estonia

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Currently, one case is pending before the national DPA. No decision has yet been delivered. No information is available on cases handled by the national CERT. *Judicial decisions* – In 2008, over 150 computer related fraud cases were registered in Estonia. *Awareness measures* – Several websites have been launched to raise awareness of the general public, one of them specifically addressed at children and youth. The national CERT website contains educational videos on actual cases of persons falling victim to online malpractices and instructional videos on how to reduce online risks. Also, the national DPA informs and warns about spam on its website. Finally, the consumer protection authority has a website section with information on how to safely use the internet, including information on spam. *Complaint channels* – Complaints regarding spam can be filed with the national DPA. Electronic submission is possible provided it is digitally signed. Also, complaints regarding unfair commercial practices and general consumer protection issues can be filed online with the consumer protection authority. Finally, end users can address security incidents to their service provider or system/network administrator for further follow-up with the national CERT.
Measures undertaken by the service provider industry	ISPs have spam filters in place on their mail servers. Some websites of mobile operators contain security advice on WAP security, Bluetooth and IrDA security, mobile viruses and PIN codes.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The ministries of defence, education and research, justice, economic affairs and communications, internal affairs and foreign affairs jointly developed information society and cyber security strategies for 2008-2013. An important part thereof is raising awareness of the general public, where possible in cooperation with the private sector and sharing expertise and experience at both the domestic and international level. The strategies also indicate the responsible authorities and urge for a review of relevant legislation. The Estonian Informatics Council has the task of ensuring horizontal coordination between the public and private sector.
Cooperation between government and industry	Increased cooperation between government and industry is the purpose of the cyber security strategy for 2008-2013 (see above). A cooperation agreement was signed in 2006 between the leaders of Estonia's largest banks and telecom companies and the ministry of economic affairs and communications. The agreement envisaged the launch of the Computer Protection 2009 initiative, which aims at making Estonia the most secure information society in the world through appropriate investments in PC protection, user awareness and widespread use of the electronic identity card. As far as cooperation between ISPs and the national CERT is concerned, Estonian ISPs pointed out that the legal basis for such cooperation is unclear.
Cooperation at international level	Increased international cooperation is the purpose of the cyber security strategy for 2008-2013 (see above). Estonia participates in the CNSA. Estonia also hosts the NATO Cooperative Cyber Defence Centre of Excellence, an international initiative established in 2008 to enhance NATO's cyber defence capabilities[33].

General assessment
Estonia can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the

[33] Participating countries are Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic and Spain.

combat against online malpractices such as spam, spyware or malicious software.

The legal framework governing spam is fragmented – several legal acts regulate in one way or another sending of unsolicited e-mail. The lines of responsibility relating to spam enforcement between various government authorities appear diffused. One spam case is pending before the national DPA.

The fact that legal persons are not adequately protected from spam, even if there is no legal requirement under EU law to have an opt-in principle for legal persons, and the opt-out exception stipulated in the relevant law is perceived as being problematic.

Dissemination of spyware, malware or computer viruses is a criminal offence. The legal framework as well as the investigation of such cases is clear and offers adequate protection to both individuals and legal persons.

Estonia has an advanced and well implemented national IT infrastructure (electronic ID-card is mandatory; well established Public Key Infrastructure (PKI); e-government services and private sector e-services built on the public infrastructure; common digital signatures; Mobile-ID; etc). This enables Estonia to bring online security to a whole new level – banks are phasing out password based authentication (highest phishing risk) and gradually only ID-card and Mobile-ID (+PIN calculators) can be used to access e-banking services.

Increased cooperation between governmental bodies and between the government and the industry is part of the cyber security strategy for 2008-2013, which demonstrates the general awareness to combat cyber security problems. At the international level, Estonia cooperates in the CNSA.

8. Finland

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No information available. *Judicial decisions* – In the case "m00p" (conviction number 08/951 at Pori first instance court on 3 June 2008), a Finnish citizen was convicted of writing malicious software as a member of an international group. The case included use of spyware and spam and the offender was found guilty of endangering information system operations, and first sentenced to 7 months in prison, which was later commuted to 162 hours of community work. *Awareness measures* – Upon initiative of the ministry of interior, the government defined a program paper for combating on-line malpractices from a national security perspective, as part of organised

	crime. The national CERT notifies warnings on information security incidents on the web, as RSS, by e-mail, by SMS and teletext. *Complaint channels* – Citizens and organisations may submit complaints on the website of the national CERT. Organisations, administrations and selected professionals have additional complaint channels at their disposal (e-mail, telephone, tetra network VIRVE and face-to-face meetings).
Measures undertaken by the service provider industry	Service providers are called on by the government to inform users on various online risks and how to mitigate the risks, to offer information security services, to actively monitor for suspicious network activities and to respond to them accordingly. Service providers are explicitly entitled by law to take the necessary measures to ensure information security by removing malicious software from messages or preventing transmission of e-mail messages if necessary for safeguarding the network and their services in general. Finally, they are also asked to cooperate effectively with the national CERT. The Finnish IT association FiCom together with Finnish MNO's and data security companies has launched an Information Security Manual for Mobile users. The site offers a collection of practical advice on how to protect against security threats common to mobile devices and on how to act in the case an incident occurs. Internet service providers have an obligation to inform their customers on the different information security risks they might be exposed to, and to advise on the available methods for mitigating those risks. In practice, the main service providers sponsor awareness campaigns and offer contractual services to easily include information security services with other network services. Service providers are also obliged to monitor their networks and services in order to detect fraud and in the case of information security breaches. The obligations require that any found irregularity will need to be corrected by switching off, re-routing or by filtering network traffic. The national telecom regulator provides a so called Abuse Helpdesk in order to help and advice internet service providers in fulfilling these obligations. The national telecom regulator organises annual Abuse

	seminars for internet service provider information security personnel, in order to raise awareness and create working relations between different actors.
Measures undertaken by the vendor industry	The Internet Security Guide provides tips and instructions which aim at making Internet use safer for network users. It is an informative web-site on basic precautions and netiquette. The site is managed by the national telecom regulator, but it is sponsored by various software vendors and service providers as permanent channel linking the yearly "Safer Internet Day" activities. The online safety school website has been created to provide support for information security learning throughout all grades in primary school as well as for teachers and parents. For a younger audience, the site offers an online learning game on information security. The site is managed by the national telecom regulator, but it is sponsored by various software vendors and service providers as permanent channel linking the yearly "Safer Internet Day" activities. The projects SAFECode and OWASP regroup a large number of Finnish information industry companies. Finnish information security vendors such as F-Secure, Stonesoft and SSH contribute to awareness campaigns and publish information and warnings on information security risks to both consumers and professional organizations such a CERT-FI.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The division of competences between the national DPA and telecom regulator is difficult to determine in Finland. Whereas the DPA supervises the processing of personal data, the telecom regulator supervises the processing of identification data. To define better the responsibilities of each organisation and to define common actions to be taken for the combat of internet related crime in the form of unlawful collection of network users' personal data, a memorandum is being drafted by the competent authorities, which will be made public during 2009.
Cooperation between government and industry	The national CERT plays an important role in monitoring incidents at national level and cooperates with equipment, networks and software suppliers.
Cooperation at	The national CERT plays an important role in monitoring incidents at

international level	international level. Apparently, Finland does not participate in the CNSA.

General assessment
Finland can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. In the field of combating online malpractices, Finland has benefited from various positive elements. First, Finnish language raises the difficulty to successfully launch large online malpractice campaigns from abroad. Secondly, Finland has been able to develop and maintain rigorous attribution and control criteria for top level domains (TLD) assigning, which has made the .fi TLD a very risk free name space for Finnish web users. Thirdly, a good public awareness on information security has played a key role in avoiding large scale online security incidents related to identity theft and related crimes. Fourthly, Finnish online banks and e-commerce sites rely on a relatively difficult to "phish" online authentication method based on two factors. This has resulted into only modest criminal success by mass spam harvesting for online banking details. In many cases the efforts made by the national telecom regulator have played a key role and cooperation between the different competent authorities as well as service providers has been consensus driven. The government implemented various measures to strengthen cooperation with the service provider industry. Some challenges remain still. Some of the challenges are related to handling of problems related to identity theft and personal data theft resulting from targeted spam, spyware and other malicious software: as only few victims file criminal complaints, the national CERT and bureau of investigation cannot investigate most of the security incidents any further. Another challenge is that a number of "natural" safeguards such as the language barrier or the generalised use of two-factor authentication for online transactions, are not permanent safeguards and new development in spyware and malicious software technology can quickly deteriorate the Finnish information security environment. The core problems of identity theft and handling of personal data in various online stores should be addressed more strongly in order to encounter better the new development and speed of innovation in targeted spam and spyware tools and methods. Notwithstanding its active national, Finland does not demonstrate strong cooperation at international level.

9. France

Measures undertaken to combat malware

Measures undertaken by competent national authorities	*Administrative decisions* – The national DPA has considered that both Article L34-5 CP&CE and the Data Protection Act are applicable to these practices. They indeed make use of the contact details of the recipient, i.e. his/her personal data, in so far as the sender needed to process the MAC address and the Bluetooth identifier of the mobile phone, both part of the recipient's IP address. [34] Moreover, the reception is not anonymous: it provides the sender with information that enables him to identify the recipient. However, as shown by the debates around the nature of IP addresses and by the fact that some ruling has considered that IP addresses were not personal data, this position remains weak. The report to the French parliament on the implementation of the e-commerce act asks for the regulation of this phenomenon. *Judicial decisions* – The national DPA brought some cases to the public prosecutor in 2002. No information is available on the outcome thereof. In several cases, spam practices were sanctioned based on contract law. The first ruling in France punishing spamming practices has been rendered by the TGI of Paris on 15 January 2002. The spam sender had challenged his ISP before courts for unilateral breach of contract. The spam sender had had his internet access cut by the ISP after the latter had noticed a significant number of e-mails being sent by this user. The user was condemned by the Court to pay the amount of 1524 EUR for abusive procedure. A similar case was judged on the 28 February 2001 by the TGI of Rochefort-sur-Mer based on massive sending of advertising messages to a discussion forum. The spammer were sanctioned for breach of contract based on article 1135 of the Civil Code that states that 'Agreements are binding not only as to what is therein expressed, but also as to all the consequences which equity, usage or statute give to the obligation according to its nature.' Finally a third case could be mentioned, from 2004. The Tribunal of Commerce of Paris in a Judgment of 5 May 2004 condemned for breach

[34] The French DPA has considered that the concept of personal data, as understood under French law, was very broad and related to any natural person directly or indirectly identifiable, either through an identification number or other elements, including a vehicle plate number, a phone number or an IP address. CNIL, *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*, 2 August 2008, available online at : http://www.cnil.fr/index.php?id=2549&tx_ttnews[backPid]=2452&tx_ttnews[pointer]=2&tx_ttnews[tt_news]=332&cHash=7d73167c7a. For further analysis on the debate about personal data in France see COUDERT, Fanny, WERKERS Evi, Note d'observation sous l'arrêt C.J.C.E. (gr. ch.)du 29 janvier 2008: La protection des droits d'auteur face aux réseaux peer-to-peer : la levée du secret des communications est-elle justifiée ?, R.D.T.I. n°30/2008, p.76-85.

	of contractual terms an online service providers that was carrying out e-mailing campaigns advertising products via the ISP AOL and using a MSN Hotmail e-mail box. Both ISPs explicitly prohibit the use of services with commercial purposes. Laws relating to trademarks can also provide a valid ground for the prosecution of spam practices. In a summary judgment of 6 April 2004, the TGI of Paris ruled that the use of the e-mail address "package-internet@hotmail.com" could mislead users who could think that Microsoft had authorised this service. The Tribunal prohibited the company ALLIANCE BUREAUTIQUE SERVICE to use a European trademark of Hotmail from Microsoft. ALLIANCE BUREAUTIQUE SERVICE has also been sanctioned for its practices under the data protection law by a ruling from the Supreme Court of 14 March 2006.[35] The head of the company had been put before Courts for the collection of personal data (e-mail addresses) with purposes of direct marketing using robot software on Internet (websites, directories, forum) without informing and collecting the prior consent of the data subject. Article 226-18 punishes the collection of personal data by fraudulent, unfair and unlawful means. The judgment of the Supreme Court confirmed the Appeal Court ruling and stated that the collection of personal e-mail addresses from natural persons without the owner being aware of it is an unfair practice, as this does not allow for the user to exercise his right to object. The Supreme Court also considered that the identification and processing of e-mail addresses, even without their recording into a file, for purposes of sending e-mails to their owners, constitutes a collection of personal data. Even if the law has been modified with the e-commerce act, this ruling is still relevant for non-commercial operations of communications by e-mail in so far as it establishes that e-mails addresses and other personal data available on the Internet publicly accessible from the Internet are subject to the provisions of the data protection act. *Awareness measures* – The government's media development department has a website with general educational information about spam.

[35] Cour de Cassation, Chambre criminelle, 14 mars 2006. The text of the decision is available at (in French) : http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-criminelle-14-mars-2006.html

	In addition, public and private parties jointly set up the organisation and website signal-spam.fr, which provides information on spam prevention and protection. Also, information on spam, applicable legislation, complaint channels and models of complaint letters can be found on the website of the national DPA. Finally, the associations of telecom and mobile operators launched a website specifically dedicated to mobile spam. It provides information on what is mobile spam and what the user can do about it. *Complaint channels* – Signal-spam.fr is the single point of contact for spam reporting. It offers the possibility to use a plug-in that will automatically inform the organisation about spam received by the user and transfer such information to competent authorities if relevant. Before that, in 2002, the national DPA had set up e-mail inbox for the reporting of spam messages but this project was quickly abandoned due to insufficient resources.
Measures undertaken by the service provider industry	Several ISPs offer their clients spam filters, use black lists, etc. ISPs have cut off the internet connection of users identified as spam senders on basis of a breach of contractual obligations. Several judicial decisions have confirmed the lawfulness of such practices. Since 15 November 2008, a specific platform dedicated to mobile spam has been implemented by the government and mobile operators. From the very launch of the platform, more than 10.000 reporting messages had been received. The platform will make an inventory of the messages received, the spam senders' numbers and identify them, block the spam received by users and further prosecute the spammers whenever possible. To that effect, when the mobile phone user receives a spam SMS, he can send a copy to the number 33700. He will then receive an SMS back asking him to enter the phone number of the spam sender. This operation costs the price of 2 SMS (1 for the copy of spam and one to communicate the number of the spammer). The three main mobile operators (ORANGE, SFR, BOUYGUES TELECOM) via their Association SMS+, together with the FFT and AFOM have launched a website dedicated to mobile spam: http://www.33700-spam-sms.fr/#. It provides information on what is spam and what the users can do about it.

Measures undertaken by the vendor industry	The French direct marketing association adopted a code of conduct with rules on the collection and use of electronic contact details for the purpose of direct prospection.
Other measures	There is also a personal website which provides up-to-date information on all kinds of online malware. This site is referenced on the website of the internet rights' forum.

Cooperation activities to combat malware	
Cooperation between governmental bodies	In October 2007, the national DPA and Signal Spam signed a partnership agreement to coordinate their efforts in the fight against spam. The agreement foresees: - the regular information of the national DPA of statistics about spam reporting received by Signal Spam - the possibility for Signal Spam to bring users' complaints against an identified spammer before the national DPA. The national DPA receives on a monthly basis a list of companies reported as spamming. - the carrying out of informative actions or common recommendations in France and at international level - the designation of specific correspondents within both organizations and the commitment to regular meetings. On the basis of this co-operation, the national DPA has started a series of controls in companies reported as spamming. The controls bear on the methods of collection of e-mails (origin of the data and of databases used to send the e-mails), the conformity of the consent of users with legal requirements and the respect of the right to object. Moreover, some companies have already been called to comply with legal requirements and have been placed 'under surveillance' by the national DPA which is doing a close follow-up of their marketing activities.
Cooperation between government and industry	The co-operation between private and public stakeholders in the fight against spam and coordination of their actions at national and international level is promoted by the action group for the fight against spam, created on 16 January 2004 by the French Government and managed by the media development department. It has developed several sector committees and lead to the creation of the SIGNAL SPAM association in 2005, a French resource center and complaint channel for spam, which gathers the main French public and private entities

	concerned by the fight against spam. Also, within the French telecom association, a specific commission on security matters deals with spam related issues and works in direct relation with competent authorities. Also, on 27 November 2008, the French direct marketing association and Signal Spam have signed a partnership agreement. This has been followed by the signing of other partnership agreements with 22 of the members of the direct marketing association. They all commit to implement a 'feedback loop' ('*boucle de rétroaction'*) initiated and developed by Signal Spam. This 'boucle de rétroaction' intends to facilitate Internet users to exercise their right to object. When a user notifies using the Signal Spam button spam from this partner, Signal Spam further transfers this notification to the e-mail sender (the partner) which will contact the controller to delete this user within the database. Finally, on 29 November 2007, Microsoft and Signal Spam signed a partnership agreement to ensure and promote users' trust towards Internet. According to this agreement, the e-mails (overtly) issued from or to Microsoft, or using without authorisation the trade mark and services of Microsoft that are reported to Signal Spam are transferred to the company. No personal data from the user is transferred to Microsoft in the first place but Microsoft, via Signal Spam, could contact the user at a further stage for the judicial prosecution against spammers.
Cooperation at international level	On 5 May 2006, France and Japan signed a joint statement within the framework of a coordinated international action in order to fight spam. Both countries especially consider to exchange information and good practices regarding the field of anti-spam policies and strategies. France also participates in the CNSA.

General assessment
France can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. France has adapted its legislative framework and has progressively built an institutional framework

to fight against spam. By way of example, the national DPA obtained special powers, e.g. to impose financial sanctions, carry out on-site inspections or issue public warnings. It can also order controllers to cease the sending of spam and if necessary impose a financial penalty or an injunction to stop the sending of spam. The French government strongly promotes cooperation with the industry. At the international level, France participates in the CNSA and concluded a bilateral agreement to fight spam with Japan.

Nevertheless, a series of issues remain.

First, some limits of the current legislative framework are identified:

- in the *narrow definition of spam*. The French DPA had to deal with two specific cases, the use of direct marketing databases for political campaigns and the regulation of B2B marketing. Both have required specific solutions and have shown the limits of the actual wording of the Law.

    - ***Unsollicited emails with a political nature**:* Messages sent by political parties, charities or other organizations, solely expressing views, thoughts and ideas without a direct commercial purpose are thus excluded from the scope of Article L.34-5 CP&CE (that transposes article 13 of the E-Privacy Directive). Nevertheless, these activities are still covered by the general regime of the Data Protection Act. In that case, in the moment of the collection of the data, individuals are only asked whether they agree to the use of their contact details for marketing purposes without any further specification of the products or services that will be further promoted. Problems have aroused when a political party have subcontracted the services of a specialized company to promote his ideas. In these cases, the objection or lack of objection of the data subject to receiving such information may indicate his political believes. The question consisted in defining whether the general rules applying to direct marketing should apply in the same way when such databases were used to send messages with a political nature. The French DPA considered that attending to the sensitiveness of the situation, stricter rules should be followed: 1) in the moment of the collection, the data subject should be informed of the fact that his/her address can be used for marketing with political purposes; 2) in the moment of the reception of the message, (s)he should be informed of the origin of the database from which the data are obtained of the fact that the political party originating the communication does not have the email addresses at its disposal (when the marketing campaign is sub-contracted).

      The report to the French Parliament suggests to engaging into a reflexion in order to consolidate the French DPA's position. One of the reporters advocates for broadening the definition of spam to any automatic unsolicited communication.

    - ***B2B spam**:* The wording of article L.34-5 CP&CE refers to the use of the contact details of a natural person for direct marketing purposes. In case of B2B marketing, only email addresses such as sav@entreprise.com or contact@entreprise.com fall outside the scope of application of such article. The French DPA has thus first considered that prior consent was required in any other case.

However, the French DPA has reviewed its position after engaging into discussions with direct marketing stakeholders. It now considers that the spirit of the law is to protect consumers' privacy and not to hamper commercial communications between professionals. It follows that direct marketing directed to professionals will not fall under the provisions of article L.34-5 CP&CE in case the content of the message is related to the function the recipient is in charge in the company (e.g. promoting software to the person in charge of the computer department). Such messages will not require his/her prior consent, provided that (s)he has been able, in the moment of the collection of his/her data, to object to any commercial use of their contact details.

The Report to the French Parliament advocates for consolidating this interpretation of the French DPA and distinguishing between B2C and B2B direct marketing.

the regulation of *'blue spam'*, i.e. advertising via Bluetooth. Taking into account that these practices are called to develop, the report to the French parliament on the implementation of the e-commerce act asks for the regulation of this phenomenon.

Secondly, the means put in place to fight spam remain insufficient. The report to the parliament identifies the need for a stronger institutionalisation of the fight against spam granted with more significant means. In practice, the fight against spam is delegated to an association SIGNAL-SPAM which counts of only one employee and to the national DPA which has limited resources and remains a relatively small structure to be able to deal with all the problems.

Finally, the parliamentary report advocates for the need to enable the right for network operators to sue spammers. This possibility is nowadays only given to users. Operators are identified as also being victims of such practices and they moreover have more economic resources and an international dimension that allow them to prosecute spammer more efficiently.

10. Germany

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No information available. *Judicial decisions* – The German Federal Court of Justice (Bundesgerichtshof – abbr.: BGH) ruled on 11.03.2004 (file no. I ZR 81/01) on the illegality of Spam. With BGH I ZR 197/05 of 17.07.2008 the Federal Court of Justice ruled that the mere provision of an email-address on a website does not represent an invitation to send e-mails advertising products or services. There are numerous cease and desists orders of district courts and

	higher courts, e.g. as a result of law suits filed by the German Anti-Spam-Alliance (consisting of Bundesnetzagentur - BNetzA, Bundesverband Verbraucherzentralen - vzbv, Wettbewerbszentrale – WBZ, and eco – the German ISPA), threatening the defendant with administrative fines not exceeding 250.000 EUR alternatively arrest for contempt not exceeding 6 months (e.g. Kammergericht Berlin, 9 U 52/06, 26.01.2007: Oberlandesgericht Düsseldorf, 15 U 45/06, 24.05.2006; Amtsgericht Krefeld, 2 C 187/06). The convict usually carries the court costs and legal fees. Court orders actually *imposing* these fines are not publicized, hence cannot be referred to other than with file number (e.g. LG Bonn, LG Lüneburg 9 O 220/08). In cases of the Anti-Spam-Alliance, defendantregularly are convicted to pay an administrative fine of 2.500 EUR for each violation of the cease and desist order. *Awareness measures* – The German ISPA has two informative websites for end-users, on which they provide general information on how to combat spam, awareness messages about online risks (www.internet-beschwerdestelle.de and www.eco.de/initiativen/anti-spam.htm). They also provide an anti-spam guide for end-users, a detailed anti-spam brochure, guidelines for direct marketers and legal recommendations for ISPs as regards e-mail traffic filtering. In addition to this, klicksafe.de informs and educates parents, teachers and children on questions of safer internet use. *Complaint channels* – The German complaint hotline initiated by Internet industry stakeholders (°1998) and operated by the German ISPA works within the consortium Internet-Beschwerdestelle (www.internet-beschwerdestelle.de) and is co-founder and driving force of the German anti-spam-alliance (see below). Finally, the national telecom authority can be contacted by e-mail for complaints about unsolicited calls, SMS or spam e-mails containing telephone numbers.
Measures undertaken by the service provider industry	The ISP industry actively takes the lead role in the fight against spam through self-regulation. It organises a yearly anti spam summit since 2003. A whitepaper with anti-spam guidelines for ISPs was produced after the first summit. Several ISP's offer their clients spam filters, use black lists, etc. They also have an anti-spam policy in their terms and conditions. In 2004-2005, the German ISPA also set up a central German White list

	project in cooperation with the German Direct Marketing Association. The reason for this is that mass mailers complain that a substantial portion of solicited mailings – such as newsletters – are no longer reaching their destinations because of mail filtering. The original way of working, whereby mass mailers had to negotiate with individual ISPs, proved not to be workable in practice. The German White list projects centralises inclusion of mass mailers on a white list. It works with standardised procedures which ensure a consistent, high level of quality. It also has an efficient complaint management system. A centralised white list not only establishes a spam "fence", but also an interface between mass mailers and ISPs which aims at improving the quality of e-mail as a medium and – above all – ensures that genuinely desired mailings (on both parts) from serious originators reach their destination without the mailer needing to worry about their mail being black listed. This approach conserves resources on the part of both ISPs and mass mailers. The service is free for the ISPs, while the mass mailers pay both a registration fee and regular subscriptions. The German association of banks is active with regard to anti-phishing activities.
Measures undertaken by the vendor industry	No information available. The biggest German anti-spam software provider company is called eleven (www.expurgate.de).

Cooperation activities to combat malware	
Cooperation between governmental bodies	The federation of German consumer organisations and the agency against unfair competition periodically exchange information on current cases and share a list with previous cases to avoid redundancies. They also meet on a regular basis to discuss cases and strategy of the anti-spam alliance with ISPA (see below).
Cooperation between government and industry	The ministry of economics, the German network regulator and the German ISPA participate together in CNSA meetings. The ministry of consumer protection, the agency against unfair competition and the German ISPA have initiated the anti-spam alliance between them and the agency against unfair competition. The organisational responsibilities among the partners of the alliance have been agreed in a memorandum of understanding signed in 2005. It was

	later joined by the German regulatory authority. It has brought more than 120 spam cases to court. The federal information security office and the German ISPA organise workshops to set up a common anti-botnet strategy. Furthermore, the German ISPA is participating in the federal and state police project group on information- and communication-technology related crimes.
Cooperation at international level	Germany participates in the CNSA, Operation Spam Zombies and in the SpotSpam project. The German ISPA also participates in the LAP as industry supporter and in the APWG.

General assessment
Germany can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. Germany is one of the forerunners in combating online malpractices in comparison to some other Member States. The internet industry invests considerable financial resources and efforts are being made to coordinate actions efficiently. International cooperation, not only in the fight against illegal and harmful material on the Internet but also in countering spam, is regarded as essential by industry stakeholders. Congresses like the annual Anti-Spam-Summit organised by the German ISPA are a forum to strengthen and enhance existing cooperation and to establish new ones. This and other actions as a industry self-regulation approach in the fight against spam are supported by the German government. The industry has been very successful in countering advertising campaigns with traceable origin. Nevertheless, even in a forerunning Member State like Germany, competent authorities are said to lack financial and human resources to consider all spam complaints. As a consequence, only severe and constant offences are processed.

11. Greece

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The Greek DPA has issued some decisions on the processing of personal data for marketing purposes. It also dealt with a case of SMS spam and imposed fines to the data controller a) of 20.000 EUR for sending SMS spam to random mobile numbers without prior consent and b) 10.000 EUR for not giving the recipients the

	opportunity to object. *Judicial decisions* – In 2002, the Athens first instance civil court imposed a fine of 5.869 EUR on a company that was repeatedly sending marketing material (in paper) to a citizen who had subscribed to the Article 13 list (Robinson's list). In the same year, the same court held that the collection of personal data of other users is illegal in the context of sending of a web newspaper to user e-mails addresses. The case did not end in a ruling for damages, because the application was rejected. *Awareness measures* – The website of the national DPA contains spam information for citizens, including advice on how to protect themselves against spam and on how to file a complaint in case they are victims of spamming. Currently the Greek DPA is considering the adoption of guidelines/recommendations for the ISPs in four main directions: a) general policy and customer awareness measures, b) measures against outgoing spam, c) measures against ingoing spam and d) cooperation measures among ISPs. *Complaint channels* – Complaints can be made through the website of the national DPA (as well as by post, e-mail or fax).
Measures undertaken by the service provider industry	The service providers have a code of conduct for online advertising. The mobile provider Vodafone published a mobile telephony guide for parents with a part on spam, in which customers are urged to contact the service centre to allow them to spot the spammer. Several service providers have awareness information on their website and offer spam filters, use black lists, etc. One service provider actually offers a personalised anti-spamming service, which can be activated/deactivated according to the wishes of the service and offers the creation of personal white and black lists. The Hellenic Bank Association issued a press release on 1 November 2005, informing and warning bank clients about the risks of internet banking, in particular phishing, of which many clients had become victim.
Measures undertaken by the vendor industry	The vendor industry is actively involved in the national safer internet project.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The various competent authorities have clearly defined roles and according to their establishing laws and statutes there is an obligation to cooperate among each others. The authorities also transfer a file to the competent authority, if they see a reason to intervene. There is close cooperation with them at general level, without the creation of special working groups. Recently, the creation of a working group was proposed that would aim at the clarification of the responsibilities between the various public competent authorities.
Cooperation between government and industry	The Hellenic DPA created a working group comprised of members of the Hellenic DPA and representatives of the main private and public ISPs, which discussed the adoption of a Code of Conduct on fighting spam. The Code has still not been adopted, due to lack of consensus among the ISPs on the implementation of technical measures against spam.
Cooperation at international level	The Greek DPA participates in the CNSA, operation spam zombies and the OECD anti-spam working group.

General assessment
Greece can be considered as a Member State with comprehensive information on actions and measures taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. However, the fact that responsibilities are split between various competent authorities on very specific issues appears to have created difficulties in the uniform reaction to online malpractices. By way of example, the national regulatory authority is not responsible for spam, although part of its competence is the regulation of consumer protection issues in the electronic communications sector. Greece does however show great dedication to protecting online privacy and safety, in particular confidentiality of communications, dialers, value added services etc. Pursuant to a large wiretapping scandal, Greece strengthened its regulatory framework on securing telephone communications' secrecy and security with a law adopted in 2008. Examples of both administrative and judicial sanctions for e-mail spam and/or mobile spam exist. Competent authorities generally work closely together and the DPA strives for close cooperation with the industry. At the international level, Greece participates in various initiatives: the CNSA, Operation Spam Zombies and the OECD anti-spam working group.

12. Hungary

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – In 2007, a total sum of about 6.400 EUR was imposed in fines. In 2008, this sum was ten times higher, because the fine, which can be imposed, was bigger. The maximal fine was about 2.000 EUR in 2008. In 2008, one spammer was fined seven times with a total sum of fines amounting to 1.6 million HUF (around 5.333 EUR at the time of redaction of this report) for sending spam to more than 10.000 e-mail addresses each time. In addition, the fines were treated as marketing cost.*Judicial decisions* – No information available. *Awareness measures* – Several websites exist which provide spam related information. One of them is the website of the telecom regulator. Another one is a website developed by the Forum of Friendly Internet with the support of the ministry of telecom and the national telecom authority. On this website, parents and teachers can find general information on combating spam and awareness messages about online risks. There is also the crime prevention website of the Hungarian police with advice on safe use of the internet. *Complaint channels* – Complaints can be sent by e-mail to the telecom regulator. Also, complaints could be addressed to the consumer authority for misleading content of spam messages or to the competition authority for infringements of applicable legislation in this field. Complaints about malware can be sent to the Hungarian police via its website. There is also a private Hungarian website with information on spam and complaint channels.
Measures undertaken by the service provider industry	A comprehensive summary of tasks against malicious actions, including spam, can be found in the Acceptable Use Policy (AUP) of the Council of Hungarian Internet Providers, which is compulsory for all members. Most ISPs take technical measures against malicious actions via filtering of spam, blocking of malware and limiting traffic. Several ISPs also have an explicit spam policy in their terms and conditions.
Measures undertaken by	Many IT vendors sponsor the yearly day of IT security.

the vendor industry	One of the IT security vendors carried out a survey with Hungarian companies and institutions about their information security preparedness.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The telecom and competition authorities entered into an agreement for the protection of the electronic communications market and compliance with its applicable legislation. The competition, consumer protection and financial supervision authorities cooperate against unfair commercial practices against consumers, in particular through information exchange and other related tasks. The national CERT signed cooperation agreements with the national telecom and financial regulator and with most major Hungarian players.
Cooperation between government and industry	The telecom regulator provides an online information channel for ISPs on their legal duties. The Hungarian police has separate cooperation agreements with the largest service providers. The experts in this field have good personal and informal contacts with the representatives of the network and service providers.
Cooperation at international level	Hungary participates in the CNSA, in operation Spam Zombies, in the LAP and the OECD. The Hungarian national CERT also participates in the international watch and warning network as part of the international cyber security framework established for the exchange of information and cases.

General assessment
Hungary can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. Whereas Hungary has the legislative instruments in place, it appears that the role of IT security may be undervalued and that the government regards IT security threats not as significantly dangerous for the society or for the economy. Due to the state reform and the changes in the economy there is

not yet a responsible national organisation for the awareness raising or an organisation authorised to coordinate the fight against spam, spyware and malware. Also, it appears that the national telecom regulator does not have dedicated resources to fight spam. No information is available that indicates concrete cooperation between governmental bodies in the field of spam or spyware. Existing cooperation schemes relate to the protection of the electronic communications market and the protection of consumers against unfair commercial practices. On the other hand, the Hungarian police would have separate cooperation agreements with the largest service providers. On the international level, Hungary participates in several cooperation schemes.

13. Ireland

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – In the last 2 years, the national DPA has received a total of 104 e-mail spam complaints, 581 SMS spam complaints and 1 adware complaint (currently under investigation). The national DPA has had two successful prosecutions for the sending of unsolicited text messages. In September 2005, the company Fours a Fortune was fined €1500 for sending 5 text messages. In November 2008, the company Clarion Marketing was fined €2000 for sending 6 text messages. *Judicial decisions* – The DPA currently has over 300 summonses before the District Courts in relation to 5 separate companies. These summonses are all related to offences under Section 13 (1) (b) of SI 535. In January 2009 the premium rate mobile text provider Realm Communications unsuccessfully challenged the procedures of the DPA in the High Court in relation to the issuing of 60 District Court summonses for breach of the prohibition on sending unsolicited text messages. As a result, these prosecutions are expected to proceed. The same company has commenced a legal challenge against the decision of the self-regulating body of the communications industry that a 12-month suspension from sending premium rate text messages be imposed on it for breaches of its code of practice. In late 2008 the case was transferred to the Commercial Court list for hearing in early 2009. *Awareness measures* – The national DPA has published substantial guidance material, both on its website and in its Annual Reports in relation to raising awareness in the area of online malpractices. The Department of Communications each year runs a computer security

	awareness campaign, "Make IT Secure" which deals with these issues. *Complaint channels* – The national DPA offers an online complaints procedure and also receives written complaints. In addition, the national ISPA offers since 1999 a hotline where the public can report material suspected to be illegal, including spam containing contain illegal content (other spam is dealt with by the DPA). The self-regulating body of the communications industry offers a complaints service which can be activated by telephone or in writing.
Measures undertaken by the service provider industry	The Irish Cellular Industry Association (ICIA) has a code of practice which covers spam. ICIA is affiliated to the Telecommunications and Internet Federation, which is part of ICT Ireland, the voice of technology with the Irish Business and Employers Confederation (IBEC). ISPA members also adhere to a code of practice, which states that members will follow best industry practices in using anti-spam software. The self-regulating body of the communications industry also has a code of practice addressing spam. One ISP generates statistics on spam.
Measures undertaken by the vendor industry	All the major software providers provide advice on protection against online fraud, spyware, viruses, etc. There were reports in the media in early 2008 of a survey by Microsoft's Malware Protection Centre in Dublin concerning the extent of cybercrime in Ireland. However, such survey appears not to have been made public.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The national DPA interacts with the Department of Communications in the drafting of any legislation covering the regulation of spam, spyware etc. It provides views on how the area should be regulated and how this would compliment other legislation in regard to data protection. The national DPA also has a close working relationship with the telecom regulator and the self-regulating body of the communications industry. This relationship allows it to discuss issues that arise and to agree common strategies for dealing with those matters.
Cooperation between	The national DPA has met in the past with national ISPA to discuss

government and industry	issues in relation to spam. It also meets on a regular basis with the Mobile Network Operators to discuss a broad range of issues including issues in relation to spam text. In particular, ISPs may have to disclose identifying information in relation to those involved in sending spam etc. to the DPA and other enforcement bodies.
Cooperation at international level	The national DPA participates in EU Data Protection working groups, including an IT working group which deals with data protection issues. These working groups are comprised of members from each of the EU Data Protection agencies. The DPA also participated in the International Spam Enforcement Cooperation workshop, hosted by the UK Office of Fair Trading and the US Federal Trade Commission. It has also contributed to the OECD Directorate for Science, Technology & Industry Task Force on SPAM. Ireland also participates in the CNSA and the LAP.

General assessment
Ireland can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. In Ireland, the necessary legislation is in place and penalties for the sending of unsolicited communications have recently been significantly increased. There have been successful prosecutions in two cases relating to spam to date and a large number of prosecutions are pending. The national DPA cooperates with various governmental bodies, with the national ISPA and is involved in various international initiatives. One difficulty pertaining to this area is the range of different regulatory bodies involved, one of which does not at present operate on a statutory basis, although this is set to change in the near future. The number of regulatory bodies involved may cause confusion among the general public. With the convergence of technologies e.g. the availability of e-mail via mobile phone, confusion may also arise on the part of customers as to which provider is responsible. The national ISPA identified difficulties in prosecuting those responsible for spam etc. where they operate across jurisdictions.

14. Italy

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The national DPA issued an order to clarify the content of legislative provisions in the area of spam. It also issued a number of decisions in the field of spamming, especially in the period 2002-2003, ordering to stop the sending of spam via e-mail/SMS without consent, to stop the use of personal data and/or to provide the claimant with information about the processing of his personal data. In a case where the order was not followed, the DPA denounced the company in question to the competent prosecutor. In 2008, the DPA imposed a fine of 570.000 EUR on an SMS spammer. *Judicial decisions* – In 2004, the Naples Court of peace sentenced a spammer to a fine of 1,000 EUR plus 750 euro (refund of costs of the proceedings). Vierika' is the first case in Italy regarding the diffusion of malware and spyware. The defendant sent 900 users an e-mail with a software attached. This software was a spyware and malware, aimed to steal information from the attacked computers and to infect the system. The judge of first instance (Court of Bologna, First Chamber, decision of 21 July 2005) sentenced the defendant to 6 months of imprisonment, commuted to a fine of 6,840 euro, for violation of Sections 615-ter and 615-quinquies of the Criminal Code. The Court of Appeal, then, modified the decision and sentenced the defendant to 2 months of imprisonment and the payment of 2,628 euro as fine. The imprisonment has been commuted to a fine, so that the defendant has been finally sentenced to pay 4,280 euro. It is important to point out, then, that the Court of Appeal states that the diffusion of a malware is always a crime (to be more precise, the crime pursuant to Section 615-ter of the Criminal Code). *Awareness measures* – The Police of Communications set up a website where citizens and enterprises can get information about illegal activities that take place on the Internet (including spam, malware and spyware). *Complaint channels* – Via the website of the Police of Communications, victims can report cybercrimes. It is not possible to file an online complaint with the national DPA. This must be done via regular mail. The completion authority offers a toll free phone number for the

	reporting of aggressive commercial practices, including spam.
Measures undertaken by the service provider industry	Several ISPs offer to their clients spam filters or other security tools. Telecom Italia, for instance, offers a 'total security' service to its clients against payment of a small fee of around 4 euro/month. This offers extensive protection against spam, viruses, spywares, etc.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	In 2003, a permanent observatory group for security and protection of networks and communications was created by the Minister of Communications, the Minister of Justice and the Minister for Internal Affairs. It has generic competences to verify the state of the art regarding network security, including the risks linked to malware and spyware attacks. Up to now the group has performed mainly research activities, as it does not have any real power to enforce legal bans. The national DPA and the police of communications collaborate on a regular basis to sop and prevent criminal activities involving spam and spyware.
Cooperation between government and industry	The working group on privacy, phone interceptions and spam of the national ISPA has the duty to collaborate with the national DPA and to manage the relationships between the two entities.
Cooperation at international level	The national DPA participates in the CNSA on behalf of Italy.

General assessment
Italy can be considered as a Member State where substantial information can be found on the actions and measures that can be taken by public authorities and industry actors in relation to the combat against online malpractices such as spam, spyware or malicious software. As an overall assessment, it is possible to say that Italy is in a good position in combating online malpractices. There have been successful prosecutions in spam related cases and the national DPA recently imposed relatively high fines. Also the DPA cooperates with the police and the national ISPA and participates in the CNSA at international level . Several ISPs offer to their clients spam filters or

other security tools. Therefore, a lot of work has been done so far. However, what seems to be compelling is the rationalisation and simplification of the existing legislative sources (especially in the criminal field: in other words, there are several laws that set criminal sanctions but these rules seem to be often not fully consistent, and therefore there are problems when they have to be applied to real cases) and of the enforcement powers of the relevant authorities. Sometimes, in fact, it is not very clear who is competent for what, and some clarifications by the lawmaker would undoubtedly render the work performed by the Privacy Authority and the Competition Authority more effective.

15. Latvia

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The national DPA imposed fines in two cases for a total amount of EUR 4.300. *Judicial decisions* – No court proceedings are known. *Awareness measures* – There are no warning actions carried out by Latvian authorities. *Complaint channels* – End-users can submit spam complaints to the consumer protection center and the national DPA. The site netsafe.lv is partially state funded and aims at increasing the safety of children in the internet. It also allows for the possibility to lodge complaints. It is not specifically dedicated to spam.
Measures undertaken by the service provider industry	Several ISPs offer their clients (web-based) spam filters, use blacklists, etc. Bank inform and warn clients via their website about the risks of internet banking, in particular phishing, of which many clients had become victim.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The national DPA, the consumer rights protection centre and the public utilities commission cooperate for the protection of personal data in electronic communications services, including the fight against spam.

Cooperation between government and industry	No information available.
Cooperation at international level	Latvia participates in the CNSA and the LAP.

General assessment
Latvia can be considered as a Member State with little information on the actions and measures related to the combat against online malpractices such as spam, spyware or malicious software. Even via internet, little information is available. In Latvia, it appears that governmental institutions and other organisations only begin to combat online malpractices at the time of this report. There is indication at this point of substantial efforts to combat online malpractices. Nevertheless, the national DPA carried out some investigations regarding spam activities and imposed a total amount of 4.300 EUR in fines in two cases. Also, Latvia cooperates internationally in the CNSA and the LAP. Several ISPs offer their clients (web-based) spam filters, use blacklists, etc.

16. Lithuania

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – In 2008, the national DPA investigated a total of 9 complaints regarding unsolicited direct marketing using spam. Administrative sanctions were applied in 3 cases, 2 of them were confirmed by the administrative court and 1 case is still pending. In 2008, the consumer rights protection authority registered a total of 11 complaints related to unlawful marketing using spam, 6 of them were forwarded for further investigation. *Judicial decisions* – Apparently there were 2 cases in the criminal court but no detailed information is available. *Awareness measures* – The websites of the telecom regulator (on behalf of the national CERT) and the DPA provide specific information on spam, spyware, malicious software and actions to prevent them. The national CERT publishes quarterly reports on security incidents including spam, spyware and malicious software. *Complaint channels* – Complaints may be filed through a specific

	complaints website of the telecom regulator.
Measures undertaken by the service provider industry	No information available.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The national telecom regulator and DPA cooperate for the protection of personal data in electronic communications services including the fight against spam.
Cooperation between government and industry	No information available.
Cooperation at international level	The national DPA participates in the CNSA on behalf of Lithuania.

General assessment

Lithuania can be considered as a Member State with little information on the actions and measures related to the combat against online malpractices such as spam, spyware or malicious software. Some moderate efforts in this respect seem to be taken in the recent past. The national DPA carried out some spam related investigations and applied sanctions in a few cases. Another two spam related cases are said to be dealt with by criminal courts. Also, the national DPA cooperates with the telecom regulator in the fight against spam and participates in the CNSA. On the other hand, no information is available on measures taken by the service provider industry.

In short, the major problems encountered in Lithuania in comparison to more active Member States appear to be the following:

- absence of a sole central government institution with adequate legal powers and financial resources for combating incidents related to spam, spyware and malicious software as well as the discretion to impose administrative sanctions;
- little degree of co-operation between competent government authorities and e-communications network/service providers as well as lack of joint-coordinated actions;
- absence of government initiatives in order to raise public awareness regarding the risks of

spyware and malicious software;

- a small number of public initiatives of communications network and service providers as well as software producers in addressing and combating spam, spyware and malicious software.

In the third quarter of 2008, the national CERT investigated a total of 105 security infringement cases including 53 spam, 2 phishing and 11 malicious software incidents.

The Lithuanian Government has approved the framework for the Law on the Security of Electronic Networks and Information. The framework lays down legal principles which should be later incorporated in the Law on the Security of Electronic Networks and Information. It is planned to issue the law by 2010 at the latest.

17. Luxembourg

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No information available. *Judicial decisions* – No malware related decisions. Nevertheless, worth mentioning may be the following computer crime related decisions. 1) An employee of the Luxembourg over-indebtedness service was sentenced to 10-month imprisonment in 2005 for entering the service's database and trying to sell the personal data of 3,000 Luxembourg citizens to a journalist. 2) A hacker was fined 1.240 EUR in 2001. 3) An employee of a Luxembourg company was fined 1.240 EUR and sentenced to 18-month imprisonment for falsification of computer data so as to pocket the money deposited by clients (namely 80.665 EUR). He also has been sentenced to pay the bank 49.578 EUR in damages. *Awareness measures* – In terms of prevention, the Ministry of Economy and Foreign Trade has initiated with CASES an ambitious project that strengthens awareness and contains a lot of theoretical and practical information on on-line malpractices and risks related to Internet (such as spam, spyware, virus, worms, Trojan horses, loss of data, phishing, etc.). Through its website, CASES provides highly-comprehensive information on the theoretical risks relating to the computer systems and information networks and makes children, citizens, SMEs and central government aware that the careless handling of personal data on social networking tools, home pages and blogs leads to spam. It also provides information on practical tools against computing risks (such as antivirus and antispyware software, firewalls, cryptography solutions, intrusion detection system, etc.), as well as instructions for use of

	computing technologies in order to ensure the protection of data. CASES is not entitled to investigate cybercrime but has been recognised good practice by ENISA. *Complaint channels* – No specific spam related complaint channels are provided. End-users can file a criminal complaint through an online complaint form on the website of the Luxembourg police force.
Measures undertaken by the service provider industry	Several ISPs offer their clients spam filters, use blacklists, etc. The ISP Netline broadcasts on its website information on how to combat spam and viruses. Most ISPs prohibit spam in their T&C.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The police cooperates with CASES for computer-related crime prevention campaigns. However, there is no specific cooperation as regards the prosecution of computer-related crimes. CASES also cooperates from time to time with the national DPA by sharing information on internet related risks and with local governments for awareness campaigns.
Cooperation between government and industry	Cases cooperates with several ISPs in order to raise awareness on risks like phishing, social networks or cyber-bullying.
Cooperation at international level	Luxembourg does not participate in the CNSA, the LAP or operation spam zombies. It has however participated in the anti-spam working group of the OECD.

General assessment
Luxembourg can be considered as a Member State where comprehensive information can be found on actions and measures related to the public awareness actions on online malpractice such as spam, spyware and malicious software. The government initiated an ambitious information and awareness raising project in cooperation with the service provider industry. Several ISPs offer their clients (web-based) spam filters, use blacklists, etc. Also, no information is available that would indicate international cooperation at the moment of this Study. However, on the basis of the available information, the actual repression of spam and spyware

seems to be quite low at this stage. One reason of this absence of repression may be that citizens are now so used to receiving spam that they do not complain about them with criminal authorities. In this context, it would be useful to offer to end-users an easy channel enabling them to inform the competent authorities of the spam they receive, such as a dedicated e-mail address or a website for instance. Also, no specific authority is dedicated to the prosecution of online threats whereas the police and public prosecutor generally do not act at their own initiative. Worth mentioning is also that since 2008, the ministry of economy and foreign trade can request the district court for an injunction order against unsolicited commercial communication.

On the other hand, Luxembourg has made many efforts in the area of network resilience, but also in the area of information security in general. Especially some governmental initiatives have achieved to tie some very close links to specialised governmental bodies but also private companies. This well coordinated approach creates many synergies and allows large scale campaigns involving for instance all ISPs or mobile phone providers. IT security awareness raising has been made an obligatory topic in school. Cyber bullying is addressed together by schools, ISP, mobile phone providers, Police Force and Public Prosecutors. Public administrations are aware of the needs to invest in IT security.

18. Malta

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No information available. *Judicial decisions* – No cases of unsolicited communication have ever been prosecuted in court. *Awareness measures* – Awareness measures relate more to general data protection and internet security. No specific spam or malware related awareness measures are reported. *Complaint channels* – The national DPA provides an online complaint form for unsolicited commercial communication.
Measures undertaken by the service provider industry	In June 2008 the two major mobile operators in Malta – GO and Vodafone – signed a Code of Conduct by which they agree to use common measures to combat illegal use of their networks in order to protect users, and particularly minors, from unsuitable content and unsolicited communication. The major ISPs in Malta provide extensive information on their websites to help users fight spam and other security issues. This includes detailed help pages, FAQs, recommendations on installing anti-virus software,

	examples of 'phishing' e-mails and online channels for reporting incidents and queries directly to their customer care representatives. The major ISPs in Malta also follow best practices and use industry standard infrastructure and software to reduce the impact of spam upon their users including automated spam filtering and blacklisting. Most ISPs have explicit clauses on their websites in their "Terms & Conditions" and "Privacy Policy" sections stating that spam and unsolicited communication is expressly forbidden and that malicious use of the services being provided may result in termination of service and legal prosecution. Local banks provide extensive information, warning adverts, and regular reminders to users of their Internet banking systems to be vigilant against giving out personal information to non-trusted sources.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information is available that would indicate specific spam related cooperation in Malta. The ministry for communication established the national information society advisory council, representing all stakeholders, including the private sector. In 2006, the government established the national e-security working group, representing key stakeholders in matters of e-security.
Cooperation between government and industry	The national DPA apparently maintains informal relations with ISPs and mobile network operators to ensure data protection policies and new legislation is implemented and adhered to. When the data retention directive came into effect in 2008, discussions where held between service providers to create a memorandum of understanding between the providers and the authorities, including the DPA.
Cooperation at international level	The national DPA participates in the CNSA on behalf of Malta.

General assessment

Malta can be considered as a Member State with limited information on actions and measures related to the public awareness actions on online malpractice such as spam, spyware and malicious software.

There are no central, formal and statistical sources of information about the issues of online security, spam, spyware and related matters. Available information is scattered amongst different organisations, websites and individuals. Detailed and statistical information about online malpractices is limited in Malta.

The competent authorities have only relatively recently began moving towards formulating policies that deal specifically with issues of spam, spyware, malware and other online malpractices. However the various authorities and organisations competent for online security have a keen sense of the importance of the issue. This is reflected in the publication of consumer guidelines and working documents, co-operation with foreign bodies, and complaint channels on the various websites.

Basic legislation is in place but investments of financial and human resources by the government to raise awareness, prevent or investigate incidents are limited. Positive action is being taken and online safety is becoming more of a priority: a national agency is in the pipeline, practical policies are being formulated, existing legislation is being reviewed and the topic now forms a major part of the National ICT Strategy for 2008-2010.

Finally, the service provider industry is seen to take various selfregulatory measures and use state of the art software to reduce the impact of spam, such as spam filters and black lists.

19. Poland

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Only two anti-spam proceedings have been concluded so far by the competition and consumer protection authority and one more is pending. All three have been handled by the Consumer Policy Department (cases allegedly involving infringements of collective interests of consumers). Statistically a decision is issued in this category of proceedings within 5 months. One of the proceedings resulted in an order to cease infringement of collective interests of consumers committed by dispatching unsolicited commercial e-mails. The other proceedings were for misleading e-mail sender headings. *Judicial decisions* – Between 2003 and 2006, the police initiated 71 proceedings involving spam as a misdemeanour, dismissing 16 of them, issuing two mandatory fines, and referring to a petty offence courts in 53 cases. No information on actual judicial sanctions is available.

	Awareness measures – In March 2006, as a part of the Fraud Prevention Month activities, the competition and consumer protection authority organised a conference on network security, a workshop for public prosecutors on online-malpractices (including spamming) and a meeting with internet access providers on the same issue. *Complaint channels* – No separate channel for submitting complaints exists. They may be submitted either on paper or by e-mail to the competition and consumer protection authority.
Measures undertaken by the service provider industry	The first ISP in Poland (NASK) still combines its commercial practices with R&D activities. Among the latter it hosts a team of the national CERT, which allows for submitting information on security incidents, analyses and remedies them, and disseminates outcomes of the process.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information is available that would indicate cooperation between the relevant authoritiesOnly the competition and consumer protection authority acknowledges its enforcement authority regarding spamming practices, for which the telecom regulator refuses its powers. Furthermore, it appears that cooperation between the police and other authorised authorities is vestigial. The telecom regulator claims its willingness to take a more proactive role if it was provided with a stronger legal basis for establishing a "spambox" and an appropriate budget. If enacted, the rearrangement would lead to centralisation of the enforcement policy, again downplaying the cooperation issue.
Cooperation between government and industry	No information on cooperation schemes is available.
Cooperation at international level	The competition and consumer protection authority participated in the SPAM zombies project. In 2005-2006 NASK participated in the SPOTSPAM project.

General assessment
Poland can be considered as a Member State with limited information on actions and measures related to the public awareness actions on online malpractice such as spam, spyware and malicious software. Allegedly, Poland ranks amongst the main sources of malware in the EU. During a major security incident in November 2008, it is said to have produced the largest spam volume. The general issue of network security, paramount to an effective anti-malware strategy, does not appear to have been seriously addressed yet by the public authorities in Poland. Also, no elements indicate that a feasible model of co-regulation with the Internet-related industries, which would provide for a clear and mutually acceptable incentive structure, has been devised. At the same time, the current model of self-regulation (and absence of governmental action) appears to have been ineffective so far. No information is available on filtering or other similar measures undertaken by the internet service providers' industry. Therefore, it may be beneficial to incentivise the industry to provide a more appropriate technical architecture response (security measures) to practices hindering Internet traffic and limiting satisfaction of the Internet users. At the time of this Study, two proposals aimed at strengthening anti-spam provisions in the telecommunications law are being discussed in Poland. The first is authored by the main opposition party. It broadens the definition of spam radically, by encompassing also non-commercial unsolicited messages, and raises statutory penalties for spamming by twenty times, from the current 5.000 PLN (i.e. approx. 1.200 EUR at the time of this Study) up to 100.000 PLN (i.e approx. 24.000 EUR at the time of this Study). Another proposal is being prepared by the ministry responsible for telecommunications. This proposal concerns a draft amendment to the telecommunications law on spam and is more moderate. Both of the drafts reinforce powers of the national telecom regulator regarding spam prevention. The authority claims the amendment is necessary for the establishment of a spam-box – an internal unit responsible for counteracting on-line malpractices.

20. Portugal

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Both the telecom regulator and the national DPA can impose fines. In practice, only the DPA is said to have imposed fines so far. *Judicial decisions* – There is no track record of judicial sanctions on spam and, notwithstanding the number of processes in the inquiry phase, no

	references have been found regarding the last two years. *Awareness measures* – The national telecom regulator is expected to provide more educational information to web users on its website, including the response to a 2008 query on spam. *Complaint channels* – Via the website of the national telecom regulator, communications users and subscribers can upload their complaints against unsolicited communications and other malpractices on electronic communications. Complaints are also possible via e-mail, fax, mail or directly. Criminal complaints can also be filed on the website of the police but apparently this function has never been used by citizens.
Measures undertaken by the service provider industry	Almost all ISPs offer free anti-spam filters. About half of them offer anti-virus software.
Measures undertaken by the vendor industry	Software producers tend to make available anti-spam filtering.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information is available that a formal, institutional and systematic cooperation has been implemented between the competent authorities. A first approach has been taken by the national telecom regulator and the DPA, who organise meetings to analyse future actions, together with the foundation for national scientific computation. This project is still in an early stage but it is expected to lead in the future to a cooperation protocol.
Cooperation between government and industry	The national CERT is starting a program with ISPs in order to cooperate within the scope of reported illegal activities. This may constitute a first step for a new approach of ISPs in order to adopt preventive measures against malpractices of their clients, in particular in relation to spam.
Cooperation at international level	The national telecom regulator participates in the CNSA, the LAP and the OECD on behalf of Portugal. The foundation for national scientific computation always attends the ICANN's worldwide meetings to ensure the exchange of information and cooperation on spam.

General assessment
Portugal can be a seen as Member State where no comprehensive information about measures against online malpractices is available. The laws do not provide a clear understanding about the leading role of the regulators and there is no clear and concise rule on anti-spam actions. It seems plausible that the telecom regulator may act regarding spam and spyware on corporate bodies, the national DPA on spam and spyware regarding individuals and the police computer crime unit on malicious software. The lack of clarity and coherency of the Portuguese legal framework leads to uncertainty on the competences to act against online malpractices. In fact, it may be acceptable that different authorities may act against quite similar situations, without a feasible explanation. This may be the major explanation for the absence of comprehensive actions by regulators. Apparently, the national DPA imposed some fines. Nothing indicates that competent authorities on this matter are cooperating on the implementation of coordinated public rules. On the other side, it seems that ISPs are willing to take more proactive approaches against online malpractices. Currently, most of them already provide anti-spam filters and about half of them offer anti-virus software.

21. Romania

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – In response to spam related complaints, the telecom regulator applied fines in 20 cases in 2008, ranging from EUR 250 to 500. It intends to apply in the future higher and higher fines. The national DPA applied two fines for mobile spam (via SMS). *Judicial decisions* – There are no Court cases related to online malpractices such as spam or spyware. *Awareness measures* – The ministry of communications informs end users about spam and other internet related crimes via its website. For 2009, the national telecom regulator plans to launch a website with information regarding online malpractices such as spam, spyware, and also to start two campaigns against spam. More information about the spam phenomena and guidelines regarding the measures to be taken by an end user against unsolicited commercial communications, are provided by private associations through their

	websites. The Romanian Association for Technology and Internet provides the first Romanian black list of spammers through its website. *Complaint channels* – A complaint form for cybercrime, including spam and spyware, is available on the website of the ministry of communications. The website of the Romanian Association for Technology and Internet provides an online complaint form. Such complaints are then forwarded to the telecom regulator.
Measures undertaken by the service provider industry	Several ISPs offer their clients packages for internet protection including anti-virus, anti-spam, anti-spyware. Such technical solutions are developed together with software producers. Some ISPs have included an explicit spam policy in their T&C, reserving the right to suspend user access for an unlimited period of time.
Measures undertaken by the vendor industry	Software producers develop solutions in coordination with ISPs. One software producer provides though its website relevant information regarding unsolicited commercial communications in Romania, as well as statistics and advices on how to avoid spam.

Cooperation activities to combat malware	
Cooperation between governmental bodies	The national telecom regulator and DPA signed a cooperation protocol with regard to the breaches of the legislation regarding unsolicited commercial communications and the supervision regarding the protection of personal data sent by electronic communications. However, the protocol between the two authorities is not public. Also, the telecom regulator has a protocol with the ministry of administration and internal affairs with respect to the cooperation between the telecom regulator and the department for organised crime, as both authorities are in charge with the investigation of computer-related crimes. In most cases, the telecom regulator forwards computer crime related complains when they exceed its investigation and punishment powers. However, the protocol between the two authorities is not public.

Cooperation between government and industry	Not much information is available. One example of cooperation is the website of the Romanian Association for Technology and Internet which forwards complaints via its website to the telecom regulator.
Cooperation at international level	Romania does not participate in the CNSA, Operation Spam Zombies, the LAP or the OECD anti-spam working group.

General assessment
Romania can be a seen as Member State with an increasing amount of comprehensive information about measures related to the combat against online malpractices such as spam, spyware or malicious software. The first steps in the fight against spam and spyware, were undertaken in 2008, when a large number of complaints was filed with the telecom regulator and the first sanction for unsolicited commercial communication was applied by this authority. This shows an increase of the interest of the end users in the fight against spam. However, no centralised information about the impact of such online malpractices among the Romanian companies is available. With rather poor results in combating online malpractices so far, the telecom regulator aims for a decrease of unsolicited commercial communications in 2009, by starting a campaign against spam, and by launching a website dedicated to combating online malpractices. Apparently, the telecom regulator also cooperates with the national DPA. The service provider industry contributes by offering their clients packages for internet protection including anti-virus, anti-spam and anti-spyware. Information on cooperation between the government and the industry is however not available.

22. Slovakia

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Both the Slovak telecom regulator and the trade inspection can impose fines. In practice, only the latter is said to have imposed fines so far. It receives many complaints (75 in 2006, 104 in 2007 and 33 in 2008). Around half of them are usually legitimate and subsequently handled. Only 41% of cases were handled successfully. A total of 39 fines has been imposed (of which the highest was around 3320 EUR. *Judicial decisions* – No information available. *Awareness measures* – The KRYSA Project formulated 10

	commandments on how to correctly deal with electronic mail. The web site krysa.sk educates end users and provides general information about combating spam and awareness messages about online risks. *Complaint channels* – There is currently no special online malpractices complaint channel provided by competent authorities to end-users and subscribers.
Measures undertaken by the service provider industry	Several ISPs offer their clients (web-based) spam filters, use blacklists, etc.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information available. The competences of the relevant authorities are laid down in various laws. There is no exchange of information nor any kind of closer cooperation.
Cooperation between government and industry	There is no information available on the existence of co-operation protocols or formal and informal procedures related to the co-operation of competent authorities with e-communications network and service providers.
Cooperation at international level	Slovakia does not participate in the CNSA, Operation Spam Zombies, the LAP or the OECD anti-spam working group.

General assessment
Slovakia can be considered as a Member State where insufficient information can be found related to the combat against online malpractices such as spam, spyware or malicious software. In comparison to Member States having comprehensive information in this field, Slovakia can be considered as a beginner country where not many actions and measures have been taken by public authorities and industry actors in the fight against those online malpractices. Supervisory authorities have no real investigating and sanctioning powers. The government invests considerable financial resources but efforts are not being made to coordinate actions efficiently between governmental bodies or between such bodies and the private sector. Also, Slovakia is not

participating in any international cooperation schemes to fight spam. On the other hand a development towards a more coherent and integral approach to internet safety can be seen. Increasingly, different players in the internet security chain such as software vendors, ISPs and domain name registrars are being held responsible for the roles they can play and the measures the can take to improve internet safety; partially they substitute the role of government in this field. Several ISPs offer their clients (web-based) spam filters, use blacklists, etc.

23. Slovenia

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No decisions have been taken so far. *Judicial decisions* – Apparently, about 50 cases of malware are reported to state attorneys per year but no information on respective jurisprudence is available. *Awareness measures* – The web page of the safe.si project summarizes all relevant information on spam and malicious software. Information is also provided by the consumer authority. *Complaint channels* – No specific complaint channels are available.
Measures undertaken by the service provider industry	No information available.
Measures undertaken by the vendor industry	There are two interesting examples of actions undertaken by software producers in Slovenia. The first is a website that explains the major threats and offers various software solutions, whilst the other is an internet application, where servers in Slovenia can be (via entering their IP addresses) checked on their security status. If the server is on the list (white list) it shall be secure.

Cooperation activities to combat malware	
Cooperation between governmental bodies	No specific formal cooperation agreements appear to exist. There is however a non formalised principle of (obligatory) administrative assistance. In practice this would mean that any competent authority must, when a case of spam is presented, inform the other competent

	authorities.
Cooperation between government and industry	No specific information available.
Cooperation at international level	Slovenia does not participate in the CNSA, Operation Spam Zombies or the OECD anti-spam working group. There is no special organisation or instrument focusing on international cooperation in Slovenia. The contact point under Directive 2000/31 functions as an intermediary between Slovene authorities and foreign users, contacting through their national contact points and vice versa. Typically a case of spam in Slovenia from another member state is reported to the contact point which then contacts the contact point of the member state involved and asks for mutual legal assistance. There were some individual examples of spam originating in another Member State that were reported to Slovenia in 2006, however due to lack of evidence (failure to provide the original communication with headers) no formal proceedings could be launched.

General assessment
Slovakia can be considered as a Member State where insufficient information can be found related to the combat against online malpractices such as spam, spyware or malicious software. On the one hand, Slovenia seems to be a country that is less affected by spam and malware, both as a target and as an originating country. On the other hand, the level of awareness of different internet related threats is very high not only in terms of the threats themselves but also in terms of their legal consequences. A good and comprehensive legal framework enabling the fight against spam is in place. At present nothing indicates the existence of administrative or judicial enforcement practice. To a certain extent this is logical though as spam cases often result from misunderstandings of legislative provisions by the culprits and not of an organised spamming activity. A similar observation can be made in respect of malware, which is also limited to certain individual cases of which however none deserved any judicial or administrative epilogue to be mentioned. Slovenia is not seen to participate in international spam related cooperation schemes. Some other general observations: it is sometimes unclear to whom a spam related claim should be submitted. None of the responsible enforcement authorities has a specific budget for the fight against spam and malware. No information on spam related measures by the service provider industry is available.

24. Spain

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The national DPA imposed 39 fines in 2008 of for sending unsolicited e-mail and SMS, two of them for 30.000 EUR (one of which for unsolicited SMS) with a total of 85.500 EUR. *Judicial decisions* – In 2006 and 2007, three rulings were issued regarding cybercrime with stolen information. *Awareness measures* – The internet users' association tried to create a platform with information on the fight against spam. In 2005, the national DPA published recommendations to prevent spam. In 2008, INTECO published a very comprehensive report named "Study on the situation, nature and economic and social impact of spam". It also provides prevention information on its website. *Complaint channels* – Privacy related complaints can be filed via the website of the national DPA.
Measures undertaken by the service provider industry	The service provider TELEFONICA informs its clients extensively on how to combat spam and how to avoid other fraudulent practices on Internet. Likewise, TELEFONICA offers its clients different tools to combat spam, spyware and malicious software like spam-filters, antivirus, etc… VODAFONE, in its privacy policies, informs its clients on how to avoid frauds on the Internet.
Measures undertaken by the vendor industry	Several companies offer solutions against spam, virus and fraudulent mail (phishing) or malicious (spoof). An example of a Spanish company is Spamina. It offers to its clients control and mobility in the management of their mail addresses, no matter what is the device used to access to the e-mail (PC, portable, PDA, BlackBerry, etc.).

Cooperation activities to combat malware	
Cooperation between governmental bodies	No information available on specific spam and malware related cooperation. There is however cooperation more generally in the field of information security.

Cooperation between government and industry	No information available.
Cooperation at international level	Spain participates in the CNSA, operation Spam Zombies, the LAP and the anti-spam group of the OECD. Also, the national DPA cooperates with Latin-American countries on data protection matters.

General assessment
Spain can be considered as a Member State where moderate information can be found on a diversified series of actions and measures related to the combat against online malpractices such as spam, spyware or malicious software. Whereas the national DPA imposed several spam related fines and offers an online complaint channel, no information is available that would indicate cooperation between governmental bodies or between the government and the industry. Nevertheless, the ministry of industry and trade created a separate entity, INTECO, to foster security and confidence by internet users. Also, the national DPA obtained more powers in the past years. Finally, Spain demonstrates participation in various international spam related cooperation schemes. The largest ISP Telefonica offers its clients different tools like spam filters and anti-virus software.

25. Sweden

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – No actual cases are known. *Judicial decisions* – No actual case are known. *Awareness measures* – The telecom regulator offers a website with an interactive education tool on internet security for end users. The Swedish consumer agency gives advice to consumers about spam and internet security. *Complaint channels* – The Consumer Agency offers the possibility for individuals to report spam via their website.
Measures undertaken by the service provider industry	Several providers filter spam either for free or against a monthly charge and provide their customers with detailed information about internet security. They also have an explicit a anti-spam and anti-virus policy in

	their T&C. There is no national ISPA in Sweden. The Swedish direct marketing association provides guidelines on its website regarding direct marketing. The interest organisation of financial institutions offers information on banking security on its website.
Measures undertaken by the vendor industry	No information available.

Cooperation activities to combat malware	
Cooperation between governmental bodies	SAMFI is a collaboration group which supports agencies within the information security field. The group consists of the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Armed Forces, the Swedish Civil Contingencies Agency (MSB - Myndigheten för samhällsskydd och beredskap), The Swedish Police, SITIC and the Swedish Administrative Development Agency.
Cooperation between government and industry	The website surfalugnt.se is a large public-private partnership initiative with the aim of creating a more secure web browsing experience for the general public.
Cooperation at international level	The national telecom regulator and the consumer agency participate in the CNSA on behalf of Sweden.

General assessment
Sweden can be considered as a Member State where moderate information can be found on a diversified series of actions and measures related to the combat against online malpractices such as spam, spyware or malicious software. The Swedish strategy – from a governmental point of view - focuses mainly on educating users to increase the security level of their computer equipment and less on administrative actions against malicious software. A lot of practical work is most likely done at the level of ISPs who offer security packages and filter spam and e-mails containing viruses. There seems, however, not too much co-operation between ISPs and software companies except in cases of information campaigns. The government and the ISP industry created a PPP initiative to create a more secure web for the public.

One of the aims of the government seems to be to give the ISPs the legal power to prevent spreading of malicious software. The work in this regard has, however, not started yet. Focusing on the weakest link in the chain does make sense and therefore educating the users will almost certainly decrease the possible spreading of spam, viruses and malicious software. Cases of this sort are, however, not prosecuted by the police or the courts to a large extent.

26. The Netherlands

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – The telecom regulator imposed various fines in the past years. In 2004, a spammer was fined 42.500 EUR for having sent 4 spam-runs. An SMS spammer was fined 20.000 EUR. In 2006, a spammer was fined 75.000 EUR. In 2007, three Dutch companies were fined 1 million EUR for placing adware and spyware. In 2008, a spammer was fined 510.000 EUR. *Judicial decisions* – In 2004, a company was condemned for sending unsolicited commercial e-mail. The court imposed a daily fine of 50 EUR for every messages sent after the judgement. In 2002, a company was condemned for sending unsolicited commercial e-mail to mail addresses it had obtained from a public database. The court imposed a daily fine of 2500 EUR for every day of non compliance with the judgment. In 2003, Nigerian spammers were convicted for money laundering and falsification of documents. *Awareness measures* – The ministry of economic affairs initiated several projects that strengthen awareness and public private partnerships. Via digibewust.nl, public and private parties inform about safer internet measures. Via surfnet.nl, a computer network for universities, academic hospitals, research institutes and other scientific institutes, clients receive information on the combat against internet threats, such as spam. Via spamklacht.nl, citizens can find general information about combating spam and awareness messages about online risks. Via consuwijzer.nl, consumers can get (practical) information about spam and spyware. On this website consumers can also find information where to file a complaint.

	Complaint channels – Complaints for misleading content of a spam message can be addressed via spamklacht.nl, a website provided by the telecom regulator and consuwijzer.nl, a dedicated consumer website.
Measures undertaken by the service provider industry	Via the website www.xs4all.nl/helpdesk/e-mail/spam, the service provider XS4ALL informs its clients extensively on how to combat spam. The website www.spamvrij.nl, which is no longer maintained and updated but only kept online for historical reasons, was set up by volunteers who wished to publicly expose companies that were responsible for running sending spam mails (spam runs) and, to a lesser extent, for facilitating them (including ISPs). Several ISPs offer their clients (webbased) spamfilters, use blacklists, etc. Via the website www.infofilter.nl, organised by the branch association of Dutch consumers can ask for free to be blocked from unsolicited commercial communications or offers by telephone, post or from market research by telephone. SURFnet recommends the use of SpamAssassin, an open source spam filter, using a number of techniques to determine whether an e-mail message is spam or not. One of these techniques is SURBL (Spam URI Realtime Blocklists). SURFnet has its own mirror of SURBL and offers it as an experimental service to its members. Several ISPs have an explicit spam policy in their T&C. The interactive advertising bureau developed a code of conduct on 15 June 2004 against spam per e-mail and SMS, based on the principle that marketing via e-mail and/or SMS is only allowed on the basis of opt-in. Via the website www.3xkloppen.nl, bank clients are informed and warned about the risks of internet banking, in particular phishing, of which many clients had become victim.
Measures undertaken by the vendor industry	SpamExperts is a worldwide anti-spam consultancy company with headquarters in the Netherlands. SpamExperts provides e-mail security solutions to private individuals, small and medium enterprises, large organizations in a wide variety of industries, governmental institutions, hospitals, and Internet service providers.

Cooperation activities to combat malware	
Cooperation between governmental bodies	***Telecom regulator and police*** – The high tech crime unit of the Dutch national police and the telecom regulator signed a cooperation protocol. They both are in charge of the investigation and prosecution of computer-related crime and have therefore defined their respective responsibilities and cooperation procedures in this field. In particular, the cooperation between both authorities makes it much easier to exchange information about ongoing investigations than it was the case before. ***Telecom regulator and consumer agency*** – The national telecom regulator and consumer agency signed a cooperation protocol for the common supervision of consumer interests in the field of electronic communications in the Netherlands. It stipulates amongst others a procedure for interpreting legal definitions and a procedure for cases of overlapping competences. ***Telecom regulator and DPA*** – The telecom regulator and DPA signed a cooperation protocol to structure the common supervision on protection of personal data in electronic communications. This protocol integrates previously made working arrangements (19 October 2004) between the same parties in relation to spam. Amongst others, the parties agreed to adopt the same interpretations of legal definitions and to inform each other and to cooperate in the fight against internet insecurity, spam mails, unsolicited calling games ('dialers') and spyware on computers. ***Other forms of cooperation*** – Consuwijzer.nl is a joint initiative of the consumer protection authority, the competition authority and the telecom regulator. It has been established to inform consumers about their rights and obligations and their options to obtain what they are entitled to according to consumer law. Several government agencies met on an informal basis in 2006 to discuss cyber crime issues. The public prosecutor and telecom regulator meet on a regular basis on the possibility of initiating proceedings. The telecom regulator gave training sessions to judges.
Cooperation between	The national DPA maintains a website with a collection of consumer complaints about spam and with information and recommendations for

government and industry	internet service providers. This database is an important source for the telecom regulator to carry out its law enforcement tasks. On 24 April 2008, KPN and the telecom regulator announced their cooperation charter to better ensure compliance with the Telecommunications Act by KPN. The latter agreed to adapt its internal organisation. In case of non compliance, KPN will spontaneously contact the telecom regulator.
Cooperation at international level	The national telecom regulator participates actively in international forums such as CNSA, LAP, OECD and ICANN to ensure the exchange of information and cooperation to combat spam and assists in international investigations. Also, on a regular basis the telecom regulator exchanges information with the Federal Trade Commission of the United States of America. The Commission is responsible for enforcing the Can-Spam Act.

General assessment

The Netherlands can be considered as a Member State where comprehensive information can be found on a diversified series of actions and measures related to the combat against online malpractices such as spam, spyware or malicious software.

The national telecom regulator perceives the role of the Dutch government as strongly dedicated to the fight of online threats. It has real investigating and sanctioning powers and actually make use of these. It also set up various voluntary projects, such as a botnet project, defining guidelines for ISPs to help botnet infected customers with cleaning up their systems. Also, most ISPs offer their clients (web based) spam filters, use blacklists, etc.

In comparison to other Member States, the Netherlands are probably one of the forerunners in combating online malpractices. The government invests considerable financial resources and efforts are being made to co-ordinate actions efficiently. It is a Member State where actions undertaken against spam are followed by results, as it can be summarised in the below table.

Actions Results

The national telecom regulator was given adequate legal powers and financial resources to enforce its anti-spam competences

- it participates actively in international forums
- it has taken a proactive approach at national level, e.g. by hosting the cybercrime working

group for competent government agencies and by starting voluntary initiatives

- it has a spam enforcement policy and rules for sanctioning

it concluded formal national and international cooperation agreements where possible and exchanges information with the USA (federal trade Commission), with Australia and New Zealand

Combination of solid anti-spam laws and active enforcement resulted in a drop of identifiable Dutch origin spam with 85%

Various administrative fines (up to 510.000 EUR for spam and 1 million EUR for adware and spyware!) and judicial sanctions were imposed in the past years

Formal cooperation protocols make the exchange of information about ongoing investigations easier than before

The national telecom regulator actually trains other spam LEAs and civil servants from all over the world

Immediate intervention of the telecom regulator makes it possible to stop potentially major security incidents in a very early phase

27. United Kingdom

Measures undertaken to combat malware	
Measures undertaken by competent national authorities	*Administrative decisions* – Both the DPA and office for communications can impose sanctions, in the latter case including a financial penalty of up to £5,000. To date, these powers have not been exercised. *Judicial decisions* – A number of prosecutions involving spyware have been made under the auspices of the Computer Misuse Act 1990. In the case of R v. Waters the accused was convicted of an offence and sentenced to a term of 4 months imprisonment when he admitted engaging a firm of private investigators to install spyware on a computer used by his wife. The couple were in the process of divorcing and the accused was suspicious that the wife was transferring assets abroad. Use of the spyware software allowed the investigators to discover passwords for her bank accounts and e-mail messages.

	Operation AJOWAN, was an investigation by the serious organized crime agency of the UK (SOKA) into the activities of UK-based criminals who conducted their crimes using the Internet. The criminals traded stolen bank, credit card and identity information using a website they had created, which allowed criminals around the world to share information without ever meeting. Complex and sophisticated methods to perpetrate the offences were identified, and UK citizens were arrested, prosecuted and convicted. The potential loss to the UK finance sector from the actions of just one of the conspirators was assessed at in excess of £6m. Another similar conspiracy saw the deployment of an advanced 'Trojan' virus, which covertly infiltrated home computers and key-logged personal/financial data. The conspirators were able to access the harvested data remotely. While the potential loss to the UK finance sector from this activity was estimated to be in excess of £10m, the early intervention by SOCA restricted the losses to £265,000. When the conspirators were brought to trial, the quality of the investigation was commended by the judge. *Awareness measures* – The DPA provides extensive information on its website. Also, a specific consumer website of the UK government informs consumers on how they may protect themselves against a range of fraudulent online schemes. *Complaint channels* – The DPA provides on its website an online form for the reporting of spam mails. The office of communications advises individuals on its website to raise complaints with the DPA.
Measures undertaken by the service provider industry	Most ISPs offer their clients (web based) spam filters, use blacklists, etc. Most ISPs have an explicit spam policy in their T&C. The organisation representing those undertakings providing payment services to consumers offers via its website both general information to customers how to safeguard their on-line accounts and information about emerging fraudulent schemes.
Measures undertaken by the vendor industry	SpamExperts is a worldwide anti-spam consultancy company with headquarters in the Netherlands but which also operates in the United Kingdom. SpamExperts provides e-mail security solutions to private individuals, small and medium enterprises, large organizations in a wide variety of industries, governmental institutions, hospitals, and Internet

	service providers.

Cooperation activities to combat malware	
Cooperation between governmental bodies	A letter of understanding was signed by the DPA and the office of communications in August 2007 which lays down the manner in which the Privacy and Electronic Communications Regulations are to be enforced.
Cooperation between government and industry	The internet watch foundation is independent of government but has established close links with a number of Government departments including the Department for Business, Enterprise and Regulatory Reform and the Ministry of Justice. Links also exist with police forces including extensive connections with the Serious Organised Crime Agency. Its prime focus is operating a hotline to enable the public to report instances of potentially illegal child sexual abuse images hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK, for example via websites, newsgroups, mobile services or other on-line services. Given this limited scope, its work is perhaps of limited significance to the Study.
Cooperation at international level	Operation CATTERICK, was a ground breaking joint operation between the serious organized crime agency of the UK (SOKA) and Russian law enforcement into extortion demands made by organised Russian criminals using distributed denial of service attacks against UK based online companies. Three Russian nationals who appeared at the Regional Court in Balakovo were prosecuted and convicted by the Russian authorities with extensive support from SOCA specialist officers. The sentences (of eight years imprisonment without parole) were appealed. SOCA again provided support and evidence for the appeal court hearings, leading to all appeals being dismissed. The UK also participates in operation spam zombies.

General assessment
The United Kingdom can be considered as a Member State where comprehensive information can be found on a diversified series of actions and measures related to the combat against online malpractices such as spam, spyware or malicious software. Although issues of spam and spyware receive considerable publicity in the United Kingdom,

relatively few formal controls or (cooperation) procedures exist. The website of the United Kingdom's regulatory agency for the electronic communications sector, the Office of Communications (OFCOM) indicates that the agency does not regulate Internet content and advises individuals with concerns about spam or spyware to 'ask their ISP'. Most ISPs offer their clients (web based) spam filters, use blacklists, etc. Although legislation has been introduced, sanctions are limited and few resources have been allocated to the agencies charged with enforcing the rules. No cases have been reported of action being taken against spammers. The situation is a little more optimistic regarding spyware and although there have not been many cases, there is no doubt that the provisions of the Computer Misuse Act will apply in respect of this form of behaviour, at least where software is installed without the authority of a computer owner.