Trafficking in human beings: Internet recruitment

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EG-THB-INT (2007) 1

Trafficking in human beings: Internet recruitment

Misuse of the Internet for the recruitment of victims of trafficking in human beings

prepared by Athanassia P. Sykiotou
Lecturer in Criminology
Faculty of Law
Democritus University of Thrace (Greece)

Directorate General
of Human Rights and Legal Affairs
Council of Europe
2007

Édition française : *Traite des êtres humains : recrutement par internet*

The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.

The study on the *Misuse of the Internet for the recruitment of victims of trafficking in human beings* was carried out in the context of the Council of Europe Campaign to Combat Trafficking in Human Beings and funded by the government of Monaco.

Gender Equality and Anti-Trafficking Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

First printing, October 2007
Printed at the Council of Europe

The **Council of Europe** is a political organisation which was founded on 5 May 1949 by ten European countries in order to promote greater unity between its members. It now numbers forty-seven European states.[1]

The main aims of the organisation are to promote democracy, human rights and the rule of law, and to develop common responses to political, social, cultural and legal challenges in its member states. Since 1989 it has integrated most of the countries of central and eastern Europe and supported them in their efforts to implement and consolidate their political, legal and administrative reforms.

The Council of Europe has its permanent headquarters in Strasbourg (France). By Statute, it has two constituent organs: the Committee of Ministers, composed of the foreign ministers of the 47 member states, and the Parliamentary Assembly, comprising delegations from the 47 national parliaments. The Congress of Local and Regional Authorities of the Council of Europe represents the entities of local and regional self-government within the member states.

The European Court of Human Rights is the judicial body competent to adjudicate complaints brought against a state by individuals, associations or other contracting states on grounds of violation of the European Convention on Human Rights.

Anti-trafficking activities of the Council of Europe

Trafficking in human beings constitutes a violation of human rights and is an offence to the dignity and the integrity of the human being. The Council of Europe, whose principal vocation is the safeguard and promotion of human rights, has been active in the fight against trafficking in human beings since the late 1980s.

The Council of Europe Convention on Action against Trafficking in Human Beings [CETS No. 197] was adopted by the Committee of Ministers on 3 May 2005 and opened for signature in Warsaw on 16 May 2005, on the occasion of the 3rd Summit of Heads of State and Government of the Council of Europe member states.

This new Convention, the first European treaty in this field, is a comprehensive treaty focusing mainly on the protection of victims of trafficking and the safeguarding of their rights. It also aims to prevent

[1] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Georgia, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, "The former Yugoslav Republic of Macedonia", Turkey, Ukraine, United Kingdom.

trafficking and to prosecute traffickers. In addition, the Convention provides for the setting up of an effective and independent monitoring mechanism capable of controlling the implementation of the obligations contained in the Convention.

For further information on the Council of Europe's activities to combat trafficking in human beings please consult our Web site: http://www.coe.int/trafficking/.

Gender Equality and Anti-Trafficking Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex
Tel. +33 3 88 41 20 00
E-mail: dg2.trafficking@coe.int

Contents

Foreword

Trafficking in human beings is the modern form of the old worldwide slave trade. It treats human beings as a commodity to be bought and sold. The victims are put to forced labour, usually in the sex industry but also, for example, in the agricultural sector or in sweatshops, for a pittance or nothing at all. Trafficking in human beings directly undermines the values on which the Council of Europe is based: human rights, democracy and the rule of law.

The *Council of Europe Convention on Action against Trafficking in Human Beings [CETS No. 197]* was adopted by the Committee of Ministers on 3 May 2005 and opened for signature in Warsaw on 16 May 2005, on the occasion of the 3rd Summit of Heads of State and Government of the Council of Europe member states.

This new Convention, the first European treaty in this field, is a comprehensive treaty focusing mainly on the protection of victims of trafficking and the safeguarding of their rights. It also aims to prevent trafficking and to prosecute traffickers. In addition, the Convention provides for the setting up of an effective and independent monitoring mechanism capable of controlling the implementation of the obligations contained in the Convention.

In 2006 the *Council of Europe Campaign to Combat Trafficking in Human Beings* was launched under the slogan "*Human being – Not for sale*". The aim of the Campaign is to raise awareness of the problem of trafficking in human beings and identify solutions to it among governments, parliamentarians, local and regional authorities, non-governmental organisations and civil society. The Campaign also promotes the signature and ratification of the Convention.

When drawing up the Convention, the drafters looked at use of new information technologies in trafficking in human beings and decided that the Convention's definition of trafficking in human beings covered trafficking involving use of new information technologies. For instance, the definition's reference to recruitment covers recruitment by whatever means (oral, through the press or via the Internet). It was therefore felt to be unnecessary to include a further provision making the international-cooperation arrangements in the Convention on Cybercrime [ETS No. 185] applicable to trafficking in human beings.

However, given the rapid development in the use of information technologies, in particular the Internet, and the new possibilities which have opened up for the traffickers, it was decided in the context of the Campaign, to further examine this aspect of trafficking in human beings. The project on the Misuse of the Internet for the recruitment of victims of trafficking in human beings (2005/DG2/VC/405) aimed to provide member states with appropriate legal, administrative and technical measures and more effective awareness raising. The project was funded by the Government of Monaco.

In addition to this study, a seminar on the *Misuse of the Internet for the recruitment of victims of trafficking in human beings* was organised in Strasbourg on 7-8 June 2007. Participants included Council of Europe experts, representatives from Eurojust, Europol, International Labour Organisation (ILO), national police forces and non–governmental organisations. Experts presented legal, administrative and technical measures to fight against the recruitment of victims of trafficking in human beings through the Internet and representatives from non-governmental organisations explained how they contribute to preventing this misuse. The discussions emanating from this seminar are reflected in this study. The proceedings of the seminar are available on the following Council of Europe website: http://www.coe.int/trafficking/.

The author of the study, Athanassia P. Sykiotou, is a Lecturer in Criminology in the Faculty of Law of Democritus University of Thrace (Greece). Ms Sykiotou was an active member of the former *Ad Hoc Committee on Action against Trafficking in Human Beings (CAHTEH)*, the Council of Europe Committee responsible for drafting the Convention. She is actively involved in the *Council of Europe Campaign to Combat Trafficking in Human Beings* through her participation as keynote speaker in a number of regional information and awareness raising seminars. She has made several publications on trafficking in human beings including: *Trafficking of Human Beings in the Balkans*, Ant. Sakkoulas Publ., 2003; *The Concept of Victim in Trafficking in Human Beings*, in: Poinika Chronika, 2006, (pp.684-693); *Organised crime and trafficking in Human beings: fighting against the phenomenon in EU*, forthcoming in: Poinika Chronika, 2008.

The Council of Europe project – The 2003 report and methodology of the present report

The 2003 report

The Council of Europe started developing a European policy on use of the new information technologies in its efforts to combat violence against women and all forms of sexual exploitation of women after the 1997 Summit of Heads of State and Government. As part of this policy, it set up a Group of Specialists (EG-S-NT) in 2000, to study the impact of the new technologies on trafficking in human beings for purposes of sexual exploitation. In February 2003, after two years' work, the Group produced a final report,[1] based on the work done on trafficking by the Council of Europe and other international bodies, plus information and data which it had collected on what was still, at the time, a largely unexplored topic.

The report covered three main issues:

I. The impact of the use of new information technologies on trafficking in human beings for purposes of sexual exploitation and its scale: techniques employed by users; various kinds of user, their *modus operandi* and motives;

[1] Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, EG-S-NT (2002) 9, Strasbourg, 17 February 2003. Referred to hereinafter as the 2003 report.

II. existing national and international legislation and its limitations, and the role of the law in combating illegal or harmful use of the Internet; and

III. the new challenges involved in protecting human rights and guaranteeing proper use of new technologies, in particular the effects of use of the new information technologies on the victims of trafficking, freedom of expression and the Internet, and the role of the media.

The report took account of the findings of two studies on “the impact of the use of new communication and information technologies on trafficking in human beings for the purpose of sexual exploitation: a study of the users” and on the “role of marriage agencies in trafficking in women and trafficking in images for the purpose of sexual exploitation”[2], in investigating the links between trafficking for purposes of sexual exploitation and new information technologies, particularly the Internet.

The Group decided that trafficking in human beings for purposes of sexual exploitation, based on use of the new information technologies, was, especially in the human rights context, a comprehensive term encompassing child pornography, enforced prostitution and other forms of sexual exploitation.

It decided to study the impact of new information technologies on trafficking in the case of both children and adults. It also considered the current state of legislation in this area, and the role that laws could play in preventing the new technologies’ potentially harmful effects.

The 2003 report focused on use of the Internet for trafficking in adult s (over 18), especially those who were sexually exploited without leaving their countries, and whose images were distributed on the Internet without their consent. It concentrated mainly on pornography and concluded that – up to then – many countries, and especially the former Soviet countries, had laws against trafficking in human beings. It insisted on the need for a Council of Europe convention in this area.

The legislative situation has improved markedly in the meantime. The Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197)[3] was opened for signing on 16 May 2005, and has already been signed by 29 member states and ratified by 7.[4] It covers all forms of trafficking – national or transnational, based or

[2] Hughes, Donna, at: `http://www.uri.edu/artsci/wms/Hughes/`.

[3] Hereafter referred to as the Convention on Action against Trafficking in Human Beings or the Anti-Trafficking Convention

not based on organised criminal groups, affecting women, children and men, and committed using means of all kinds.

Methodology of the present report

This report, which is voluntarily funded by Monaco, follows the Council of Europe's 2003 report on *The impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation*, and attempts to tackle the issue from a new angle.

Its sets out to show the various ways in which victims are recruited via the Internet, and also – given the Internet user boom – anticipate possible future techniques.

Specifically, it:

- Lists the means used to recruit victims of trafficking in human beings via the Internet;
- Identifies the legal, judicial, administrative and technical means used by member states to combat this misuse of the Internet;
- Inventories best practices used to combat this misuse of the Internet;
- Makes recommendations on legal, judicial, administrative and technical means of combating use of the Internet to recruit victims of trafficking in human beings.

The time available for preparation of this report was extremely short – only six months to collect and evaluate the data, and draft the text. A questionnaire, covering its main aspects, was sent to the member states as a matter of urgency, via the Greek Parliament's Scientific Committee, in December 2006. Twenty-one states responded (the questionnaire did not go to Greece, since the rapporteur was familiar with Greek law). Of the 22 states covered, 15 are members of the European Union, and 4 (Albania, Moldova, Romania and Slovakia), of which two are also European Union members, have ratified the Convention on Action against Trafficking in Human Beings.

The following Council of Europe member states replied: Albania, Andorra, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, "the Former Yugoslav Republic of Macedonia", Germany, Italy, Latvia, Moldova, Montenegro, Norway, Poland, Portugal, Romania, Slovakia, Sweden and the United Kingdom.

[4] At 24 August 2007. Full texts of conventions, together with up-to-date information about signatures and ratifications, can be found on the Council of Europe's Treaty Office's Internet site, `http://conventions.coe.int/`.

For research purposes, we interviewed a number of police officials, especially Mr Manos Sfakianakis, Head of the Greek Police Security Division's Computer Crime Unit, whose assistance was extremely valuable.

The report also reflects the discussions at the Seminar on the Misuse of the Internet for the Recruitment of Victims of Trafficking in Human beings, organised by the Gender Equality and Anti-Trafficking Division of the Council of Europe's Directorate General of Human Rights and Legal Affairs, in Strasbourg on 7-8 June 2007. This seminar, also funded by a voluntary contribution from Monaco, was organised as part of the *Council of Europe Campaign to Combat Trafficking in Human Beings*. Its aim was to discuss the various methods used to recruit victims of trafficking on the Internet, and identify possible legal, administrative and technical remedies. Participants included representatives from Monaco and member states which had ratified the *Convention on Action against Trafficking in Human Beings* (Albania, Austria, Bulgaria, Georgia, Moldova, Romania and Slovakia), as well as experts from Eurojust, Europol, the International Labour Organisation, national police forces and NGOs.

We say nothing about prostitution, since the legality or otherwise of prostitution in a given country is irrelevant to its laws on trafficking in human beings. A country may consider prostitution legal, and its exploitation illegal. We feel that the previous report in a sense blurred the distinction between trafficking and prostitution by trying to connect them. We also feel that, for the Council of Europe, it is more than clear that trafficking involves exploiting the human body and should be banned. Freely exercised and consented prostitution, either legal or illegal, has nothing to do with trafficking – which is why we decided not to deal with the laws on it again.

Since the Council of Europe's 2003 report focused in particular on pornography via the Internet, we thought it better to concentrate, in the present one, on the recruitment via the Internet of victims who are mainly sent abroad for sexual or other types of exploitation.

We have made no in-depth analysis of technical aspects of the various Internet venues or services which traffickers can use to recruit victims, since these were thoroughly discussed in the 2003 report.

Executive summary

Part I: The current situation – techniques used by traffickers to recruit their victims via the Internet

Offering employment through various channels, both formal and informal, seems to be the main ploy. the Internet offers a wide variety of possible approaches to recruitment; from offers aimed at a broad audience, such as employment opportunities (essentially abroad), through the use of search engines or pop-ups to publicise tempting offers, all the way to more targeted spaces, e.g. chat-rooms, spam mail and Internet dating, where victims can be recruited.

Traffickers now have an effective and unrestricted means of recruiting their victims. Online employment agencies (particularly those ostensibly seeking fashion or artists' models) and marriage agencies can all be lures for victims. Internet chat-rooms, too, can be used to "befriend" potential victims. For young people, the danger of falling into the traffickers' clutches has increased substantially. Seemingly innocent Web sites, such as "chat-rooms" – extended versions of the Web discussion sites, open to all surfers – can be highly dangerous as well.

The use of the Internet to recruit victims is not a new form of trafficking, but simply a new weapon in the traffickers' armoury. Previously, press advertisements (employment, marriage, dating, etc.) were one of their best-known staples. Nowadays, when advertisements appear both in print and digital form, technology gives traffickers even more effective means of achieving their criminal ends.

The difference between using the Internet to recruit for pornography and using it to recruit for other forms of sexual exploitation is that the victims in the first case are not required to leave their home countries, while those in the second are trafficked abroad.

Section I: Users

Categorising potential Internet users, we find that women, men and children use the Internet in different ways and for different reasons, and apply different levels of technical skill. Users can be potential victims – but also clients, and indeed traffickers.

Police operations in several member states and at Europol suggest that the Internet and mobile phones are more widely used to recruit victims of trafficking in human beings than was originally thought. They point to the use of the Internet for purposes of labour exploitation, and also sexual exploitation, via bogus escort services, marriage agencies, job advertisements and chat-rooms.

Section II: Factors that impede recruiting victims of trafficking in human beings via the Internet

Communications infrastructure and Internet use are not equally developed in all the member states, and it seems likely that recruitment would be higher if conditions of access to the Internet were easier in some of the potential victims' countries.

Surveys over a seven-year period show that communications infrastructure and Internet use have developed considerably in source countries. However, we still need to find out how many users are frequent users, how they use it, and what their break-down is in terms of age and gender. All of these factors must be considered together, and also the cultural differences which make the Internet more appealing to some than to others.

Part II: Legal, administrative, technical and other means of combating the recruitment of victims of trafficking in human beings via the Internet

Section I: Legal measures

Laws against trafficking seem fairly satisfactory in the 21 member states discussed in this report, even if only 7 have so far ratified the Convention. Most have ratified the Palermo Protocol on trafficking and/or, as European Union members, the Framework Decision on trafficking. Fewer than half the Council of Europe's members have ratified its Convention on Cybercrime, but all of those which are also European Union members have transposed the European Union Directives on communication, whose provisions on liability of providers when serious crimes are committed via the Internet extend to trafficking in human beings.

Section II: Administrative measures

It should be noted that many European countries now have specialised units to combat cybercrime. There are still no such units, however, in the countries regarded as sources of victims of trafficking in human beings.

Section III: Technical measures

Technical measures comprise:

1. those which could contribute to prevention;
2. those which could effectively facilitate prosecution of traffickers who recruit victims via the Internet, and

3. those which could do both.

Many measures aimed at prevention and prosecution have been taken at national and international level, both by governmental and non-governmental authorities – a fact reflected in the successful national and international police operations conducted in recent years. One project which offers hope of effective prevention and prosecution is GRETA – the monitoring system introduced by Chapter VII of the Convention on Action against Trafficking in Human Beings, which is designed, not only to monitor compliance with the Convention, but also to put pressure on the member states to do everything possible to prevent trafficking, prosecute traffickers and protect victims.

It also appears that some countries have the legal and technical infrastructure needed to combat trafficking via the Internet, while others have the laws, but lack the technology – in spite of net progress on infrastructure. Most of the countries which have ratified the Cybercrime Convention are not among the most developed in terms of technical facilities. In other words, some countries have the laws, but not the technical facilities they need to fight and punish crimes committed via the Internet, while others have the technical means, but not the laws.

The fact is, some countries have the capacity to detect and respond rapidly to computer-related crimes, while others have a fair capacity to do the first, but not the second, and others again can do neither. Obviously, potential victims of trafficking in human beings are most at risk in countries in the last two groups. As we have already said, the fact that victim recruitment via the Internet has not so far assumed major proportions is due to limited Internet use and telecommunications infrastructure in source countries.

Section IV: Best practices against trafficking in human beings via the Internet

So far, plenty of practices against trafficking in general seem to have been devised. There are numerous manuals on preventing trafficking in human beings and on investigating and prosecuting it effectively. All of them cover good practice principles. Some of the technical measures adopted by governmental and non-governmental organisations, either national or international/regional, might also be regarded and applied as good practices against trafficking in human beings via the Internet. Examples include the hotlines for reporting or providing information on sites with sexual content, or featuring spurious modelling agencies, operated by the Internet Watch Foundation and Safemodelling.org.com in the United Kingdom, the comprehensive Web sites run by the Italian NGOs On the Road and Gruppo Abelei, and systems like the Headway transnational on-line database on various forms of trafficking, which facilitate international co-operation.

Systems already established to combat child pornography might also be reviewed and adapted for use against other types of recruitment and exploitation via the Internet.

Introduction

The 2003 report noted that the growth of transnational criminal networks and the emergence of wider and more open global marketplaces triggered by privatisation had combined with new computer communication technologies to offer increased opportunities for transnational crime. This technological aspect of globalisation also opens the way to worldwide transfer and laundering of criminal earnings.[5]

The growth of these phenomena is also due to the cheapness and accessibility of the new technologies (e.g. "webcams", which can be used to broadcast images worldwide at relatively little cost). This is a key factor in exploitation of the technical opportunities offered by the Internet.

Nowadays, any crime can be a cybercrime committed via the Internet, which can send text, images, audio and video files around the world in seconds. Significantly, access to this global communications network is now within the financial reach of most people in the wealthier nations[6].

Of course, none of the new technologies should be considered harmful *per se.* the Internet's global network combines benefits (it can be used to fight organised crime more effectively) with drawbacks (it facilitates the growth of organised crime).

However, we should be careful when we talk about cybercrime – a term which we often tend to apply to different types of crime, committed in different ways and using different means. Cybercrime includes: a) computer-related offences; b) crimes against the confidentiality, integrity and availability of data and systems; c) offences related to infringement of copyright and related rights and d) crimes which use computers and

[5] 2003 report, p.13.

[6] D. Hughes, "Globalization, Information Technology, and Sexual Exploitation of Women and Children", *Rain and Thunder – A Radical Feminist Journal of Discussion and Activism,* Issue #13, Winter 2001.

the Internet to commit specific crimes, such as trafficking in human beings in its various forms, e.g. sexual exploitation, child pornography, etc.

It is not true that "the boom in new technologies, in particular the Internet, has paved the way for new forms of crime, also known as cybercrime, including notably sexual exploitation and child pornography"[7].

What is true is that the new technologies have given traditional forms of crime, especially organised crime, a new dimension. Money laundering, drug sales, the dissemination of child-abuse material and prostitution have all evolved as a result of new technological developments.

The Internet offers traffickers unprecedented opportunities, which they have been quick to exploit. It, and other telecommunication technologies, give the sex industry and individual users new ways of finding, marketing and delivering women and children into appalling conditions of sexual exploitation and modern-day slavery.[8]

According to Europol's 2006 Report on Organised Crime, "the advantages the Internet offers in terms of information and communication technology are extremely beneficial to organised crime".[9]

Communication between organised criminal groups and their members must be wholly secret or at least sufficiently impenetrable to avoid giving the police advance notice of their plans. These groups must be able to communicate quickly and securely. E-mail, Internet, chat-rooms and instant messaging all offer them new facilities, as do Web-based and client server mail accounts, Web sites and message boards. They provide fast communication and, thanks to encryption, unprecedented security of the data they store and exchange. Free, encrypted Web-based mail is also available. Advanced communication networks and in-depth knowledge of information technology enable organised crime to operate in a well-organised manner, covering both legal and criminal activities".[10]

Technology is increasingly important for organised criminals, and also for the police in their efforts to mitigate the dangers of organised crime. One major problem is the fact that the law reacts slowly to technological change, with the result that the use of some technologies falls outside its scope.

[7] See 2003 report.

[8] 2003 report: D. Hughes, "A Study of the Users".

[9] Europol, *Organised Crime Threat Assessment Report* 2006, pp. 18-19.

[10] Europol, op. cit., p.19.

Part I: The current situation – Techniques used by traffickers to recruit their victims via the Internet

Misuse of the Internet

In fact, “misuse” of the Internet seems the wrong term, since the Internet offers all users the same technical possibilities. “Misuse” means that a user is not using the capacities offered by a specific tool correctly or fully. The fact that some people use the Internet for criminal purposes does not mean that they are “misusing” it, but that they are using it for improper purposes. In other words, we should not blame the Internet. Talking about “misusing” it to commit a crime is like talking about “misusing” a knife to kill someone.

Criminals use the Internet in exactly the same way as legal businesses – to advertise and attract clients. Basically, the Internet is a commercial tool used to promote and sell products and services of all kinds.

Job-offers through various channels, both formal and informal, seem the main approach to recruitment. Its nature being what it is, the Internet offers a broader range of approaches to recruitment: from offers aimed at a broad audience, such as employment opportunities (essentially abroad), through the use of search engines or pop-ups to publicise tempting offers, all the way to more targeted spaces, e.g. chatrooms, spam mail and Internet dating, where victims can be recruited.

Traffickers now have an effective, unrestricted means of recruiting their victims. Online employment agencies, particularly those seeking fashion or artists’ models, and marriage agencies can all be used to lure victims. Internet chat sites are often used to “befriend” them. For young people, the danger of falling into the traffickers’ clutches has substantially increased.

The Internet, and other types of new technology, are the means which traffickers use to commit their crimes. And, as means, they are user-friendly, fast and anonymous – and deliver victims “on a plate” to traffickers, who no longer have to leave their homes to find them. Broadband and Internet-based wireless networks (e.g. WIMAX) have made things even simpler for them, since they are extremely rapid and cheap.

Cybercrime has the following characteristics:

- It is easily committed;
- It is cheap for the criminal;
- It is anonymous, since the criminal does not have to reveal his identity;
- It is fast and leaves only digital traces;
- It cannot be committed by just anyone, since it requires a thorough grasp of the technology involved;
- The criminal does not have to leave his home place, while the crime itself can produce consequences in various countries simultaneously and affect numerous victims; and
- It can be hard to locate. To cover their traces, criminals operate in various countries, making it hard for national police agencies to determine where the crime was committed.

In other words, the Internet is an efficient tool in the hands of perpetrators of all kinds of crime (especially organised and transnational crimes) and, of course, an easy path to bigger profits. As the 2003 report on pornography emphasises, "Many of the child pornography collectors would never have engaged in this activity, certainly not to the extent they did, if not for the new information technologies that were available to them. The technology did not provoke their interest or activity, but it played a heavy role in facilitating it" (p. 37).

Thus, the recruitment of victims of trafficking in human beings via the Internet is not a new form, but simply a new means, of trafficking. Previously, press advertisements (employment, marriage, dating, etc.) were a well-known way of recruiting victims. Nowadays, with the expansion of the new technologies, these advertisements have also moved to the Internet. Victims no longer need to buy newspapers, while traffickers no longer have to pay for advertising space (although some specialised papers also offered free advertising in the past). the Internet has simply changed the means used to recruit and promote sex – market victims – and has certainly contributed to the rise of trafficking in human beings.

Seemingly innocuous Web sites, such as "chat-rooms" (an extended function of the discussion sites), which are open to all surfers, can prove very dangerous, especially to minors (adolescents), who may come into contact with traffickers and be recruited by them.

The challenge we face today, is: how can we fight this new means of trafficking?

An in-depth knowledge of the methods used by traffickers to recruit victims via the Internet might help us to grasp the full extent of the phenomenon, and combat it more effectively by proposing countermeasures, sensitising decision-makers and public opinion, and alerting potential victims. As the 2003 report notes, a multidisciplinary approach is needed to give us information on computer crime techniques and on trafficking (p. 15). It is true that police cybercrime units in most countries have only a partial knowledge of the methods used by Internet traffickers, since they mainly investigate pornography and child stalking.

The methods of traffickers who recruit victims via pornographic sites often differ from those who recruit them via marriage, escort, dating or job sites. The difference for victims is that those recruited for pornography via the Internet do not have to leave their home places, while those recruited for other forms of sexual exploitation are trafficked abroad.

Users

Just as we should not confuse the means used to commit a crime with the way in which it is committed, so we should not confuse the use of the Internet with the way in which trafficking in human beings is committed. According to the Convention on Action against Trafficking in Human Beings, trafficking is committed by: "the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person". The English version of the Convention may speak of "recruitment by means of the threat or use of force, etc.…", but it obvious that, in legal terms, it is referring to the way in which the crime is committed, using specific means (including the Internet). There is no such problem in the French version, which does not use the word "means", but speaks of recruitment by threat, as follows: "…recrutement... par la menace de recours ou le recours à la force ou d'autres formes de contrainte…". This is an important point, and relevant to the legislative measures we shall be examining in the second part of the report.

The frequently heard general question: "Who are the users? What are their motives?" (the 2003 report also raised it[1]), misses the mark, since there are various users with various motives, just as there are various crimes with various motivations. Categorising potential Internet

[1] These questions had been singled out for research by the experts who drafted Committee of Ministers Recommendation No. R (2000) 11, as very little was known about these matters. In order to gather more information about Internet users and their motives, the Group carried out research in this area, based on the findings of Ms Hughes' work and existing studies in the field. It thus discovered that most users were involuntary users, often minors, in some cases lured into the business through harmful use of technologies by traffickers, and that those users were themselves potential victims.

users, we find that women, men and children all use it in different ways, for different purposes and applying different levels of technical skill. Users can be potential victims, but also clients and indeed traffickers.

Internet users connected with trafficking fall into 3 general categories:

- Traffickers
- Clients
- Potential victims

Traffickers

One general point is that most traffickers who use the Internet are organised in transnational criminal groups. Technology is the main facilitating factor for such groups.[2]

According to Europol's 2006 Report on Organised crime, there are four main categories of organised criminal group[3]:

- Indigenous groups, which are principally territorially based and have extensive transnational activities – especially groups which are able to shield their leadership and assets, even inside the European Union;
- Groups which are mainly ethnically homogeneous, and have their leadership and chief assets abroad;
- Dynamic networks, whose organisational set-up is less vulnerable to attack by law enforcement agencies than their communications and finances;
- Groups which are strictly organised, have no ethnic component, and have a large international presence.

To better understand the way in which traffickers operate through various agency sites, we must try to answer two questions:[4] (a) How do traffickers use the Internet? and (b) What methods do they use to approach their victims? The first concerns the setting-up of sites, the second the types of site used by traffickers to recruit their victims.

How do traffickers use the Internet?

Anonymity, disguise and measures to impede tracing of their communications are crucial for criminals. They may try to avoid being traced by communicating through a whole series of carriers, each using a different

[2] Europol *Organised Crime Threat Assessment Report* 2006, p.17-18.

[3] Europol OCTA Report 2006, p.5.

[4] This information was supplied by the Greek Police, Computer Crime Unit.

technology, e.g. local telephone companies, long-distance telephone companies, Internet service-providers, and wireless and satellite networks. They may send their communications through various countries in different time zones, in one of which at least it is night. This complicated routing makes them difficult to trace for technical, bureaucratic, political and logistical reasons. They may try to avoid being identified by sending their messages through anonymous re-mailers, who delete and replace identifying headers. For example, one re-mail service removed all identifying features from the header, held all incoming message until five minutes past the hour, and then re-despatched them in random order, thus making it harder to trace individual messages. Messages could be sent through anything from five to twenty other re-mailers, with at least one in a country known for its failure to co-operate with the global law-enforcement community.

As stated in the 2003 report, cell and satellite phones can be used far from the user's home base. Mobile phones can also be programmed to transmit false identification. Criminals can sign up for mobile phone services, then discard the phone after a short time, or when a specific crime has been committed. Pre-paid phone cards can also be used anonymously.[5]

File transmission has become easier and criminals now have more ways of disguising themselves. Improved Internet connections, such as cable modems, make communication even faster. All of these technologies have made it easier to produce, store and disseminate images of sexual exploitation.[6]

Internet venues, applications and services

The 2003 report analysed a number of Internet venues and media formats, based on different technologies, which offer ways of exploiting women and children sexually. They include: communications-Usenet newsgroups, the World Wide Web, e-mail, live synchronous communication (text and voice chat), bulletin or message boards, webcams for the live transmission of images or videos, live video-conferencing (live video-chat), streaming video, peer-to-peer servers, and file-sharing programmes. Peer-to-peer networks and file-swapping programmes seem to be the latest technologies.

The 2003 report offers a detailed analysis of all the different types of Internet instrument available to users worldwide.[7]

[5] 2003 report, p. 22.

[6] Ibid.

How each is used for sexual exploitation depends on the activity's legality, which varies between countries, the techniques adopted by the sex industry or individual users, and the level of privacy or secrecy sought by users.

These programmes create a decentralised system, i.e. there is no central server through which all communications pass. Consequently, transmissions are not logged, and cannot be traced, since each site can trace the connection back one level only. Users can enter the public network or create private ones of their own. These are the features which make this new technology so attractive to traffickers.

Encryption is another programme which claims to take anonymity a step further by disguising users.

Whenever criminal activity on the Internet is talked about, encryption is mentioned as a technology which is likely to be used to disguise file content.[8]

Beside the familiar "spammers", the sex industry uses such techniques as "page-jacking" and "mouse-trapping" to pull in surfers who had no intention of visiting a pornographic site, and find themselves trapped, as page after page of pornography opens up when they try to quit the site. Page-jacking is a technique used by sex-industry practitioners to misdirect users onto their Web sites.[9]

It appears that 70% of Internet sites are invisible[10] (sites which have a reference, but are not pointed to by others, cannot be located). This applies to many illegal image sites, whose life is very limited.

Young people downloading free DVDs, songs, music MP3s, games and videos use the same software as paedophiles, e.g., peer-to-peer (eMULE, LimeWire, Gnutella, Morpheus, etc.).

It appears that 89% of 12- to 17-year-olds love to chat on the Internet: class-mates, unknown users, game networks via chat-rooms or Web-nets (MSN Live Messenger, Orange, Yahoo, Lycos). These are perfect contact points for traffickers and paedophiles, who use false identities to lure potential victims to a meeting.

[7] 2003 report, p. 18.

[8] Loc. cit., p. 20.

[9] Loc. cit., p. 21.

[10] According to Jean-Philippe Noat, Technical Director, Action Innocence Monaco, in his presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

The Internet Watch Foundation[11] processed 31 776 reports (a 34% increase) in 2006; 91% of the victims were under 12 years old; 80% were female, and child abuse domains totalled 3 077. Moreover: 83% of all child abuse domains were hosted in the United States and Russia. Specifically, 55% of child abuse sites are hosted in the United States, followed by 28% in Russia; 8% in Europe and 7% in Asia.

Unsolicited e-mail

It should be stressed that criminals also operate through unsolicited e-mails, luring users into revealing sensitive data via so-called "phishing" e-mails. Privacy is at risk from spyware, spread by e-mail or software, which tracks and reports on users' behaviour.

The security firms Symantec and MessageLabs estimate that spam[12] accounts for 54% to 85% of all e-mail. In 2005 Ferris Research estimated that spam cost €39 billion worldwide, while Computer Economics calculated that malicious software cost €11 billion globally. The very latest figures from Sophos say that 32% of relayed spam came from Europe, topped by Asia at 34%.

At European Union level, the European Commission acknowledged, in a recent Communication on spam[13], that laws to combat these threats are already in being – particularly the European Union-wide "ban on spam", adopted under the ePrivacy Directive in 2002[14]. However, enforcing them is still a problem in most European Union countries. To improve the situation, they should now assign clear responsibility for using the tools available in European Union law effectively. Spam was reduced in the Netherlands with the help of prosecutions brought by OPTA, an anti-spam agency with just 5 full-time staff and 570 000 euros' worth of equipment.

The European Commission's Communication calls on industry to co-operate fully by applying proper filtering policies and following good commercial practices online, in accordance with data protection law. In Finland, filtering measures of this kind cut spam from 80% to 30%.

[11] According to Sarah Robertson, IWF Communications, in her presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

[12] See Appendix 1, page 144.

[13] Communication of 27 November 2006; it can be downloaded at `http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1629&format=HTML&aged=0&language=EN&guiLanguage=en`.

[14] See Part 2, page 71, for more details of European Union legislation.

The Commission will further reinforce its dialogue and co-operation with non-European Union countries which are high on the list of spam-senders. The United States and the European UnionEuropean Union have agreed, for example, to co-operate on tackling spam through joint enforcement initiatives, and explore ways of fighting illegal spyware and malicious software. For Asia, the Commission has issued a Joint Statement on International Anti-spam Co-operation, which was adopted at the ASEM conference on eCommerce in 2005.

The Commission is now re-examining the relevant laws, with a view to introducing legislative proposals on strengthening user privacy and security in 2007. These proposals may oblige service providers to report security breaches which lead to personal data-loss and/or interruptions in service supply. National regulatory authorities would have power to ensure that operators implemented adequate security policies. Member states would be required to ensure that any person or organisation with a legitimate interest in combating violations of the ePrivacy Directive could take legal action before a national regulatory authority.

Production of sites

There is a certain consistency in production of the sites which are mainly used to recruit victims for sexual exploitation abroad. Traffickers can be grouped in three categories,[15] depending on their contribution to the production of sites, and the uses they make of them. It should be noted that these three categories are often connected with the organised transnational form of trafficking in human beings, and that traffickers can figure in all three categories simultaneously:

i. Traffickers often set up sites in the countries of origin and in the languages of potential victims, e.g. in Russia and in Russian to recruit Russian girls.[16] Such sites then spawn others, often building up to form national recruitment networks. They are also tailored to the market the traffickers are targeting (e.g. tall, blond women are the type generally favoured by the Greek sex industry[17]).

ii. The material collected via the first site is then used on a second, aimed at attracting clients. Information on the recruited victims is translated into English and the languages of other sex markets where the traffickers wish to operate. At this stage, "escort service" sites start seeking subscriptions from members (clients), who are

[15] The 2003 report also included consumers among perpetrators, see p.102.

[16] See `http://www.strada.org.pl/`

[17] According to the Greek Police, Greece does not produce material for these sites (i.e. no Greek victims are recruited), but it does use them.

given the option of paying online to visit the girls in their own countries or, alternatively, "import" them (availability in terms of place and time is specified). If a client wants to bring a girl to his own country, a local go-between makes sure that she gets in and out "safely". The same process may apply if a local trafficker wants to bring in victims advertised on the Internet and exploit them in his own business. Often, this involves contacting a middleman – which can be the case with most forms of trafficking in human beings, from domestic slavery to sexual exploitation (but not pornography, which does not require victims to leave their home countries). Traffickers in these two groups may be identical (the same person) or, more often, the second may act as accomplice to the first.

iii. The third type is the trafficker who recruits victims (mainly as "models") and exploits them directly (without middlemen) via online booking with clients.[18]

iv. A distinction should obviously be made between traffickers who set up sites themselves and then exploit the victims recruited, and operators who are paid by traffickers to set up sites, thus becoming their accomplices. These people play a key role in trafficking in human beings via the Internet, since they have the technical know-how needed to create sites, and hide electronic traces from the police. (N.B. innocent IP addresses can also be stolen by traffickers and used to hide their true addresses). In some cases they are themselves traffickers.

Sites that recruit and exploit (mainly) women from abroad differ from pornographic sites in being harder to manage and exposing traffickers to greater risks, e.g. the risk that a girl will be stopped at the border, and that border officials may need bribing. This partly explains why this type of trafficking seems mainly to attract organised criminal groups.

However, there are other problems, e.g. when criminals use proxy servers, usually based in countries with no proper legislation – which makes it increasingly difficult to identify the people behind the Web sites. These sites (especially pornographic sites) can also use payment methods such as e-gold and Web money – virtual charge cards, which make it hard for the police to follow the money trail.

[18] One such site is: `http://www.greekescort.com/`.

Methods used by traffickers to recruit victims

It should be noted that, as a result of the Internet's technical aspects, the potential Web-recruited victim's profile is, in a sense, narrower than that of other victims:[19]

1. Basic computer literacy and Internet access are needed to find on-line offers. For example, people in impoverished rural areas, where basic infrastructure is lacking, do not normally have regular access to modern information technologies.
2. Internet access can be private or public. Job-seekers, for example, can find it at job centres, in libraries, etc. Children and young people, on the other hand, use the Internet at school, in friends' houses and at home.
3. Trust and confidence in the information society also play a role. The psychological reasons for using the Internet are worth considering. Some of the people who turn to it for information may simply be following the trend, and may feel that companies with attractive Web sites are more trustworthy than others.

The two methods chiefly by traffickers to recruit victims via the Internet are:

- spurious advertisements for employment, marriage, dating agencies, etc.
- chat-rooms.

The recruitment sites used by traffickers are:

- marriage agency sites (can act as mail-order bride agencies or dating clubs);
- escort service sites;
- dating clubs;
- employment sites seeking e.g.:

– home helps
– waitresses/bartenders
– au pairs/carers
– models
– dancers/hostesses
– people to work in the building trade/factories/agriculture
– people to take educational courses
– people to work in tourism

[19] Klara Skrivankova, Antislavery International, presentation at the Council of Europe seminar on the Misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

– sex workers (it should be noted that the fact of already being a prostitute does not exempt a woman from being trafficked).

Research suggests that victims are normally (but not always) recruited in their own countries. There, a recruiter from the “employment agency” persuades them to sign an incomplete or incomprehensible job contract. The necessary documents (visa, work permit etc.) are then procured by the agency, which normally charges a fee or makes the victim a “loan” to cover costs. Persons recruited are often assisted by “agency representatives” and, on reaching their destination, are taken over by a local contact. Supposedly for their own protection, their papers are often taken from them. Without papers, and often without knowing the local language and environment, they are easily manipulated.

When victims have no computer access, a relative (this is commonest in the case of marriage agencies) or friend acts as go-between and either provides Internet access or replies to the fraudulent job offer for them.[20]

In a straightforward Google search, we turned up over 128 000 suspect sites, advertising marriage, escort, dating, modelling services, etc. We would emphasise that these sites can only be termed “suspect”, since there is no evidence that the girls on offer for sexual services or marriage are actual or potential victims of trafficking. Sometimes, however, there are strong indications that this is the case. Of course, the mere fact of a woman’s coming from a certain area (poor and often rural) is not – even when the 2003 report’s[21] remark that “review of the marriage or introduction agencies that operate on the Internet reveals that sometimes subtle, but often blatant, sexualised photographs of the women are used to appeal to men” and that “the descriptions of the women claim they are oriented towards pleasing men” applies – is not per se a sure sign that these women are victims of trafficking in human beings. Essentially, it is the dominant role played by men in society which leads women to play this kind of game. For centuries and in numerous societies, women have been trying to please and appeal to men in the very same way. Feminists would argue that this reflects their exploitation by the system and by the submissive role they are expected to accept in a man’s world. However, we cannot connect it directly with the legal concept of sexual exploitation based on trafficking in human beings, unless there are definite indications or police evidence that this crime has been committed.

[20] This was mentioned in the Polish reply to our questionnaire as the “informal way”.

[21] 2003 report, p. 45.

We must not confuse soliciting to engage in prostitution, which involves sexual exploitation, with procuring. While procuring merely facilitates[22] an existing, freely taken decision to engage in prostitution, soliciting involves the use of persuasion, deception or coercion to make a person engage in prostitution – which shows that the victim's consent is not freely given; in other words, his/her will has been altered. This is actually the reason why the Convention on Action against Trafficking in Human Beings and the Palermo Protocol state that consent is irrelevant[23] if the person concerned has been trafficked (in the case of adults).

We must also stress that cultural differences between member states can make it difficult for potential victims to grasp the risks they run by signing up with these agencies.[24]

We should also distinguish marriage or other agencies which recruit women for exploitation purposes, and lawful agencies which provide Internet access at their offices, so that women can contact men (who are charged for talking to them). As the 2003 report notes (p. 46), these agencies may not themselves be involved in trafficking for purposes of sexual exploitation – but they are providing Internet access and contacts in the West which may increase the likelihood of their clients' encountering traffickers.

A Danish police report notes suspect advertisements for nannies, waitresses and dancers on Web sites in Latvia and Lithuania.[25] Traffickers use such sites to advertise jobs in Western Europe, just as they do in magazines and newspapers. Magazine ads give mobile phone contact numbers, while We sites give e-mail addresses.

It must be stressed that links between the Internet and trafficking can take several forms:

1. victims may fall prey to traffickers via Web sites and other Internet services;
2. trafficked victims may be traded, or their services "advertised" to clients, via the Internet;
3. victims recruited in traditional ways may be forced to contact clients online.

[22] See the distinction between the two crimes in the Greek Criminal Code. Soliciting adults to engage in prostitution is punishable by imprisonment for up to 10 years (Article 351), while procuring is punishable by imprisonment for at least 18 months (Article 349 (3)).

[23] The 2003 report refers (p. 77) to a Swiss Supreme Court ruling that consent given by a person from a very poor country carries no weight – but gives no reference.

[24] 2003 report, p. 45.

[25] The report can be downloaded at http://www.coe.int/T/E/human_rights/Trafficking3_Documents/Reports/#P473_60876.

A brief examination of many Web sites reveals their commercial interests in bride-trafficking, sex tours and prostitution. There are catalogues of women, mostly from Asia and Eastern Europe, giving pictures and stating their names, height, weight, education and hobbies. Bust, waist and hip measurements are sometimes included. The age range is 13 to 50.[26]

Escort or "personal" services

An example is provided by Cosmos Escorts International,[27] a site which offers sexual services in 37 cities worldwide, 35 of them in Europe. Its advertisement reads: "Cosmos Escorts International can provide you with local escorts in many European cities and also in Sydney. Each of our young ladies is very attractive, charming, well educated and very discreet at all times - they are either models or natural beauties".

Another site[28] is advertised as an "International Escort Agency, offering an exclusive and personalised service available worldwide". It contains photos of girls, and indicates when they are available in various places. The client can book a specific girl online, checking when she will be in his city, and the day and hour when she will be available. He can choose to suit his own convenience, and pay online by credit card.

There are thousands of these erotic sites offering "escort" services worldwide. Again it must be stressed, however, that no one can be sure that the women whose services are offered are victims of trafficking in human beings; they may equally well be prostitutes plying their trade voluntarily – even though this may be illegal in some countries.

Recruitment – examples

Estonia – Finland

Much sexual abuse has hidden origins on the Internet. The most popular site in Estonia[29] is estimated to have, on its own:

- 360 000 registered users;

[26] D. Hughes, "Use of the Internet for Global Sexual Exploitation of Women and Children", at `http://www.uri.edu/artsci/wms/hughes/`.

[27] `http://www.cosmos-escorts.com/`.

[28] `http://www.greecescort.com/`.

[29] `http://www.rate.ee/` (according to the presentations given by H.K. Kolkanen and K. Spiegel from Estonia's Central Criminal Police, and K. Eriksson and J. Lappalainen from Finland's Criminal Investigation Division at the Council of Europe Seminar on the Misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007).

- 130 000 users per day;
- 350 000 visits per week;
- 19 million pages displayed per day.

The users are nearly 80% women and 20% men. National statistics indicate that this site generates two-thirds of Estonian Internet traffic.

In July 2006, the Helsinki District Court found eight people guilty of bringing 15 Estonian women, one of them mentally handicapped, to Finland and forcing them to work as prostitutes between October 2005 and March 2006. The victims had been recruited via the Internet and mobile phone. Five Estonian men, one Estonian woman and two Finnish men were given prison sentences of two to five years for aggravated human trafficking and pimping. They had placed their victims in apartments or hotels in five Finnish cities between October 2005 and February 2006. They had strict rules, forbidding their victims to leave their place of work, visit restaurants or receive visitors without their permission. Clients were charged €70-€80 or €120-€140. The victims had to pay a weekly fee of €500-€2 000, which went to criminals based in Estonia. In addition to this weekly fee, they were forced to hand over at least 50% of the money they received from clients. A separate arrangement was made with each victim. The mentally handicapped victim received no money at all. Women who broke the rules were threatened with violence and fined €500.

The two leaders of the gang ran the scheme while already serving prison sentences in Estonia. They used mobile phones and Internet to recruit victims, and advertise sexual services on the popular site referred to above.

Their orders were carried out by another Estonian, who employed his wife and another woman to update Web pages, and receive and distribute the takings. Another Estonian resident in Finland ran a group of Finnish and Estonian pimps, who rented apartments, organised transport and kept watch on the victims.

Sexual advertising is prohibited in Finland, and so the site was established in the Netherlands, where no such ban applies.[30]

This was clearly a highly sophisticated operation, using the Internet to advertise its "products", and deliberately isolating its victims. The fact that the chief organisers were already in prison shows the importance of seizing criminal assets. Imprisonment was plainly no check to their activities, and confiscating the proceeds would certainly be a more fitting pen-

[30] Discussions at the Council of Europe Seminar on the Misuse of the Internet led to co-operation between Europol, Eurojust and the Finnish Police on investigating the Netherlands provider's liability in this case.

alty and, perhaps, greater deterrent. The sums that their victims were required to hand over make it clear that they needed to receive a great many clients to keep anything themselves. Indeed, the mentally handicapped victim kept nothing and was, to all intents and purposes, a slave.

Latvia –Estonia – Finland

Another case of Web-recruited victims came before the courts in Latvia. On 24 November 2006, the Judicial Panel for Criminal Cases of the Supreme Court of Latvia upheld the sentence imposed on a number of Finnish, Estonian and Latvian nationals for sending women abroad for purposes of sexual exploitation.

A Finnish national was given an eight-year prison sentence, with confiscation of assets, for trafficking in human beings, sending a person abroad for purposes of sexual exploitation, and attempted procurement. A Latvian national was given a three-year prison sentence, with confiscation of assets, for trafficking in human beings and sending a person abroad for purposes of sexual exploitation.

An Estonian national (a woman) was given a three-year prison sentence (suspended, with one year's probation) for trafficking in human beings.

The sentenced persons were charged with criminal offences by the State Police in February 2004, when an international criminal network, which had sent Latvian women abroad, mainly to Finland and Estonia, for purposes of sexual exploitation, was liquidated in the course of a joint operation by the Latvian, Estonian and Finnish police.

The investigations established that the network had been managed by the Finnish national, who had already been given a seven-month suspended prison sentence for procuring by a Finnish court. He had co-ordinated the network's activities from Riga, where he moved after his conviction in Finland.

The Finnish trafficker was arrested on 31 January 2004, at the Riga Bus Station, while attempting, with the Estonian trafficker, to send another group of women abroad.

Following the arrest of these two people, police in the three countries launched a joint operation, aimed at breaking up the network. In the three countries, they closed and sealed ten apartments where prostitutes in its employ had been operating. The arrested Finnish national had controlled prices and timetables with the help of local accomplices, who visited the exploited women and collected cash from them in each city.

The clients paid €70 (48 lats) for half-an-hour, but the women received only €15-20 (10-13.61 lats). The price per hour was €120 (82 lats), of which the women received €30 euros (20.4 lats).

The Finnish trafficker had posted nude photographs of all the recruited women on the Internet, advertising sexual services. Sexual services were also advertised in newspapers, giving the phone numbers of operators based in Tallinn.

In the course of searches, Finnish police found concealed surveillance cameras and computers, which the Finnish trafficker had used to control the prostitutes, in a number of apartments. Two prostitutes were also arrested.

This case has nothing to do with victim recruitment via the Internet, but it does involve use of the Internet to attract clients. Since using victims' services is prohibited by the Anti-Trafficking Convention, the latter does apply.

Greece

Since November 2006, the Greek police have launched two major and one smaller operation,[31] similar to the above, concerning recruitment of victims for purposes of sexual exploitation.

i. In November 2006 police officers from the Computer Crime Unit found a Web site offering the sexual services of "famous models" worldwide for sums ranging from €250 to €4 500.

   Online, they booked the services of a "model" in an Athens hotel on 24 November 2006 for €450. The officer/client took marked banknotes and met the "model", who came from an East European country. The police confiscated €4 570 euros and 5 100 Czech crowns, and a notebook containing clients' phone numbers and e-mail addresses, as well as the addresses and phone numbers of various European hotels. The woman told them that another East European victim was in the same hotel, working for the same site. The latter handed over €4 800, and both women co-operated with the police on dismantling the network, which had international ramifications. The women had never met its leader, but were required to hand over the proceeds of their "European tour" at the airport of a European capital city.[32] They stated that they had visited three European capitals in the past three weeks, and had taken at least €60 000. The Greek Police passed this information on to In-

[31] Press releases of the Greek Police, Directorate of Security, Crime Sub-Directorate, 25 November 2006 and 13 January 2007.

[32] The press release does not say which.

terpol, and the head of the network was eventually charged with trafficking in human beings, and the site destroyed.[33]

ii. The second case was very similar. Again while surfing the Web, police officers from the Computer Crime Unit found a site offering the sexual services of "models" worldwide for sums ranging from €250 to €900.

They booked the services of two "models" in an Athens hotel on 12 January 2007 for €600. The officer/client again took marked banknotes when he met the two "models", who were from Eastern Europe. The police confiscated €7,300 euros and three mobile phones. The women stated that that they had been coerced into providing sexual services worldwide for a criminal network acting through this site. Digital analysis enabled the police to trace the head of the network, and they passed this information on to Interpol.

iii. A few years ago, another Internet-based network was dismantled in Greece. The French national football coach, who had met a girl whom he wanted to marry through an escort site in Greece, contributed to the operation's success. She revealed that she was a victim of trafficking, and the police found other women, locked in a hotel room.

A frequent problem is that victims trafficked abroad are slow to reveal their plight, fearing that middlemen may kill them.

Of course, it should be said that the police in the first two cases were initially investigating illegal prostitution networks, but this led them to victims of trafficking. This shows that they should be more proactive in searching Internet sites for possible victims.

It should be noted that Article 351 (6) of the Greek Criminal Code (amended by Act No. 3064/2002), which punishes trafficking for purposes of sexual exploitation, defines "sexual exploitation" as "the perpetration for profit of any *indecent act* (meaning *debauchery*), or the use for profit of a person's body, voice or image for actual or simulated perpetration of such an act, or for the provision of work or services aimed at sexual stimulation".

United Kingdom – Operation Pentameter

Operation Pentameter was the first co-ordinated effort to tackle human trafficking on a national scale, and the largest co-ordinated policing op-

[33] Since the criminal proceedings are still under way, the police could say no more.

eration[34] ever carried out in the United Kingdom.[35] Its remit was as follows:

Launched on 21 February 2006, Pentameter was a multi-agency, victim-focused initiative aimed at tackling trafficking in human beings for purposes of sexual exploitation.

Operational activity was co-ordinated across the United Kingdom and involved all 55 Police Forces in England, Scotland, Wales, Ireland and the Channel Islands for the first time ever. The United Kingdom Immigration Service, the Serious and Organised Crime Agency (SOCA), the Crown Prosecution Service and several non-governmental organisations, like Poppy and Chaste, were also actively involved.

As a result, dozens of court cases against alleged traffickers are now in progress in all parts of the country, and hundreds of demand-reduction operations have been conducted in brothels and massage parlours across the United Kingdom. Evidence gathered from Web sites used by prostitutes' clients to swap information suggests that these men have been reading articles on trafficking in national newspapers, and urging others to be on the lookout for trafficked women and share any information they have with the police.[36]

The Operation Pentameter campaign appealed directly to men who used prostitutes to help by providing information on women who were possibly being forced to work in the sex industry. The Crimestoppers number (0800 555 111), which allows informants to remain anonymous, was a central part of this. At the same time, the police advised men who used prostitutes that they risked being charged with rape if they had sexual intercourse with trafficked women, who were forced to work through fear or intimidation – and that providing information was thus in their interest.[37]

During the three-month operational phase, 84 trafficked women and girls were rescued by police in various parts of the country. Of these, 12 were aged between 14 and 17.

Most of these women and girls came from Eastern Europe and the Far East, but South America and Africa were also on the list.[38]

Police visited 515 premises nationwide and made 232 arrests.[39]

Here again, the Internet does not seem to be used to recruit victims, but rather to disseminate information to clients.

[34] http://www.pentameter.police.uk/.

[35] http://www.ukhtc.org/.

[36] Ibid.

[37] http://www.pentameter.police.uk/news.php?id=2.

[38] http://www.pentameter.police.uk/news.php?id=4.

Marriage agencies

Marriage bureaux, often operating online, also play a potentially significant role in recruiting victims; it is no coincidence that many are located in the main source countries, or specialise in providing women from them. The women involved may have to make a substantial up-front payment (€1 600 is one reported figure)[40] – for many, an astronomical sum. This fee alone might well create an element of debt bondage between them and the agency. According to Europol,[41] a simple Google search on Internet yields 10.2 million hits on Web sites which offer such services, together with tours to meet prospective spouses, while a search on modelling agencies yields 7.8 million (although many of these hits probably concern the same sites).[42] It was reported in 2004[43] that content analysis of these agencies' Web sites showed that many of them exploited women sexually by offering such tours, escort services and pornographic photography services. There are also marriage agency Web sites which specialise in vulnerable women, underage children and the disabled[44]. In addition to monitoring use of these marriage bureaux and modelling agencies, the police should thus compile a database of suspect agencies for use by visa-issuing authorities in source countries. People running these bureaux and agencies should also be vetted for previous links with trafficking. According to Europol, people who run online marriage bureaux seem to have close links with those who operate pornographic and exploitative PPV Web sites (if indeed they are not the same).

We need to distinguish between sites which offer mail-order brides (slaves who can be purchased online by credit card), and marriage agency sites which are obviously offering sexual services

One well-known agency[45] (of the second kind) in Greek police records advertises itself as "Greece's biggest and most serious marriage

[39] `http://pubs1.tso.parliament.uk/pa/jt200506/jtselect/jtrights/uc1127-iii/uc112701.htm`. Another operation, Pentameter 2, was planned for January 2007. See the information given the Joint Committee on Human Rights, in connection with its inquiry into human trafficking by the Deputy Chief Constable of the South Yorkshire Police.

[40] Donna Hughes, "The Role of Marriage Agencies in the Sexual Exploitation and Trafficking of Women from the Former Soviet Union", 2004.

[41] Nick Garlick, Europol, presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking, Strasbourg, 7-8 June 2007.

[42] Our personal research turned up only 128 000 such sites.

[43] Ibid.

[44] `http://www.frantana.ru/`; see presentation by Nick Garlick, Europol, at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking, Strasbourg, 7-8 June 2007.

[45] `http://www.kavadas.1000s.gr/`.

agency, working with serious agencies in Bulgaria and Ukraine". It is based in Ioannina in north-western Greece, but works with other agencies in Larisa and Athens, and its representatives also visit Patras weekly (probably to "ship" the "products" abroad!). Cursory inspection of its site reveals that:

- it is aimed exclusively at men;
- it offers so-called "private services". Clients can go to Ukraine for €700, covering transport from Thessalonika, 3 to 4 days' hotel accommodation in a double room (€800 euros for a single room), breakfast and dinner. Alternatively, for €500 euros, the agency brings the woman to the man's home place, where he can offer her Greek "hospitality".

Although the site-owner has past convictions for aggravated soliciting (he promoted, not only adult women, but also minors), the site itself – strangely – still exists.

A second look at the sites of the many suspect marriage agencies makes it clear that they are offering sexual, and not just match-making services.

Look for "marriage agencies in Albania" on Google, for instance, and the first sites you find are one which is obviously not a marriage agency, but is offering the sexual services of women from Odessa (Ukraine);[46] and one which operates from Latvia, and whose nature is revealed by its banner: "Welcome to passion – sexy personal services for passionate singles".[47]

Another suspect site[48] advertises "ladies from Asia, Africa, Russia & Latin America for dating & marriage". Also suspect is an Indian site[49] which operates only between India, the United States, the United Kingdom, Australia and Canada (the girls are obviously Indian, and are "advertised" to "grooms" in those countries). It contains photos of women only, and entering a "groom" search produces no results. It offers free chat with the girls, promising privacy and claiming that it adds over 5 000 new profiles every day.

The 2003 report tried to show a connection between marriage agencies operating in the former Soviet Union and trafficking in human beings. However, the mere fact that 120 000 women were counted on these sites does not mean that they were recruited to be trafficked (the report's use of the phrase, "women *recruited* by marriage agencies", gives

[46] http://www.odessajudies.com/contact.htm.

[47] http://passion.com/.

[48] http://www.MyForeignBride.com/.

[49] http://www.simplymarry.com/.

the impression that this means recruited victims of trafficking in human beings).[50] Nor does the fact that "of the 219 marriage or introduction agency Web sites, 78 of them offered tours to meet women"[51] prove that those agencies are active in trafficking. These are indications only, which is why the report, although it counts marriage agencies carefully, cannot say how many of them have been operating illegally.

To some extent, it is true that "due to poverty, high unemployment, and a belief in Western utopias, many women want to go abroad, and NGOs report that in many cases, once a woman decides the solution to her problems is to go abroad, she will try every agency or strategy, regardless of the risk". However, this does not give us the true measure of the recruitment of victims of trafficking in human beings via marriage agencies. Cultural differences, which make recourse to marriage agencies more popular in some countries than in others, must also be considered.

The 2003 report seems to be portraying marriage agencies as recruiters, but it also says: "It is difficult to know how many of these agencies are providing the services they claim of selling addresses, and how many are involved in activities that meet the criminal definition of trafficking in women for the purpose of sexual exploitation. Certainly, most are promoting the sexual exploitation of Eastern European women by Western men".

I repeat, we must distinguish prostitution from sexual exploitation; not all prostitutes are exploited. Poor living conditions in their own countries and a desire to emigrate are not, on their own, conclusive evidence of sexual exploitation.

I would not say that it is *certain* that these agencies *promote sexual exploitation* – simply that it is *likely* they are doing so. This is because we lack vital information: to establish trafficking in human beings, we need proof of coercion, deception, threat, etc., making the victim act against her wishes. In most of these cases, however, we know nothing of the actual circumstances which led the women involved to subscribe to, or collaborate with, these agencies.

Job sites which exploit recruits

Recruitment agencies are often the first link in the trafficking chain. If there are no clear regulations, the recruitment industry may mushroom, adopting the guise of (for example) travel/tourist, modelling and enter-

[50] 2003 report, p. 48.

[51] Loc. cit., p. 51.

tainment, and au-pair agencies. They operate in the grey zone between organised crime, illegal employment and sub-standard work. These practices often escape state regulation and the normal labour inspection routine.

ILO research[52] in Moldova, Ukraine and Russia has shown that only a very low percentage (4-12%) of migrants use registered employment services. Many start by contacting recruiting or travel agencies on their own initiative, in the hope of finding work abroad. Usually, it is only when they reach their destination that the elements of coercion and deception are revealed, and they become victims of trafficking within the meaning of the Palermo Protocol.

According to the NGO, La Strada – Poland, the Internet has, in the last ten years, become the tool most used by Poles in search of work abroad. Only 40% of Poles have Internet access, but 90% of those who found jobs abroad found them via the Internet. La Strada – Poland estimates that 30% of the trafficking victims who come to its notice were recruited via the Internet.[53]

Most of these victims were recruited on the Web – especially via dating sites or sites offering various kinds of service (e.g. plumbers, locksmiths, goods suppliers, etc.). Some posted advertisements themselves, e.g. "I am a nurse, looking for employment in England,"[54] and some, who were already sex-workers, were turned into victims by traffickers looking for women to work as prostitutes abroad.

It is thought that most of the people who prefer to look for work in chat-rooms and Web forums lack the qualifications needed to go through the professional job agencies which deal with "ordinary" job-seekers.[55] That is why they try to make contact via the Internet with people who do not ask for certificates and references.

Examples of recruitment:

Italy – Poland (Operation Terra Promessa)

Joint Italian/Polish investigations recently led to the dismantling of a Polish transnational criminal organisation which exploited victims re-

[52] According to Anne Pawletta, Special Action Programme to Combat Forced Labour, ILO, Geneva, in her presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

[53] Joanna Garnier, La Strada – Poland, presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

[54] See below, page 49, in our classification of victims, "Victims who contribute to their victimisation".

[55] Joanna Garnier, *La Strada – Poland,* loc.cit.

cruited in Poland as cheap labour in Italy. The main recruitment tool was the Internet, and Polish police identified an employment agency Web site as a key part of the process.

The criminal operation was steered from the Apulia region in Italy. The investigations were conducted jointly by the *Carabinieri* and the Central Trafficking in Human Beings Unit at police headquarters in Warsaw.

The criminal organisation was traced through statements made by victims and relatives to the Polish Consulate in Rome, with which the Italian and Polish police co-operated usefully, setting up a common database. A Polish criminal network was active in the province of Foggia, where it organised and exploited the labour of Poles who had come to work in various work camps in Italy.

The traffickers operated as follows:

- attractive work offers were used to decoy and recruit the victims;
- they were then transferred, and fees collected for go-between services and travel;
- accommodation was provided, and the victims were effectively enslaved, and their labour exploited;
- misled as to their earnings, they were held in perpetual debt bondage;
- to stop them escaping, the work camps were kept under armed guard.

The advertisements were published in newspapers and on the Internet.[56]

The judicial proceedings were conducted jointly, and the investigations under the supervision of the Anti-Mafia Prosecution Office in Bari.

The charges were: criminal conspiracy to commit slavery, trafficking in human beings and exploitation of labour, with the transnational organisation as an aggravating circumstances.

The Prosecutor's Office in Bari issued warrants for the arrest of 27 members of the organisation responsible for trafficking and enslavement. Nine of these warrants were served in Poland via the "European Arrest Warrant", a further 22 warrants were issued in Poland. More than 100 victims were rescued and assisted by the Polish Consulate and NGOs.

This operation generated an ongoing, direct exchange of information between the investigating police authorities. Each appointed a contact person to receive and transmit the data needed for investigation at both ends, with requests for information being formally channelled through Europol and Interpol. Phones were tapped to keep track of members of the network in Poland (when victims were being recruited

[56] `http://www.anonse.pl/`.

and transferred, and money collected). In Poland too, hundreds of victim reports are awaiting examination, including one alleging rape. There were also suspicious deaths – initially treated as suicides or accidents – among the Polish victims.

However, the landowners who employed these workers illegally seem merely to have been fined, although they had also - according to the Convention – made themselves guilty of trafficking by directly exploiting their labour.

Italy

According to the Italian NGO, *On the Road,*[57] the statements of people assisted by NGO social workers and psychologists suggest that the Internet is not extensively used as a means of recruitment in Italy. Nearly 6 000 trafficked people who had made used of the Italian social assistance and integration programme were granted residence permits for humanitarian reasons between 2000 and 2006, and the Internet had been involved in recruiting only a few of them:

- 2 cases reported in Florence: Two women from Kyrgyzstan came to Italy with the help of their "impresario", who found them nightclub jobs through a Web site, which was supposedly legal, and used by nightclub owners to exchange information and job-offers. They were exploited, and eventually managed to escape.
- 2 cases reported in Pisa: Two women, Polish and Russian, came to Italy to marry Italians they had met on a chat-line. One actually married, the other did not – but both were treated as slaves, and kept under lock and key in the men's houses. They finally managed to escape and contact the social services, and were eventually allowed to stay for humanitarian reasons.

These cases have no apparent connection with organised criminal groups. However, this is no proof that the Internet is not used as a means of recruitment. At most, it might indicate that:[58]

- Italian NGOs and local authorities have not so far encountered trafficked persons recruited via the Internet;
- persons trafficked to Italy come from countries where the Internet is still not widely used;
- persons trafficked to Italy are not Internet-literate.

[57] Isabella Orfano, *The role of civil society in preventing and combating the misuse of the Internet for the recruitment of victims of trafficking in human beings*, presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7 June 2007.

[58] Isabella Orfano, *loc. cit.*

According to key informants, the Internet does not seem to be used at the recruitment stage, but at the exploitation stage of the trafficking cycle, when the victims are already in Italy. For instance:

- 2 cases reported in Lecce: Two women, from Colombia and Romania, were recruited through the “traditional” channels and brought to Italy. Once in the country, they were forced to contact clients via the Internet, using the “Internet Points” which have mushroomed in the last few years.
- 2 cases reported in Milan: Two women from Brazil were recruited through the “traditional” channels and, once in Italy, forced to contact clients via the Internet.

Some Italian experts[59] think it possible that quite a large number of people are trafficked via the Internet, but are hard to reach because they are exploited in venues which social and outreach workers do not usually visit (i.e. streets and apartments). Others believe that the comparatively limited social and cultural “capital” of the trafficked people they work with makes it hard for them to use the Internet.

Europol

Europol’s[60] records include one case of Internet recruitment, in which the female owner of a Web-based modelling agency in Lugansk (Ukraine) was arrested in November 2006. She recruited 14- to 17-year-old girls on spurious modelling contracts, and trafficked them to the United Arab Emirates and the Seychelles, where they were forced to work as prostitutes.

Europol now has a wide-ranging Analysis Work File on action against trafficking, which it has set up in part-fulfilment of its obligations under the European Union Action Plan on trafficking in human beings. It intends to have priority areas in this work file, which is currently focused on Bulgaria, while Romania and labour exploitation in general are proposed as other focal points. The aim is to assist member states in their investigations by providing the co-ordination and analytical support they need to realise achievable, short-term objectives.

IOM’s cases

IOM’s Counter-Trafficking Division uses an operational tool, the Counter-Trafficking Module (CTM) database, to help manage the victims of trafficking in human beings whom it assists directly. According to IOM

[59] According to Isabella Orfano’s presentation, *loc. cit.*

[60] Presentation by Nick Garlick, Europol, at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking, Strasbourg, 7-8 June 2007.

data, between 2004 and 2007, 24 victims entered on the CTM explicitly stated that they had been recruited for purposes of sexual and labour exploitation through fraudulent job advertisements on the Internet[61] (domestic servants, waitresses, dancers, etc.). Aged 14 to 30, they comprised 22 women and 2 men – 21 from Ukraine, 2 from Belarus and 1 from Moldova. Most of the recruiters were Ukraine-based, and the main destination was the United Arab Emirates (for 9 victims); most of the others were intended for Council of Europe member states (Cyprus, Czech Republic, Germany, Russia, Turkey, Poland, Greece), and two for Egypt.

One (from Belarus) received an Internet job offer from a Russian company based in St. Petersburg, but was trafficked to Egypt for labour exploitation instead. There, her passport was taken from her, and she was forced to work 20 hours a day, 7 days a week, forbidden to go out or make any human contact, and fined when anything went wrong. In addition to all this, she was beaten by the supervisor. Eventually, she managed to make friends with a local, who helped her to retrieve her passport. Although IOM helped her to find accommodation and reintegrate, she was unwilling to co-operate with the authorities and preferred to go home.[62]

Clients

Clients are the second type of Internet user. They should be distinguished from traffickers, although – in the field of pornography – many paedophiles create their own sites, exploiting their victims directly. In such cases, they can be both traffickers and consumers. Very often indeed, they create pornographic sites for pleasure, rather than profit – a possible source of problems in countries where child pornography is punishable only when produced for profit (e.g. Greece, Article 348A of the Criminal Code, currently scheduled for review).

It is obvious that clients contribute to trafficking in human beings, since it, and the sex market in general, would not exist without them. the Internet allows them to stay safely in their homes and preserve their anonymity, giving them the feeling that they can wallow in any perversion online without fear of detection. According to the 2003 Report, "men who buy women and children for the purpose of sexual exploitation post information about their experiences in newsgroups and on the Web.[63] They often reveal a great deal about themselves – who they are, their

[61] IOM Counter-Trafficking Module Database, 2007.

[62] Ibid.

[63] 2003 report, p. 36.

attitudes to women, and how they treat them. Often, their accounts of things they have done hint at their use of trafficked women.

Most of the men who use the Internet to find women trafficked for purposes of sexual exploitation (and to share their experiences) seem to be travelling businessmen, people reporting on local prostitution, and students. In Greece, there is even a group of doctors sharing this kind of information. Some say that they consult newsgroups or Web sites before travelling and even print out information to take with them. Some write about their experiences as a way of reliving them, including graphic details which make it clear that this is their way of reviving past pleasures.

Under Article 19 of the Council of Europe Convention, using the services of a trafficked victim is a criminal offence. It must be emphasised that the fact of its possibly being hard to prove makes no difference.[64]

At this point, we should note that some of the fraudulent advertisements posted on the Internet are aimed, not just at potential victims, but also at clients (in a different way). For instance, Web sites which include nude photographs of women (some of whom may not even know that their pictures have been posted)[65] can affect both:

a) Women who never intended to let themselves be advertised as prostitutes are identified – stigmatised – as such. In these cases, the only exploitation they suffer is exploitation of their image.

b) Clients are deceived as well, since they may pay for sexual services which are never provided. In such cases, the client is the direct victim, and the woman whose picture has been published is the indirect victim.

In 2006-2007, a three-country study (Greece, Cyprus, Germany) on the demand side of trafficking was carried out as part of AGIS,[66] a European project run by the University of Thrace. This showed that most clients are unaware that trafficking in human beings is a crime, while a large percentage do not care about the girls, but only want to get the services they pay for.

Potential victims

Potential victims are the third category of user. While respecting the classification used in the 2003 Report on "different types of victim",[67] we

[64] On the demand side of trafficking, see: Andersen, Bridget and O'Connell Davidson, Julia (2004), *Trafficking – A Demand-Led Problem?*, Save the Children, Sweden.

[65] 2003 report, p. 30.

[66] Project JLS/2005/AGIS/123, co-financed by the European Commission.

[67] 2003 report, p. 99.

shall make just one more distinction – between victims who are totally innocent, and victims who contribute to their victimisation.

Totally innocent victims

As we use the term, “totally innocent victims” are:

– victims seeking “innocuous” sites, who stray onto others which are far from innocuous, e.g. young people (children) lured onto pornographic sites posing as cartoon sites; job-seekers decoyed by fraudulent employment agencies (using Web sites as they might use press advertisements); and

– victims using potentially risky sites, e.g. “chat-rooms”, dating sites, marriage agency sites, without being aware of the dangers (perhaps as a result of youth and/or innocence).

Victims who contribute to their victimisation

These include people who, knowing the risks, continue to use potentially dangerous sites, such as marriage agency sites, either because:

– they believe that nothing “bad” will happen to them (they overestimate their own intelligence or underestimate the traffickers’ cunning), or

– their situation is desperate, and they knowingly accept the traffickers’ exploitative tactics in the hope of escaping it.

Summing up this section, we may note that traffickers use the Internet either to recruit their victims via employment, marriage and dating sites, and chat-rooms, or to advertise the services of victims already recruited in traditional ways, mainly in their home places.

Internet users include traffickers, clients and victims. Clients should be seen as a user sub-category, and not as the users in general. Victims can be divided into those who contribute to their victimisation by knowingly using dangerous sites, and those who use seemingly harmless sites in all innocence.

More victims seem to be recruited for sexual exploitation, but many are also recruited for labour exploitation – especially in countries where the Internet is widely used by people seeking work abroad (e.g. Poland). Cultural differences are another relevant factor, making the Internet more appealing in some countries than others.

Factors that impede recruiting victims of trafficking in human beings via the Internet

The Internet recruitment of victims of trafficking in human beings is subject to various inhibiting factors, such as limited technological infrastructure in member states regarded as source countries, as well as cultural differences affecting, not just Internet use in general, but also its use as a contact-making, job-finding tool, etc.

Limited telecommunications and Internet infrastructure as an obstacle to increased recruitment

The importance of the role played by Internet advertising in recruiting women has been disputed.[68] Some people believe that very few girls/women have Internet access in the source countries, whose economies have not supported Internet expansion and generalised computer literacy. This is particularly true in the impoverished rural areas where many victims are recruited, and where the Internet cannot be effectively used for that purpose. Other people suggest that nearly all girls/women can access the Internet, and use to look for work abroad, in schools and libraries. According to the 2003 report, the most vulnerable potential victims in Latvia were young women from 19 to 22 years old, living in extreme poverty, primarily in the southern and Russian parts of the country, where unemployment is high, and prospects are poor.[69]

[68] 2003 report, p. 24.

[69] Ibid.

Nonetheless, we should recognise that the absence and cost of the necessary technological infrastructure have so far had significant restraining effects on the growth of victim recruitment via the Internet in source countries.

Internet use in European Union member states

Statistics on Internet use[70] indicate that Europe, with 12.3% of the world's population, has 39.8% Internet penetration, or 27.9% of total world use.

According to a European Union survey[71] of 27 000 representative households, published on 27 April 2007, nearly 20% of European households buy all-in telecom packages.

Almost 30% now have high-speed, broadband connections to the Internet, and mobile phones are increasingly taking over from fixed lines. 17% of Europeans with home Internet connections use them for Internet telephony.

- Broadband's popularity is increasing rapidly in the European Union (28%, up 6%) while narrowband is declining (12%, down 3%). Most households access the Internet via ADSL (53%, up 4%), and 34% of broadband connections are wireless.
- 17% of Europeans with home Internet connections report that they use them for phone-calls. The percentage figure is twice as high in the new member states.
- As more households connect to the Internet (42%, up 4%), reasons for not doing so are increasingly non-financial, with 45% stating that they simply are not interested.
- 28% of Europeans have had significant problems with spam, viruses and spyware – which highlights the need for increased European Union and member state action against illegal practices.[72] Overall, most have installed antivirus (81%) and antispam (60%) software.

According to another European Union survey on Internet use, carried out in 2006 by Eurobarometer[73] and chiefly aimed at children and parents:

[70] See Appendix 1, page 139.

[71] The full text of the European Union survey can be found at http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/studies_ext_consult/index_en.htm#2007.

[72] On 27 November 2006, the Commission called on all the regulatory authorities and stakeholders in Europe to step up the fight against spam, spyware and malicious software. It insisted that, although Internet safety had been on the political agenda for some time, national authorities must do more to prosecute illegal online activities.

Half the parents state that their children, aged 17 and younger, use the Internet. Nearly two in ten report that their children have encountered harmful or illegal content online (18%).

This figure is slightly higher in the 10 new member states than in the 15 others (21% v. 17%).

In the four accession and candidate countries, only 12% of parents state that their children have encountered harmful or illegal content. Most parents (48%) in these countries simply do not know. In the 10 new member states, 28% also have no opinion on the matter.

Analysis of the socio-demographic profiles of parents/guardians shows that Internet filtering tools are most widely used by people in the 25-39 age-group (56%), advanced Internet users (55%) and people living in large towns (50%). They are least used by people who left school below the age of 16 (37%).

Comparing Internet use with mobile phone ownership, over a third of respondents on average said that their child had a mobile phone (36%) – suggesting that this is less used to communicate by children than the Internet.

However, in Cyprus, Greece, Latvia, Lithuania, the Czech Republic, Italy, Austria and Portugal, mobile phones are used more frequently than, or as frequently as, the Internet.

There are also discrepancies between age-groups: nearly all parents/guardians of children in the 16-17 age-group say that their children have mobile phones (87%), which are used as frequently as the Internet by this age-group. The great majority of 14-15 year-olds also have mobile phones (80%). Mobile-phone ownership is less widespread among the under-12s, but almost a quarter (23%) of 8-9 year-olds have them.

Overall, girls and boys are equally likely to own mobile phones (37% v. 36%). However, girls tend to be slightly younger when they acquire them, and a significantly higher proportion of girls in the 16-17 age-group have them. In the four accession and candidate countries, about one child in five uses the Internet (21%), and slightly fewer have mobile phones (18%) – which is lower than the European Union average. However, there are broad differences between the four accession and candidate countries. Mobile phone ownership is quite widespread in Croatia, and comparable to that in several European Union member states. In Turkey, the proportion of children who own mobile phones or

[73] Eurobarometer, *Safer Internet,* Field Work Dec. 2005-Jan. 2006, published May 2006. The Safer Internet survey, which is part of the European Union's Safer Internet Programme, was carried out in the twenty-five European Union member states, the two accession countries and the two candidate countries, from 7 December 2005 to 11 January 2006.

use the Internet is lower than in the other three countries, and in any of the European Union member states.

Sixty percent of parents whose children access the Internet have set no rules on using it.

The top rules mentioned by parents concern "forbidding access to certain Web sites" (55%), and "controlling time spent on the Internet" (53%). Less frequent are rules on "not allowing children to meet Internet contacts in person" (35%) and "not allowing children to download music or films" (19%).

Nearly half (48%) the parents say that tools to filter or block access to certain sites are activated when their children use the Internet, and about a quarter (24%) sit with their children when they go online. This protective measure is particularly common among parents of children aged six or under, 69% of whom state that they regularly sit with their children.

Two European parents in three believe that their children know what to do if anything they encounter on the Internet makes them feel uncomfortable (66%).

44% of parents would like more information on ways of protecting their children against illegal or harmful content and contacts. There are extreme differences between European Union member states, with scores ranging from 29% of Danish respondents who feel they need more information to 86% of Greek respondents. The desire for more information is most widespread in the four accession and candidate countries (64%).

Respondents chiefly want schools (36%), Internet providers (31%) and the media (21%) to supply information on safer Internet use. On average, half know where, or to whom, they can report illegal Internet content (52%). This applies to six out of ten respondents who had used the Internet just before the survey, and four out of ten who had not used it in the month before the survey. In the 15 "old" member states, awareness has increased significantly since the last survey. In autumn 2003, 41% of respondents knew where, or to whom, they could report illegal content, while the figure in this survey is 54%.

Awareness levels are significantly lower in the accession and candidate countries than in the member states. On average, just over one person in five in those countries would know what to do if confronted with illegal content on the Internet (22%). Analysis shows significant national variations in the percentage of respondents who know that hotlines exist for that purpose. Awareness is markedly higher in Belgium

(18%), the Netherlands (13%), Austria (12%) and Slovakia (10%) than in the other European Union member states.

The same survey shows that socio-demographic profiles are a strong indication of Internet use, with age, education and occupation as the main factors. The likeliest users are students and managers are, and the least likely pensioners and people who left school below the age of 16.

Less significant factors are household size (the larger the household, the likelier its members are to use the Internet), political orientation (people on the left of the political spectrum are likelier to use it than those in the centre or on the right) and location (people in large towns are likelier to use it than people in villages).

Internet use is considerably less common in the accession and candidate countries than in European Union member states. On average, only one respondent in five in those countries had used it in the month preceding the survey (20%).

The survey also shows that most people use the Internet at home, with 38% of respondents giving this as the place where they had used it in the previous month. Nearly one in five (18%) had used it at work in the previous month, and 7% had done so at school, university or some other study centre. Places like Internet cafés had been used by 5% in the month before the survey. It appears that 57% of students use the Internet at educational establishments, although they are likelier to use it at home (68%). Since few students have jobs, the percentage of those using it at work is negligible (7%).

In the 10 new member states, the percentage of children thought to use the Internet has risen from 45% in 2004 to 48% in the latest survey. In the 15 ‘old’ member states, the percentage has not changed significantly since 2003, and now stands at 51%.

The figure is considerably lower in the accession and candidate countries (21%).

By comparison with previous surveys, the percentage of children reportedly using the Internet rose more than 10 points in Slovakia, Belgium, Malta and Cyprus, with significant increases also recorded in Greece, Lithuania, Estonia and France. Conversely, a significant drop in levels of Internet use among children was recorded in Spain (-9 points).

Overall, boys are slightly likelier to use the Internet than girls (52% v. 48%), and tend to use it at an earlier age. 37% of boys in the 6-7 age-group are users, as compared to 30% of girls, and the gap remains until the age of 9. Boys in the 14-15 age-group are again likelier to use the Internet than girls, but there are no differences between boys and girls in the 16-17 age-group.

Telecommunications and Internet infrastructure in relation to Internet use in other Council of Europe member states

As far as other Council of Europe member states are concerned, the Centre for Democracy and Technology carried out a survey of telecommunications and Internet infrastructure in 17 south-east European countries in 2000. This, of course, is already outdated, given the speed with which technology develops. However, taken in conjunction with the 2007 figures[74] on Internet use, it does at least give us some idea of the present situation.

Albania

In the 2000 report, Albania ranked lowest in south-eastern Europe. The actual number of Internet users was unknown, but was certainly quite small.[75]

In 1996, Albania, with its population of 3 330 754, had approximately 63 900 telephone lines. At 1.74 lines per 100 people, this was eastern Europe's lowest level. Penetration at that time ranged from 2.75% in urban areas to 0.22% in rural areas.

According to the statistics, there were 188 000 Internet users in 2007 (0.1% of the European total), with 6.1% penetration. However, use increased by 7 420.0% between 2000 and 2007.

Bulgaria

At the time of the report, telephone penetration was among the region's highest, but the technology was obsolete: party lines were common, and very few local exchanges had been converted to digital technology. In 1996, there were over 2.6 million main lines (about 32 per 100 population), and more than 10 ISPs Internet Service Providers) with international connectivity.

Many organisations had high-speed international connectivity and sold their unused capacity, one being the Bulgarian Industrial Association.[76] In mid-1999, BTC charged about $80 for ISPs to add a new phone line. The average charge for dial-up Internet access ranged from $10 per

[74] See Appendix 1, page 139.

[75] Central and Eastern European Networking Association, (CEENet): http://www.ceenet.org/ database/country/albania.htm. The ITU estimated that there were 1000 Internet users in 1996. *ITU Report 1998* and Centre for Democracy and Technology: http://www.cdt.org/international/ceeaccess/countrydetail.shtml#albania#albania.

[76] http://www.bia-bg.com/.

month (night-time access only) to approximately $15 per month (unlimited access). The latter charge was low in Western terms, but the average wage was about $120 per month, and so Internet access was beyond the average citizen's means.

According to the statistics, Bulgaria's Internet users accounted for 0.7% of the European total in 2007, and penetration stood at 28.7% of the population (2 200 000 from a population of 7 673 215); use increased 411.6% between 2000 and 2007.

Bosnia and Herzegovina

Bosnia and Herzegovina recorded Europe's most startling increase in Internet use between 2000 and 2007. With a population considerably smaller than that of Bulgaria (4 672 165), and 0.3% of Europe's total users (803 400), use increased 11,420% during that period, while the Bulgarian increase was only 411.6%.

Belarus

With a population of 10 409 050, Belarus had 2 128 000 phone lines in 1996, and a density rate of 21 per 100. Despite significant growth in recent years, telephone service was still inadequate to meet either business or private demand. By the end of 1994, Belarus got its first permanent Internet connection via a dedicated line from Minsk to Warsaw, supported by the Polish Academic and Research Network (NASK). As of March 1999, however, it had some 1 000 hosts only and, by one estimate, a mere 6 000 users. Set-up charges, monthly fees and connection time charges made Internet access very costly, even for those who could afford computers. (The average monthly wage was approximately $60.) As a result, Internet use was quite low in Belarus, by comparison with other east European countries. The figures for 2007 show, however, that use in Belarus – with 35.1% penetration, representing 1.1% of all European users – increased by 1 785.8% between 2000 and 2007.

Moldova

In 2000, Moldova (population: 4 457 729) had 593 300 phone lines, or 14 per 100 people.

Permanent Internet access arrived in 1995, via a leased line to Bucharest. In 1998, there were seven ISPs in the capital, Chisinau (the only city with full Internet access at the time). The relative inexperience of ISPs like MegaDat and Moldnet left them prone to incident – if not actual disaster. One such occurred on 14 July 1998, when a hacker broke into the Moldnet server.[77] High telephone charges were one major obstacle to wider access. Access to e-mail and other Internet services remained very limited, even at the National Academy institutes. Universities and secondary schools had limited access, if any.

Up to 2000, there were still several major obstacles to improved Internet connectivity in Moldova:

- Poor telecommunications infrastructure. Most lines were analog, not digital;
- High phone-call charges, and the high cost of telephone lines;
- Insufficient availability of telephone lines for private use;
- The high cost of computer equipment;
- Language problems – the preferred languages in science were still Russian and Romanian, not English;
- Dependence on international funding, which made long-term planning difficult.

Nonetheless, Internet use increased by 2 100% between 2000 and 2007, and 14.8% of Moldovans are reportedly now using the Internet.

Romania

In 1996, Romania (population: 22 395 848) had 3 161 200 phone lines, with 14% teledensity, as compared with 10% in 1990. The Ministry of Communications estimated that penetration in rural areas was only 3%; in 1997, some 2 000 villages had no phones at all. Since most Romanians lived in rural areas, this was particularly important. In 1999, Romania had at least 11 major commercial ISPs, about half with their own backbone networks. Rom Telecom, its dominant, formerly state-owned telephone service provider, was partly privatised in November 1998, when the main Greek operator acquired a 35% stake in the company. Under its license, Rom Telecom had a monopoly of local, long-distance and international telephone services and network infrastructure until 31 December 2002.

In 2004, 60% of Romania's population reportedly had access to the Internet, while the cable TV and Internet charge was about $9.

In 2007, there were 4 940 000 Internet users (23.4%) – 1.5% of the European total. Use increased by 517.5% between 2000 and 2007.

Russia

In 2000, when Russia's population stood at 146 861 022, 1.3 million households had Internet access, and the Internet was also widely used by NGOs, academics and businesses. Ominously, however, the government

[77] Oxana Comanescu, "Country Report: Moldova", Budapest Conference (September 1998).

had openly proposed imposing surveillance requirements on ISPs, many of which were already co-operating with it on unregulated monitoring.

The greatest obstacle to widespread use of the Internet was Russia's inadequate telecommunications infrastructure, which was not expected to meet Western standards for many years. Although significant progress had been made, there were not enough phone lines, and existing lines were mainly analog, slow and poor in quality. In 1996, 8.8 million applications for lines were still pending, and the estimated waiting time was over 10 years.

In March 1999, Russia had only 180 721 host computers (linked to the global network) for some 145 million people. By comparison, Finland, with a population of only 5 million, had 467 954 host computers.

In 2000, the hourly charge for on-line connection to the Internet via ordinary public phone lines was $1.50 to $3. Separate lines for connection to the Internet could also be leased from ISPs. The bill for this varied from $400 to $1,500 per month, in addition to a one-off registration/installation fee. VAT was also charged monthly at 20% on 64 Kbps leased lines – so the cost of even the cheapest Internet connection was well above the average monthly wage.

Today, Russia has some 28 000 000 Internet users (19%), or 8.7% of Europe's total, and use increased by 803.2% from 2000 to 2007.

Ukraine

In 1998, Ukraine had approximately 350 Web-servers and 400 virtual Web-servers, over 30 000 domains, over 100 000 active users, and 103 Internet Service Providers. 30% of all users lived in Kyiv, and another third in the five largest cities (Dnepropetrovsk – 2%, Kharkiv – 10.5%, Donetsk - 8%, Odessa – 4%, Lviv – 3%). Thus, one in every hundred residents in Kyiv and Dnepropetrovsk had Internet access, while the average for the whole country was one in five hundred. Internet development was also limited by the high cost of access. Many providers charged $10-$20 per month for services, and $1-$3 per hour. Prices also went much higher, but dropped sharply in 1999.

Another limiting factor was the monopoly exercised by Ukrtelecom, a state company which controlled over half the international communications channels, and nearly all local telephone services. Utel, the long-distance and international carrier, was 49% owned by a foreign consortium, and 51% owned by Ukrtelecom. Ukrtelecom's subscriber charges for basic telephone services were 6 to 8 times higher than those in, for example, the Czech Republic.

In 2007, there are 5,278,100 users (11.5%), or 1.6% of Europe's total, and use has risen by 2,539.1%.

From the above, it appears that, over the past decade:

1. some countries have managed to keep pace with technological developments;
2. some have caught up on other countries, or at least shortened the distance between them;
3. some are still far from catching up.

For instance, in 2007, when Iceland had Europe's highest user rate (86.3%), and 61% of Germans were users (15.7% of the European total), Albania still had the lowest penetration rate (6.1%). Among countries considered source countries for victims of trafficking in human beings, Internet use ranges from 6.1% (Albania), through 11.5% (Ukraine), 14.8% (Moldova) and 35.9% (Lithuania) to 51.8% (Estonia).

National and cultural differences in the use of the new information technologies

National and cultural differences affecting use of the new information technologies, and of agencies, are another factor which reduces the Internet's effectiveness as a recruitment tool.

A survey carried out by *Metron Analysis*[78] in 2000 showed that 32.6% of Greeks were active Internet users (the 2007 figure is 33.5%). Of those, 75.5% were frequent users (once or twice a week), and of those again 51.2% were Websurfers. Most (42.2%) were connected from home, and 25.6% from work. A substantial percentage (20.6%) used Internet cafés. Most users seem to be young (45.5% in the 18-24 age-group). An increasing number (36%) of men use the Internet on a daily basis, while among women the figure is 27.7%. Of total Web users, 25.5% have university degrees, and 12.4% live in large cities.

Chat-wise, street-wise, a study published in March 2001 by the Internet Forum in the United Kingdom, reported that five million young people were connected online in Britain, and that 25% of them used "chat-rooms" (the 2007 figure is 62.3%). Adolescents, particularly young girls in the 16-17 age-group, are in serious danger of "online seduction". As the 2003 report also notes, while girls tend to outnumber boys among United Kingdom chat-room users, 60% of users in the United States and Canada are male.[79]

In Estonia, where Internet use appears to have risen to 51.8% in 2007, a survey carried out in 2004 by the International Organisation for

[78] http://www.metronanalysis.gr/web/html//index.asp?language=greek&page=surveys.

[79] 2003 report, p. 25.

Migration[80] indicated that 30% of respondents would consider using the Internet to find information on jobs abroad (which does not mean that they actually do).

Also relevant is the fact that, while using marriage or dating agencies to find partners is uncommon in some countries, e.g. Greece or Spain, it is perfectly normal in others, e.g. France. In Russia, too, this seems very popular, just as looking for work on the Internet is very common in Poland.

According to the 2003 report, although some countries reported that the phenomenon had not been widespread up to 2002, particularly owing to the relatively small number of computer-users, most underlined the rapid increase in use of NIT (New Information Technologies) for purposes of pornographic/sex-related trafficking in human beings over the previous five years.[81]

The chief reasons given included:

- Increasingly generalised Internet access;
- User anonymity;
- Pornographic and related material can be lucratively marketed on the Internet without any major investment;
- A lack of appropriate laws or policies to combat this phenomenon;
- The yearly increase in the number of users;
- The affordable cost of services.

Conclusion of Part I

From all we have said so far, and from the many police operations aimed at dismantling networks of traffickers active in recruiting victims via the Internet and mobile phone in various member states, we can see that use of the new technologies in trafficking for purposes of sexual or labour has become a serious problem.

Traffickers can use the Internet and other new technologies in various ways, e.g. to deceive and lure victims, and to attract clients by advertising sexual or other services provided by those victims. Victims recruited in traditional ways can also be forced to contact clients online. Without knowing it, some victims contribute to their own victimisation.

Users can be divided into traffickers, who set up recruiting sites themselves or with the help of others, and clients. More than half of these illegal sites operate outside the Council of Europe's member states, and particularly in the United States.

[80] This can be downloaded at `http://iom.fi/files/books/trafficking_in_estonia_eng.pdf`.

[81] 2003 report, p. 14.

It is important to note that telecommunications infrastructure and Internet use are not uniform in all the member states, in spite of rapid progress and increased use in the last few years. Nevertheless, we can assume that recruitment would be higher if conditions in source countries were suitable.

However, until we have a full picture of Internet infrastructure in the potential victims' home countries, and until we also have reasonably clear user profiles (How many users are there? How many are frequent users? What do they use the Internet for? e.g. how many use it to look for work abroad or find partners?), broken down by age and gender, we shall not be able to draw conclusions on the real impact of the Internet on the recruitment of victims of trafficking in human beings for sexual or labour exploitation abroad.

It is true that many writers on the subject overreact, and tend to confuse prostitution with sexual exploitation. For example, the Hughes report says: "Sex tourism, bride-trafficking and prostitution are different forms of sexual exploitation. An examination of advertisements on the Internet reveals the links between these types of sexual exploitation, and enables us to see that the agents use women in any way that is profitable."[82]

I do not agree. It is true that the borderline between prostitution and sexual exploitation is not very clear, but comments like this may simply focus the attack on prostitution, especially when they are linked with conclusions like the following: "Western countries, that benefit commercially from the Internet industry ... do nothing to impede e-commerce and its partnership with the sex industry."[83] Accepting this line would mean banning all sexual advertising, on the Internet or any other medium.

I would like, once again, to insist that we must make an absolute distinction between prostitution, whether legal or illegal in a given member state, and sexual exploitation. Prostitution is not necessarily exploitation, although it can lead to exploitation, either sexual and/or financial. If adult persons freely choose to make a living from prostitution in countries where this is legal, there is no problem.[84] If it is illegal, they are regarded as engaging in a criminal activity, but not as being exploited. If

[82] D. Hughes, "Use of the Internet for Global Sexual Exploitation of Women and Children": http://www.uri.edu/artsci/wms/hughes/.

[83] Donna Hughes, "Globalization, Information Technology, and Sexual Exploitation of Women and Children", *Rain and Thunder – A Radical Feminist Journal of Discussion and Activism,* Issue #13, Winter 2001.

[84] The 2003 Report has shown that there are three types of member states: those which consider prostitution legal, those which consider it illegal, and those which regulate it.

a pimp takes all the earnings of a person who works as a prostitute by choice, then this may be considered financial exploitation – but not sexual exploitation, covered by the laws on trafficking in human beings. However, if a woman is forced to prostitute herself, this constitutes trafficking in human beings for purposes of sexual exploitation. If exploitation is both sexual and financial, then sexual outweighs financial exploitation; this is the act which materialises the crime of trafficking in human beings for purposes of sexual exploitation, whether or not the victim is given part of the proceeds, and whether or not prostitution is legal in the country concerned.

Part II: Legal, administrative, technical and other means of combating the recruitment of victims of trafficking in human beings via the Internet

Legal and administrative measures are as important as technical measures, and the three combine to combat victim recruitment via the Internet.

Legal measures

By legal measures, we mean laws that must be implemented at national, regional and especially – since Internet use transcends frontiers[1] – international level. These laws must be uniform, effective and updated to keep pace with technological change, and must also combat transnational organised crime.

Although anti-trafficking law has progressed considerably, Internet law remains fragmented and to some extent chaotic. This area is still not regulated coherently and systematically, mainly owing to rapid technological development, but also to lack of political pressure. Nonetheless, numerous efforts have been made, mainly at regional and national level, to combat Internet-based crime.

The Internet needs to be regulated, both as an instrument of communication in general, and as a instrument which can be used for criminal purposes.[2]

As the 2003 report noted, "as a basic principle, crimes which are punishable offline are also punishable online, and therefore the criminal norm should be applicable in principle regardless of whether the Internet was used as a means to commit the crime – that is to say neutral with regard to the technology used".[3]

That report concluded that Internet law was still very much in its infancy, and that the difficulty of legislating in this area was compounded by the fact that the Web transcends national borders.[4] It also referred to

[1] As the 2003 report pointed out, Internet-related crimes are very largely international, since the Internet transcends political or national borders. In spite of this international dimension, the report did not focus on international instruments, although it did mention two – the Cybercrime Convention and European Union Directive 31/2000 of 8 June 2000, p. 76.

[2] 2003 Report, p. 76.

[3] 2003 Report, p. 76.

the growing discrepancy between the law's attitude to child pornography – banned in many European countries, which require access providers to shut down offending Web sites – and its attitude to trafficking in adults or mail-order brides for purposes of sexual exploitation. In this second area, the law was far less clear, and legal action less effective. However, some progress has been made in the meantime.

Legal measures taken by the Council of Europe

Many of the legislative efforts made to tackle trafficking in human beings in recent years, and since the last report, have been regional (European Union and Council of Europe).

There are still no binding international instruments on Internet-based trafficking. The chief general instruments at present are the two Council of Europe Conventions: the Convention on Action against Trafficking in Human Beings and the Convention on Cybercrime (ETS No. 185).

The Cybercrime Convention (ETS No. 185)

Signed in Budapest on 23 November 2001 and in force since 1 July 2004, this is the only internationally binding legal instrument on cybercrime.

The Cybercrime Convention[5] is an important tool,[6] although it focuses on sexual exploitation of children (Article 9 makes it a criminal offence, not only to produce child pornography for distribution via computer, but also to offer it, make it available, distribute, transmit or procure it via computer, or possess it in a computer system), and does not deal directly with trafficking in human beings.[7]

Nonetheless, this Convention should be regarded as covering all crimes committed on or via the Internet. It offers procedural and investigative tools adapted to the volatile Internet environment, which police throughout the world can use to co-operate, 24 hours a day, 7 days a week, in preventing and combating all types of crime, including trafficking in human beings.[8]

[4] Loc. cit., p. 10.

[5] European Treaty Series, No. 185; see http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[6] See also the European Commission's Proposal for a Council Framework Decision on attacks against information systems [COM/2002/0173 final – Official Journal, C 203E, 27/08/2002, pp.109-113].

[7] See 2003 report, p. 76.

It includes provisions[9] on: a) crimes against the confidentiality, integrity and availability of data and systems, such as illegal access, illegal interception, data and system interference, and misuse of devices (Articles 2-6); b) computer-related offences, such as computer-related forgery and fraud (Articles 7-8); c) offences related to infringement of copyright and related rights (Article 10) and d) the use of computers to commit "content-related offences", which include child pornography (Article 9).

One of the Convention's most important provisions is Article 19, which permits inspection and seizure of computer-stored data. This applies not just to pornography – as a first glance might suggest – but to all crimes committed via computer. This means that, if anything found on a computer indicates a link with trafficking in human beings, data may be accessed and seized.[10]

It should be noted that the Cybercrime Convention covers both public and private networks and communication systems – which is of considerable importance, since many seemingly public networks may be fakes, or imitations of actual public networks or services.

Article 1 of the Cybercrime Convention defines "service provider" as:

- any public or private entity that gives users of its service the ability to communicate via a computer system, and
- any other entity that processes or stores computer data on behalf of such a communication service or its users.

The 2003 report noted that the Internet could certainly be a factor in the current growing acceptance of documents and images of this kind.[11] This is a very important point, and ties in with the suggestion that virtual pornographic images should be criminalised – something which the Convention on Cybercrime did not cover. It is true that virtual images do not affect a "real" person, or a specific child's or adult's personality, and so cannot be linked directly with pornography or trafficking. We feel, nonetheless, that they call for special attention, since they play a part in predisposing certain people to commit definite crimes.

[8] At present, 21 states (including the United States) are party to the Convention, and 22 others have signed it. Only 4 of the 7 states which have ratified the Council of Europe Convention on Action against Trafficking in Human Beings have also ratified the Cybercrime Convention (Albania, Austria, Bulgaria, and Romania); of the remaining 3, Georgia has not even signed it (probably owing to its poor Internet and telecommunications infrastructure), while Moldova and Slovakia have signed, but not ratified.

[9] See presentation by Mr Henrik Kaspersen at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

[10] Ibid.

[11] 2003 report, p. 11.

That being so, pornography should be redefined as not necessarily involving use of a "real" person, especially in the case of children, and virtual images recognised as constituting pornography, since they denote the victim.[12] National law in some countries already includes virtual images in the definition of child pornography (e.g. Greece, Article 348A of the Criminal Code).

The Convention on Action against Trafficking in Human Beings (CETS No. 197)

The Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197), opened for signing in Warsaw on 16 May 2005,[13] makes an important contribution. Firstly, it declares that trafficking in human beings violates the rights, dignity and integrity of the human person, and that all its victims thus require greater protection. Secondly, it covers all forms of trafficking (national, transnational, linked or not linked to organised crime, and involving all types of exploitation), particularly with a view to victim protection and international co-operation. Thirdly, it sets up monitoring machinery to ensure that parties respect its provisions in practice.[14]

According to the Convention, the modes of recruitment of victims of trafficking in human beings are "threat or coercion, fraud, deception, abuse of power, etc." However, the specific means used for each mode are not defined, so that all means, even the Internet, are covered. As we said earlier, even when the Convention speaks of "recruitment by means of the threat or use of force, etc....", it is clear, in legal terms, that it is referring to the way (mode) in which the crime is committed.

Again according to the Convention, trafficking can also involve taking advantage of the victim's vulnerability, i.e. the "abuse of any situation in which the person involved has no real and acceptable alternative

[12] A broad definition of pornography, extending to virtual images, was adopted by the Group of Specialists responsible for revising Recommendation Rec (2001) 16 on the protection of children against sexual exploitation, adopted by the Council of Europe's Committee of Ministers on 31 October 2001, and itself a revised version of Recommendation Rec (91) 11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults. See also the 2003 report, p. 70.

[13] We think it unnecessary to say more about the Convention at this point. Further details of the Council of Europe's work on the Convention – from drafting to adoption and the accompanying campaign – can be found on the relevant Web site: http://www.coe.int/trafficking/.

[14] We should not forget that Article 4 of the European Convention on Human Rights also remains valid for trafficking in human beings in connection with slavery and forced labour. Under that article, the European Court gave an important judgment on domestic slavery in *Siliadin v. France,* Application No. 73316/01, 26 July 2005; see http://www.echr.coe.int/echr/.

to submitting to the abuse. The vulnerability may be of any kind, whether physical, psychological, emotional, family-related, social or economic. The situation might, for example, involve insecurity or illegality of the victim's administrative status, economic dependence or fragile health. In short, the situation can be any state of hardship in which a human being is impelled to accept being exploited".[15] Persons abusing such a situation flagrantly violate human rights, dignity and integrity, which no one can validly renounce.

The wide range of means used – from abduction and violence to enticement or abuse of a person's economic insecurity or poverty – reflect differences of degree, rather than any difference in the nature of the crime, which can always be classified as trafficking, based on the use of such methods.[16]

The purpose, of course, must be to exploit an individual. The Convention provides that: "Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs". National law may therefore target other forms of exploitation, but must at least cover the types mentioned as constituents of trafficking in human beings.[17]

Under the definition of trafficking given in Article 4 of the Convention, it is not necessary for a person to have been exploited for trafficking in human beings to be involved. It is enough that he/she has been subjected to one of the acts referred to in the definition, using one of the means specified, "for the purpose of exploitation". Trafficking is consequently present before the victim is actually exploited.[18]

As regards "exploitation of the prostitution of others or other forms of sexual exploitation", it should be noted that the Convention deals with these only in the context of trafficking. The terms "exploitation of the prostitution of others" and "other forms of sexual exploitation" are not defined in the Convention, which does not therefore affect the way in which states parties deal with prostitution in domestic law[19].

The authors of the Convention also considered use of the new information technologies by traffickers, and decided that its definition of trafficking in human beings covered trafficking involving use of those technologies. For instance, the definition's reference to recruitment covers recruitment by any means (personal, through the press or via the

[15] Para. 83 of the Explanatory Report on the Convention.

[16] According to para. 84 of the Explanatory Report on the Convention.

[17] Para. 85 of the Explanatory Report on the Convention.

[18] Para. 87 of the Explanatory Report on the Convention.

Internet)[20], regardless of the mode employed (threat, force, etc.). They accordingly thought it unnecessary to add a provision specifically making the Cybercrime Convention's provisions on international co-operation applicable to trafficking in human beings.

In other words, the Council of Europe's Anti-trafficking Convention is about protecting the fundamental human rights of victims, offline as much as online. For instance, when it comes to prevention, states are required to take measures to "reduce children's vulnerability to trafficking".[21] This, of course, is particularly true online, with such tools as blocked access to certain Web sites, parental control of Internet access, etc. When it comes to reducing demand, states are asked to run "targeted information campaigns" – which again can be done both on and offline.[22]

Interaction between the two Council of Europe conventions

When it comes to prosecution, the criminal law provisions of the Anti-Trafficking Convention and the investigative tools provided for in the Cybercrime Convention seem to interact significantly, opening the way to a comprehensive onslaught on e-trafficking. For instance, law enforcement agencies can use the "production orders" mentioned in the Cybercrime Convention (Article 18) to compel suspects to release specified computer-stored data in their possession or under their control. This may be highly important in investigating cases of trafficking. The same goes for "expedited preservation of stored computer data" (Article 17), "search and seizure of stored computer data" (Article 19), "real-time collection of traffic data" (Article 20), etc. These are some of the Cybercrime

[19] Para. 88 of the Explanatory Report on the Convention. Concerning prostitution, the 2003 report noted that legal systems and practices differed in the 47 Council of Europe member states. Some are "prohibitionist" (forbid prostitution and punish clients); others are "legalist" or "regulationist" (do not punish exploitation of the prostitution of persons of full age), or "abolitionist" (do not punish prostitution, but do punish its exploitation). Prostituting oneself is not generally an offence. The one exception is Moldova, where professional (as opposed to casual) prostitution is illegal. Incitement to prostitution is, however, a criminal offence in all the countries surveyed. In Sweden, too, purchasing sexual services is punishable, while in France only purchasing the sexual services of a minor is prohibited. In the Netherlands, prostitution has been legalised. Moldova and the Netherlands are the opposite ends of the spectrum.

[20] Para. 79 of the Explanatory Report on the Convention.

[21] Address by Maud de Boer-Buquicchio, Deputy Secretary General of the Council of Europe, at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

[22] Address by Maud de Boer-Buquicchio, loc. cit.

Convention's investigative tools which are crucial to the investigation and prosecution of trafficking offences.

Legal measures taken by the European Union

The European Union has also adopted anti-trafficking in human beings measures, and been particularly active in the fight against cybercrime. Indeed, eliminating cybercrime and trafficking in human beings was one of the objectives set for an area of justice, freedom and security by the Tampere Summit in 1999, and underlined by the Treaty of Nice (2001), when it stressed the need to harmonise national laws. Since 2000, the European Union Council has issued a Framework Decision on trafficking in human beings and a series of Directives on electronic communications, regulating, among other things, the liability of providers and intermediaries, and the retention of stored data.

The European Union Framework Decision

The European Union Council of Ministers' Framework Decision on Combating Trafficking in Human Beings came into force in August 2002, and member states were required to implement it by 1 August 2004.[23] Framework Decisions are similar to European Union Directives in requiring member states to achieve a specified result – but give national authorities a free hand in deciding how to do that. They have no direct effects.

The Framework Decision is a narrower text than the Council of Europe Convention on Action against Trafficking in Human Beings, since it criminalises only the exploitation of labour or services (including forced or compulsory labour or services, slavery, and practices similar to slavery or servitude) and exploitation of the prostitution of others or other forms of sexual exploitation, including pornography.

The modes of commission it specifies are also more limited than those listed in the Council of Europe convention, since it speaks only of "recruitment, transportation, transfer or harbouring of a person". The victim's consent is also irrelevant, when the offender's conduct constitutes exploitation within the meaning of the proposal, i.e. involves:

- the use of coercion, force or threats, including abduction

[23] European Union Council Framework Decision 2002/629/JHA, *Official Journal of the European Communities* L 203, 1 August 2002, pp. 1-4; it can be downloaded at http://europa.eu.int/scadplus/printversion/en/lvb/l33137.htm; also available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0629:EN:HTML.

- the use of deceit or fraud
- the abuse of authority or influence, or the exercise of pressure
- the offer of payment

Article 3 of the Framework Decision sets a maximum penalty of not less than eight years' imprisonment for any trafficking offence which has:

- deliberately or by gross negligence endangered the life of the victim;
- been committed against a particularly vulnerable victim. Victims are considered particularly vulnerable (at least) when under the age of sexual majority in national law, and when the offence has been committed for the purpose of exploiting the prostitution of others, or involves other forms of sexual exploitation, including pornography;
- been committed using severe violence or has caused particularly serious harm to the victim;
- been committed within the framework of a criminal organisation, as defined in Joint Action 98/733/JHA, apart from the penalty level referred to therein.

European Union Directives on liability of access providers

The situation regarding Internet and electronic communications in general has evolved fairly fast in the European Union. Numerous steps have been taken towards recognition of providers' liability, and their obligation to store data when crimes are committed via the Internet. Until recently, the main problem was that providers could not be obliged to store data, without which no crime could be proved, and that intermediaries were not considered liable.

Under Article 15 of European Union Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market ("Directive on electronic commerce"),[24] providers were not generally required to monitor information they transmitted or stored, or to actively seek facts or circumstances indicating illegal activity, unless they had initiated the communication, selected the receiver or modified the information transmitted (Article 12), or unless they had actual knowledge of illicit content or, having become aware of illicit content, did not act promptly to remove it or block access to it (Article 14).

[24] OJEC., L 178, 17-07-2000, pp. 1-16.

Article 15 (2) requires service providers to inform the relevant authorities promptly of allegedly illegal activities undertaken, or information provided, by recipients of their service, and to communicate to those authorities, at their request, information enabling them to identify recipients of their service with whom they have storage agreements. In practice, however, providers were slow to do this, unless asked to do so by the authorities in specific cases, after judicial lifting of confidentiality, which was – and still is – a legal prerequisite.

So far, member states have been prohibited from obliging providers to look actively for illegal content which they may be hosting or transmitting. Under Article 15 of the Directive, providers are totally exempt from liability, unless they have actual knowledge of illegal content which they may have been storing or transmitting.

Legal and technical differences between national regulations on retention of data for the purpose of preventing, investigating, detecting and prosecuting criminal offences stood in the way of the internal market for electronic communications, since service providers were faced with different requirements concerning types of traffic and location data to be retained, and conditions and periods of retention.

The 2003 report suggests that countries should review their laws on criminal liability of persons inserting Web page hyperlinks for the content of pages to which those links send users, and of chat-room moderators, since both may be aware of the content of those sites or messages, and may provide access to sites concerned with sexual exploitation, or persons involved in it.

As the 2003 report notes,[25] it is important for providers to store data, "because of the fact that the acting person is physically not present at the place of the real impact of the action, and therefore no physical traces can be found, and telecommunication trails are the only way to investigate the crimes. Erasing or not keeping those trails would have the same effect as e.g. wiping fingerprints or blood stains at a murder scene. Anyone can connect to and communicate through telecommunication networks, very anonymously, from anywhere in the world. The use of aliases and nicknames makes the user information and identity data unreliable".

Directive 2002/58/EC on privacy and electronic communications[26] of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, was adopted to regulate the process-

[25] 2003 report, p. 94.

[26] OJEC. L 201, 31.7.2002, pp. 37-47.

ing by network and service providers of traffic and location data generated by the use of electronic communications services. Under Articles 5, 6 and 9, such data should be erased or made anonymous when no longer required for transmission of a communication, with the exception of data needed for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of added-value services.

Article 15 (1) of the Directive specifies the conditions on which member states may restrict the scope of the rights and obligations listed in Article 5, Article 6, Article 8 (1), (2), (3) and (4), and Article 9. Any such restrictions should be necessary, appropriate and proportionate within a democratic society for specific public-order purposes, i.e. to safeguard national security (i.e. state security) or for defence, public security or the prevention, investigation, detection and prosecution of criminal offences, or unauthorised use of electronic communications systems.

Several member states have now adopted laws providing for retention of data by service providers for the prevention, investigation, detection and prosecution of criminal offences.[27] Because national regulations varied, the European Union thought it necessary to ensure, at European level, that data generated or processed, in the course of supplying communications services, by providers of publicly available electronic communications services, or of public communications networks, were retained for a certain period.

This was what led to the adoption of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.[28]

Article 3 of the Directive establishes an obligation to retain the data (specified in Article 5) needed to trace and identify the source, destination, date, time, duration and type of communications, when such data are generated or processed by providers of publicly available electronic communications services or of public communications networks within the jurisdiction of the member state concerned, in the course of supplying those services. This includes data (specified in Article 5) relating to unsuccessful call attempts, when such data are generated or processed,

[27] The Conclusions of the Justice and Home Affairs Council of 19 December 2002 emphasise that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important, and therefore a valuable tool for the prevention, investigation, detection and prosecution of criminal offences, particularly organised crime.

[28] Official Journal L 105, 13-04-2006, pp. 54-63.

and stored (telephonic data) or logged (Internet data) by providers of publicly available electronic communications services or of public communications networks within the jurisdiction of the member state concerned, in the course of supplying those services.

Concerning Internet access, Internet e-mail and Internet telephony, and regarding the data needed to identify users' communication equipment, the Directive requires that the following data be retained (Article 5, para. 1 (3)):

- the calling telephone number for dial-up access;
- the digital subscriber line (DSL) or other end-point of the originator of the communication.

Concerning mobile telephony, it requires, in the case of pre-paid anonymous services, that the date and time when the service was first activated, and the location label (Cell ID) from which it was activated, be retained (Article 5, para. 1 (2) iv).

Under Article 6, data must be retained for not less than six months, and not more than two years, from the date of the communication.

Application of the Directive is set for 15 September 2007, but many European Union member states have declared that they will postpone application.

However, the European Union Directives are limited in their application, since they do not apply to services supplied by providers in non-European Union countries.

Legal measures taken at national level

Until recently, most member states have had laws on neither trafficking in human beings nor Internet-related offences.[29] The group which prepared the 2003 report found that the laws then in force in the various Council of Europe states made no attempt whatsoever to regulate use of the Internet for trafficking in human beings for purposes of sexual exploitation. A few countries dealt with the two issues – content circulating on the Internet, and trafficking in human beings for purposes of sexual exploitation – separately, but made no connection between them.[30]

[29] A questionnaire was sent to member states, and 21 members have replied (it was not sent to Greece, since the author is familiar with Greek law). Of the 22 member states covered in this part, 15 are European Union members, and 4 (Albania, Moldova, Romania and Slovakia) have ratified the Council of Europe Convention on Action against Trafficking in Human Beings (two of these are European Union members). Among countries which have ratified the Anti-Trafficking Convention, Georgia, Slovakia and Moldova have not yet ratified the Cybercrime Convention.

[30] 2003 report, p. 9.

Today, however, even if some countries have not yet ratified the Council of Europe conventions, they have all ratified other international instruments against trafficking in human beings, such as: the 1949 UN Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others; the 1989 UN Convention on the Rights of the Child with its 2000 Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography; or the 2000 United Nations Convention against Transnational Organised Crime with its Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing the Convention; and at European Union level, the member states have transposed the Framework Decision on Trafficking in Human Beings and the first two Directives on electronic communications.

Most of the European Union member states in particular have ratified the Council of Europe's Cybercrime Convention, and transposed Directive 31/2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market,[31] and also Directive 2002/58/EC on privacy and electronic communications,[32] into their domestic law. Only 6 of the 22 states which have ratified the Cybercrime Convention are outside the European Union – which is probably due to the state of communications infrastructure in many of them.

We shall now describe the present legal situation in a number of Council of Europe member states:

Albania

The legal situation regarding trafficking in human beings appears to be satisfactory, since Albania has ratified the *Convention on Action against Trafficking in Human beings* (on 6 February 2007) and the Cybercrime Convention (on 20 June 2002), as well as the Palermo Protocol.[33]

The National Anti-Trafficking Co-ordinator recently proposed an amendment to Article 298 of the Criminal Code, which the Council of Ministers has approved. This is concerned with people-smuggling across borders other than those of Albania, and is complemented by a law banning the use of speed-boats (widely used by traffickers to Italy) for a period of three years. An Integrated Border Management Strategy is also being finalised to co-ordinate the work of the border police, the

[31] EC Official Journal, L 178, 17/07/2000, pp. 1-16.

[32] EC Official Journal, L 201, 31/07/2002 pp. 37-47.

[33] More details of Albanian law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Rome, 18-19 October 2006 at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem3-2006_Proceedings.pdf.

transport authorities and the customs services, as well as the phyto-sanitary services.

There is also a proposal for a new provision on exploitation of children for forced labour purposes in the Criminal Code, and a new socio-educational assistance package for these children and their families, covering employment, schooling and other kinds of aid is being planned. In addition, regulations aimed at tourist agencies are being drafted with the Ministry of Tourism, prohibiting the sexual exploitation of women and children on hotel premises.

Moreover, the new Albanian law "on aliens", currently in process of drafting and approval, will – in full accordance with international standards – cover temporary residence permits for foreign victims of trafficking.

On 27 February 2006, Greece and Albania signed a bilateral agreement on protecting and assisting child victims of trafficking.

At present, standard agreements are being prepared and finalised on co-operation between the Ministry of the Interior (the responsible authority) and NGOs and international organisations involved in fighting trafficking in human beings. These agreements will spell out the obligations and responsibilities of the various parties, especially concerning sharing of information and co-ordinated reporting.

Belgium

The Crime Act of 10 August 2005 brought Belgian legislation into line with European Union and international standards. However, Belgium has only signed, but not ratified, the two Council of Europe conventions.[34]

The offence of trafficking in human beings is defined in Article 433 *quinquies* of the Criminal Code, which applies to all victims, regardless of their nationality. The emphasis is now on exploitation, rather than abuse of victims. Trafficking was previously covered by Section 77 *bis* of the 1980 Immigration Act. That provision was confined to foreigners, and prohibited both trafficking and smuggling in general, without differentiating the two offences. Section 77 *bis* now applies only to smuggling, which it defines clearly. Under the Act of 15 September 2006 amending the Immigration Act of 15 December 1980 (and transposing the Euro-

[34] More details of Belgium's anti-trafficking in human beings laws can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Oslo, 1-2 November 2006, at `http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem4-2006_Proceedings.pdf`.

pean Directive of 29 April 2004[35]), protection applies to the victims, not only of trafficking, but also of people-smuggling, albeit in specified cases.

The 2005 Act also introduced the offence of exploitation of begging in Article 433 of the Criminal Code. The aim here is not to re-criminalise begging, but to make exploitation by others of persons who beg a punishable offence, by analogy with the exploitation of prostitution covered by Article 380 of the Criminal Code. The text of Article 433 *ter* was inspired by Article 225-12-5 of the French Criminal Code, introduced by the Act of 18 March 2003.

In 2004 a Royal Decree set up a special Unit for interdepartmental co-ordination of action to combat people-smuggling and trafficking in human beings.

The same Royal Decree set up a Centre for information on, and analysis of, people-smuggling and trafficking in human beings (CIA-STHB). It is mainly responsible for information exchange between the various players involved in the fight against trafficking in human beings and people-smuggling.

Bosnia and Herzegovina

Bosnia and Herzegovina ratified the Cybercrime Convention on 19 May 2006 (bringing it into force on 1 September 2006), but has only signed the Anti-Trafficking Convention. Otherwise, there are no laws on use of the Internet to commit serious crimes. The latest amendments to the law on trafficking in human beings were adopted in 2004, and came into force on 6 January 2005 under the Act on amendments to the Criminal Code of Bosnia and Herzegovina. Article 186 of the Criminal Code makes trafficking of adults punishable by one to ten years' imprisonment, and trafficking in children punishable by at least five years' imprisonment. If an organised criminal group is involved, the sentence increases to at least ten years. For international procuring of prostitutes trafficked abroad, Article 187 of the Criminal Code imposes prison sentences of six months to five years, and one to ten years if there are aggravating circumstances (e.g. if a child is involved).[36]

[35] Directive 2004/81/C of the Council on the short-term residence permit issued to victims of action to facilitate illegal immigration or trafficking in human beings who co-operate with the competent authorities, OJEC L 261 of 06.08.2004, p.19-23.

[36] More details of the law of Bosnia and Herzegovina can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution*, Bucharest, 4-5 April 2006, at `http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem1-2006_Proceedings.pdf`.

Croatia

Croatia ratified the Cybercrime Convention on 17 October 2002 (bringing it into force on 1 July 2004), but has only signed the Anti-Trafficking Convention. However, it has laws on trafficking.[37] Article 175 of the Criminal Code incorporates the Palermo Protocol's definition of trafficking. A new paragraph, criminalising use of a victim's services, has also been proposed, in accordance with Article 19 of the Council of Europe Convention.[38]

Under Article 8 of the Criminal Code, *ex-officio* prosecution is also possible. The victim is not required to take part in the criminal proceedings against the accused, and does not have to co-operate with the courts or police to receive assistance.

Cyprus

Cyprus ratified the Cybercrime Convention on 19 January 2005 (bringing it into force on 1 May 2005), but has only signed the Anti-Trafficking Convention.

The main laws on trafficking are: Act 3 (I) of 2000, providing for special protection of victims of sexual exploitation; Act 11 (III) of 2003, ratifying the Palermo Protocol; and Act 22 (III) of 2004, ratifying the Cybercrime Convention and its 2003 Protocol of 2003. Cyprus has already submitted the Anti-Trafficking Convention for ratification.

Although the Cybercrime Convention has been incorporated into domestic law, it has not been possible to incorporate its procedural provisions (covering inspection and seizure of computer-stored data, expedited preservation and partial disclosure of traffic data, production orders and data collection), which are considered incompatible with the Cypriot Constitution, and particularly its human rights provisions (Article 15 of the Cybercrime Convention provides that each party shall ensure that the establishment, implementation and application of the powers and procedures provided for in that section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties). However, a bill amending Act 3 (I) 2000 is already before Parliament. This includes provisions on the recruitment of victims via the Internet, and on liability of legal entities and jurisdiction of courts, regardless of whether the offence is committed by an entity located in Cyprus, or via a system

[37] The laws on trafficking in human beings can be found at `http://www.ljudskaprava-vladarh.hr/default.asp?ru=188`.

[38] More details of Croatian law can be found in the above-mentioned proceedings of the Bucharest seminar, loc. cit.

which can be accessed from Cyprus (whether based in Cyprus or outside).

European Union Directive 2000/31/C on electronic commerce has also been transposed by Act 156 (I)/2004.

Denmark

Denmark ratified the Cybercrime Convention on 21 June 2005 (bringing it into force on 1 October 2005), but has only signed the Anti-Trafficking Convention.[39]

The Trafficking in Human Beings Bill (Folketing) of 31 May 2002 (Act No. 380/02-06-2002), which made trafficking in human beings an offence in the Criminal Code, facilitated prosecution of providers, e.g. by making it easier for the police to override confidentiality of communications. Article 262a of the Criminal Code also facilitates proactive police investigation. Traffickers in human beings can now be given prison sentences of up to 8 years (Article 125a of the Code). In 2005 the Code was amended to include trafficking in children.

A new action plan to combat trafficking in women was adopted on 1 March 2007 (the first action plan dated from 2002).

Denmark's "Neighbourhood Programme" also funds preventive action by, and capacity-building for, authorities and NGOs in Eastern Europe (Belarus, Moldova, Ukraine and, to a lesser extent, Bulgaria and Romania).

Estonia

Estonia ratified the Cybercrime Convention on 12 May 2003 (bringing it into force on 1 July 2004), but has not even signed the Anti-Trafficking Convention. In March 2004, however, it ratified the UN's Palermo Protocol on trafficking in persons.[40]

The amended Estonian Criminal Code has more provisions on trafficking in human beings than the earlier version (the new Code replaced the old one on 1 September 2002).

Prostitution is not a crime in Estonia, but trafficking for purposes of sexual exploitation can be combined with other offences specified in the Criminal Code: enslavement (§133); abduction (§134, and of chil-

[39] More details of Danish law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Oslo, 1-2 November 2006, at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem4-2006_Proceedings.pdf.

[40] More details of Estonian law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Riga on 21-22 September 2006 at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem2_2006_Proceedings.pdf.

dren: §172); illegal research on human subjects (§138); illegal removal of organs or tissue (§139); compelling persons to donate organs or tissue (§140); compelling persons to engage in sexual intercourse (§143); sale or purchase of children (§173); use of minors to produce pornography (§177); production or provision of child pornography (§178) and other sex-related offences.

The latest amendments to the Criminal Code became effective in July 2006. They introduced severer penalties for offences against minors (e.g. facilitating prostitution of minors). At present, under Article 133 of the Code (enslavement), violence and deception are necessary elements.

On 28 August 2005 the Estonian Ministers of Justice and the Interior signed the *Laulasmaa Declaration*, agreeing that the State Prosecutor's Office and the police would together prioritise the fight against all crimes linked with trafficking in human beings.

In January 2006, the Estonian Government approved an anti-trafficking action plan for 2006-2009, submitted by the Minister of Justice. Its main aim is to make the fight against trafficking in human beings more effective.

"The Former Yugoslav Republic of Macedonia"

The Former Yugoslav Republic of Macedonia ratified the Cybercrime Convention on 15 September 2004 (bringing it into force on 1 January 2005), but has only signed the Anti-Trafficking Convention.

Following amendment of the Criminal Code in June 2003, the penalties provided for in Article 418-a on trafficking in human beings have been increased to 4 years' imprisonment.

The amendments of March 2004 added an Article 407-a to the Code. Paragraph (1) provides for imprisonment for one to five years for certain crimes (specified in Articles 403 to 407) committed **through information systems.** However, these crimes have nothing to do with trafficking (Article 403 covers Genocide, Article 403-a crimes against humanity, Article 404 war crimes against civilians, Article 405 war crimes against wounded or sick persons, Article 406 war crimes against prisoners of war, and Article 407 use of unlawful means of combat.

It should, however, be noted that "the Former Yugoslav Republic of Macedonia" still has very limited technical and communications infrastructure, and does not yet appear to have machinery or procedures to deal with this form of trafficking. Nonetheless, statistics on Internet use[41] show that the user rate was 19% in 2007, and had increased by 1 208.9% between 2000 and 2007.

[41] See Appendix 1, page 139.

Germany

Germany has not so far ratified either of the Council of Europe conventions, but only signed them. However, it has inserted specific anti-trafficking in human beings provisions in the Criminal Code, Articles 180, 181 and 236 (trafficking in human beings involving children), and has also transposed the European Union Directive on electronic commerce. The use of the Internet to commit any crime is punishable.[42]

Germany is now planning to amend the existing law on telecommunications, with a view to introducing new regulations on police surveillance measures and undercover action in that field. For that purpose, a bill is being drafted to transpose European Union Directive 2006/24[43] and specify periods during which access providers must store data (especially on Internet connections) for up to 6 months.

Greece

Although Greece has not so far ratified either of the Council of Europe Conventions, but only signed them, we can say that it possesses satisfactory anti-trafficking in human beings laws, having already – like all European Union members – transposed the Framework Decision on Trafficking in Human Beings of 19 July 2002,[44] as well as Directive 31/2000 on electronic commerce.[45]

The Ministry of Justice has already set up a special drafting Committee to prepare ratification of the UN Convention against Transnational Organised Crime, and its three Protocols (especially the "Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organised Crime"), and also the Council of Europe's Convention on Action against Trafficking in Human Beings.

Trafficking in human beings for purposes of sexual exploitation was already a punishable offence in Article 351 of the Greek Criminal Code, adopted in 1951. That article referred only to pimping (soliciting to prostitution[46]), but said nothing of the smuggling of aliens into the

[42] The German reply indicates that the Internet is seen as similar to press advertising as a means of recruitment.

[43] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC, O.J. L 105, 13.4.2006, pp. 54-63.

[44] 2002/629/JHA/L203, OJEC L 203, 1 August 2002, pp. 1-4.

[45] 2000/31/EC, OJEC L 178, 17 July 2000, pp. 1-16.

[46] Prostitution is regulated in Greece by Act 2734/1999 (Official Gazette A-161) on the licensing of prostitutes, as amended by Section 12 of Act 2839/2000.

country. The offence, as defined, was confined to the exploitation of women victims (adult or minor), and the penalties were those for misdemeanours.

Since 2001 Greece has been combating trafficking in human beings more consistently. A significant step was the setting-up of the Task Force against Trafficking in Human Beings (known as OKEA), under the aegis of the Ministry of Public Order. Its membership is inter-ministerial and inter-disciplinary, and its purpose is to review the laws in this area and raise awareness of the problem. First legislative steps to combat trafficking were taken by revising the relevant articles in the Criminal Code, and introducing specific provisions on trafficking in Act 3064/2002 and Presidential Decree 233/2003.

Further steps were taken with Act 3386/2005 (Official Gazette A-212), on "Entry, residence and social integration of nationals of third countries on Hellenic territory" (transposing European Union Directive 2004/81/EC of 29 April 2004 on the short-term residence permit issued to victims of action to facilitate illegal immigration or trafficking in human beings who co-operate with the competent authorities). Sections 46-52 of that act define victims of human trafficking, and they comprehensively regulate protection and assistance for them.

Act 3064/2002 (Official Gazette No. 248/15.10.2002) on combating trafficking in human beings, crimes against sexual freedom, child pornography, the financial exploitation of sexual activity in general, and assistance for victims of these acts (transposing the European Union Framework Decision on trafficking of 19 July 2002) deals with human trafficking and exploitation of the sexual activity of vulnerable groups, such as women, aliens and minors. It also covers measures to protect and assist victims of the offences it defines.

The basic legislative innovations in this area can be summarised as follows:

1. Article 323 of the Criminal Code (on the slave trade) is followed by a new article 323A on "trafficking in human beings", which covers other modern forms of trafficking in human beings, such as trafficking for purposes of organ removal, forced or fraudulent exploitation of the labour of trafficked persons, and recruitment of children for use in armed conflicts. These are criminal offences, and punishable by imprisonment for up to ten years, plus fines ranging from €10 000 to €50 000. There are aggravating circumstances if the victim is a minor, if the offence has been committed by a public official within the context of his duties, of if the victim has suffered serious bodily harm. In such cases, the minimum penalty

is ten years' imprisonment, plus fines ranging from €50 000 to €100 000.

2. Article 349 of the Criminal Code on procuring the prostitution of minors has been amended to introduce harsher penalties – imprisonment for up to ten years, plus a fine. The difference between procuring and trafficking is that the victim of the first is not regarded as exploited, since the decision to become a prostitute has been freely taken, and the procurer merely facilitates that decision, or prevents the victim from leaving the "scene".

   In practice, pimping/soliciting to prostitution (Article 351 of the Criminal Code) can amount to trafficking in human beings for purposes of sexual exploitation. Although Articles 351 and 323A of the Criminal Code are similar (in all but their purpose) and prescribe identical penalties, the Code places them under different headings – Article 351 under sexual offences, and Article 323 A (which punishes trafficking for purposes of labour exploitation or organ removal) under crimes against personal freedom.

   It must be stressed that Greece is one of the few countries to criminalise use of the services of trafficked victims[47] (Articles 323A (3) and 351 (3) of the Criminal Code). The Council of Europe's Anti-Trafficking Convention is the only other text to include such a provision (Article 19).

   Two new articles have also been added to the Criminal Code – Articles 348A (child pornography) and 351A (sexual misconduct with a minor in return for payment or other material benefits.

3. All of the above crimes, inserted in the Criminal Code by Act 3064/2002, are punishable even when committed abroad, regardless of the law applying in the place where they were committed (Article 8 of the Criminal Code). They are also among the crimes listed in Article 187 of the Code (punished more severely if committed within the framework of a criminal organisation). Consequently, the provisions on protection of witnesses also apply here.

4. Moreover, under Section 11 (5) of the same act (3064/2002), human trafficking (Article 323A of the Criminal Code) and pimping (Article 351) are added to the list of punishable acts included in Section 1(1) of Act 2331/1995 (Official Gazette No. 173), as amended by Act 3424/2005 "on amendment, completion and replacement of the provisions of Act 2331/95 and alignment of Greek legislation on Di-

[47] Sweden criminalises the client's behaviour in relation to prostitution, not trafficking. Croatia has recently been envisaging a new provision, criminalising use of the services of victims, in accordance with Article 19 of the Council of Europe Convention.

rective 2001/97/EC of the European Parliament and of the Council on prevention of the use of the financial system for the purpose of money laundering and other provisions". This means that Act 2331/1995, which provides for seizure and confiscation of assets derived from criminal activity also applies in this case.

5. Section 11 (6) of Act 3064/2002 provides for closure of any establishment used in connection with trafficking in human beings,[48] or other offences covered by that act.

It must be emphasised that, where trafficking in human beings is concerned, Greece's definition of "exploitation" is fairly narrow, since Articles 323A and 351 of the Criminal Code do not refer to all forms of exploitation, but simply labour and sexual exploitation, as well as organ removal, and the recruitment of minors to commit acts.

The law on liability of ISPs is based on the following texts:

- Article 13 of Presidential Decree 131/2003,[49] transposing Directive 2000/31 on electronic commerce);[50]
- Article 4 (1.e.bb) of Presidential Decree 47/2005 on procedures and on technical and organisational guarantees and safeguards for judicial lifting of the confidentiality of telecommunications[51] (by derogation from Section 9 of Act 3115/2003 on establishment of the authority responsible for protecting the confidentiality of telecommunications –Official Gazette A-47), and
- Act 3471/2006,[52] transposing European Union Directive 2002/58/C of 12 July 2002[53] concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications – ePrivacy Directive).

Under Section 4 of Act 3471/2006, electronic traces count as personal data, and so even the police may not attempt to locate them without first following the legal procedure for judicial lifting of confidentiality. Al-

[48] Article 23 (4) of the Council of Europe Convention on Action against Trafficking in Human Beings (2005) also provides that states should adopt legislative or other measures "to enable the temporary or permanent closure of any establishment which was used to carry out trafficking in human beings, without prejudice to the rights of *bona fide* third parties, or to deny the perpetrator, temporarily or permanently, the exercise of the activity in the course of which this offence was committed".

[49] Official Gazette A' 116/16.05.2003.

[50] OJEC, L 178, 17/07/2000, pp. 1-16.

[51] In European Union member states, confidentiality of communications is guaranteed by Article 5 of Directive 97/66/EC, which requires them to prohibit any interception or surveillance of communications by persons other than senders and receivers, except when authorised by law.

[52] Official Gazette 133 A/28.6.2006.

[53] OJEC, L 201, 31.7.2002, pp. 37-47.

though the procedure is semi-immediate, there is always a danger that traffickers may, if they know the police suspect them, destroy all the relevant data – which is done in a matter of seconds.

The act provides for sanctions for police officers who fail to follow the prescribed procedure, even when their aim in so doing is to arrest a criminal (Section 13 refers to application of the administrative sanctions provided for in Section 21 of Act 2472/1997 on the authority responsible for the protection of personal data, and Section 11 of Act 3115/2003 on the authority responsible for protection of the confidentiality of telecommunications, depending on which has jurisdiction). Section 15 also provides for criminal sanctions, comprising at least one year's imprisonment, with a fine of €10 000 to €100 000.

A law is currently being drafted to transpose Directive 24/2006 and oblige providers to store data for at least one year (already done unofficially in practice).

Italy

Although Italy has only signed the two Council of Europe conventions, it has national laws on trafficking in human beings (Articles 600 and 601 of the Criminal Code).[54]

The 2003 report stated that Italy had no specific criminal legislation on the Internet, or on liability of the various persons active on the Internet, but it now has comprehensive regulations on provider liability – Act No. 38/06-02-2006 on action to combat sexual exploitation of children and pornography, also via the Internet, which regulates providers' obligations concerning information disseminated via the Internet, and particularly Legislative Decree No. 70/2003, transposing Directive 2000/31/CE on e-commerce.

One of the general principles of the Internet Self-Regulation Code (Articles 122 and 133 of the Personal Data Protection Code – Legislative Decree No. 196 of 30 June 2003) is that all Internet subjects must be "identifiable", in accordance with the European Union Directive of 2000. Thus, supplying technical services without knowledge of content cannot eliminate provider liability.

Concerning prevention and prosecution of crimes committed via the Internet, Article 25-*ter* of Legislative Decree No. 306 of 8 June 1992 (conversion law No. 356 of 7 August 1992) permits surveillance of all

[54] More details of Italian law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Rome, 18-19 October 2006 at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem3-2006_Proceedings.pdf.

forms of communication, when this is necessary to prevent the crimes specified in Articles 600 and 601 of the Criminal Code (slavery and trafficking in persons).

Also relevant is Article 2 of the Interministerial Decree (*Gazzetta Ufficiale* No. 23 of 29 January 2007) on technical requirements for the filtering devices which Internet providers must use to block access to sites registered with the National Centre against Child Pornography. In addition to criminal sanctions for providers, Article 6 provides for the imposition of administrative fines (€50 000-€250 000) by the Ministry of Communication's regional inspectorates.

Latvia

Latvia ratified the Cybercrime Convention on 14 February 2007 (bringing it into force on 1 June 2007), but has only signed the Anti-Trafficking Convention.[55]

Trafficking in persons is an offence in the Latvian Criminal Code, which defines it in Article 154.2, and provides for prison sentences of 3 to 8 years in Article 154.1. When there are aggravating circumstances (trafficking in human beings involving minors or by an organised criminal group), the penalty is imprisonment for 5 to 12 years, plus confiscation of assets. If the crime has resulted in serious injury to the victim, the Code provides for imprisonment for 10 to 15 years, plus confiscation of assets. If the victim has been sent abroad for purposes of sexual exploitation, Article 165.1 (as amended in 2004) provides for imprisonment for at least 5 years, and for a maximum of 15 years when there are aggravating circumstances.

In 2004, the Government adopted an anti-trafficking in human beings action plan, running from 2004 to 2008. The Ministry of the Interior set up a trafficking in human beings site,[56] carrying information on SOS lines, state policy, and laws, projects and campaigns.

Moldova

Moldova ratified the Anti-Trafficking Convention on 19 May 2006, but has only signed the Cybercrime Convention. It has also transposed the Palermo Protocol.[57]

Trafficking in human beings was inserted in the Moldovan Criminal Code in 2002 (Article 165, amended by Act No. 241-XVI of 20 Octo-

[55] More details of Latvian law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Riga 21-22 September 2006, at `http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem2_2006_Proceedings.pdf`.

[56] This information is available in English at `http://www.cilvektirdzniecіba.lv/index.php`.

ber 2005 "on preventing and combating trafficking in human beings") and is punishable by imprisonment for 7 to 15 years, or 10 to 20 and 15 to 25 years, depending on the gravity of any aggravating circumstances. Article 205 on trafficking of children provides for imprisonment for 10 to 15 years, and again 15 to 20 or 12 to 25 years, depending on aggravating circumstances. In Moldova, professional (as opposed to occasional) prostitution is prohibited.

A national plan to prevent and combat trafficking in human beings was adopted on 25 August 2005 by Governmental Decision No. 903 and others.

Montenegro

Montenegro has signed, but not yet ratified, both the Council of Europe conventions.

As for legislation, trafficking in human beings is a punishable offence under Article 444 of the new Criminal Code, adopted in 2003. The Code also regulates the criminal offence of trafficking in children for adoption (Article 445) and submission to, and transportation for, enslavement (Article 446). Under amendments to the Code adopted in July 2006, people-smuggling, previously dealt with under trafficking in human beings, is now a separate offence (Article 405 – Illegal border crossing and smuggling of human beings).

IT culture in Montenegro is still at a very low level, and so few people use computers and the Internet (17.6% penetration).

Reportedly, there have been few cases of trafficking in human beings in Montenegro, which is mainly a transit country.[58]

There are no laws on misuse of the Internet for trafficking in human beings, but the authorities are willing to introduce appropriate legislation.

Norway

Norway signed and ratified the Cybercrime Convention on 30 June 2006 (bringing it into force on 1 October 2006), but has only signed the Anti-Trafficking Convention.[59]

[57] More details of Moldovan law can be found in the proceedings of the Council of Europe seminar on Action against trafficking in human beings: prevention, protection and prosecution, Bucharest, 4-5 April 2006, at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem1-2006_Proceedings.pdf and also in the proceedings of the Oslo seminar, 1-2 November 2006, at http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem4-2006_Proceedings.pdf.

[58] Fuller information on trafficking in Montenegro can be found in the Country Reports on Human Rights Practices (issued by the State Department – Bureau of Democracy, Human Rights, and Labour, 6 March 2007: http://www.state.gov/g/drl/rls/hrrpt/2006/81373.htm.

In 2002 Norway introduced ethical guidelines for public employees, the aim being to prevent abuse of human beings through the sex trade.

The Government has launched a three-year information campaign to show the public how trafficking affects individuals and society. The intention is to change attitudes to the buying of sexual services, and reduce demand. The demand-reduction measures are based on research on who buys sex, and male attitudes to the purchasing of sexual services. The campaign's main aim is to stop people from buying sex in the first place, and cut demand by changing the attitudes of those who purchase sexual services regularly.

An action plan, covering 37 concrete measures to combat trafficking in human beings, was drawn up in December 2006, for implementation by 2009.[60]

The only reference to links between the Internet and trafficking in human beings is in Chapter 6.3 of the plan, which makes a connection between trafficking and child pornography on the Internet. The Government has committed itself to devising "preventive measures" – both in Norway and outside – to stop the link from developing.

At present the Norwegian Government reports that it is deploying vast resources and funds in an effort to solve trafficking-related problems. Little work is being explicitly done on the Internet as such, but its role in the process is to be analysed.

Poland

Poland has merely signed the two Council of Europe conventions.

However, the following articles in the Polish Criminal Code cover trafficking in human beings and other sex crimes:

- Articles 203-204 impose prison sentences of one to ten year for trafficking, including trafficking abroad for prostitution.
- Article 253 prescribes imprisonment for at least 3 years for the buying and selling of human beings. Under Article 253 (2), the organisation of illegal adoption of children carries a prison sentence of 3 months to 5 years.

[59] More details of Norwegian law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Oslo, 1-2 November 2006 at: http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem4-2006_Proceedings.pdf.

[60] An English version of the document can be found at http://www.regjeringen.no/upload/kilde/jd/rap/2007/0001/ddd/pdfv/304170-stop_human_trafficking_ 0107.pdf.

Portugal

Portugal has merely signed the two Council of Europe Conventions. However, in accordance with Parliamentary Resolution No. 32/2004, approved on 12 February 2004, it has ratified the United Nations Convention against Transnational Organised Crime.

The Portuguese Criminal Code contains several provisions on trafficking in human beings. Article 169, amended by Act 99/2001 of 25 August 2001, makes trafficking in human beings for purposes of sexual exploitation a criminal offence, carrying a sentence of two to eight years' imprisonment. The 2001 amendments extended that article's scope to include other forms of sexual exploitation.

Sexual exploitation of children is dealt with separately in Article 176 of the Code (also revised by Act 99/2001), which prescribes imprisonment for 1 to 8 years for anyone who recruits, transports, houses or receives a child under 16 years old for purposes of sexual exploitation, or arranges for a child to become involved in prostitution, or the sex industry in general, in a foreign country. The 2001 amendments have again extended the scope of this provision, which applies, regardless of the use of violence, threat, fraud or deception, which may be considered aggravating circumstances, leading to imprisonment for 2 to 10 years. If the victim is under 14 years old, or the offender has acted professionally or with the intention of making a profit, these, too, are aggravating circumstances.

Trafficking in human beings for purposes other than sexual exploitation is covered by other provisions in the Code, particularly those on criminalisation of slavery and the slave trade (Article 159), which provide for 5 to 15 years' imprisonment.

Another aspect of action against trafficking is dealt with by Decree Law 325/95 of 2 December 1995, which details legal measures to prevent and combat money laundering. Act 10/2002 of 11 February 2002 extended its scope to cover trafficking in human beings.

Finally, Act 5/2002 of 11 January 2002 describes specific measures to combat organised and economic crime, particularly concerning the collection of evidence relating to a number of crimes, including trafficking in children.

Regarding Internet use and provider liability, Portugal – like most European Union countries – has transposed the European Union Directives (2000 and 2002).

Romania

Romania is one of the two countries which have ratified both the Council of Europe conventions (the other is Albania): the Cybercrime Convention on 12 May 2004 (bringing it into force on 1 September 2004) and the Anti-Trafficking Convention on 21 August 2006.

Anti-trafficking provisions are also included in Act 678/2001 on human trafficking, and Act 39/2003 on organised crime.

Section 51 of Act 161/2003 on certain measures to guarantee transparency in the exercise of public office and functions, and in business, and on the prevention and punishment of corruption, makes "child pornography via information systems" a criminal offence, punishable by 3 to 12 years' imprisonment.

Slovakia

Slovakia is one of the seven countries which have ratified the Anti-Trafficking Convention (on 27 March 2007), but have only signed the Cybercrime Convention (on 7 February 2005). It has also accepted the UN Transnational Organised Crime Convention and the Palermo Protocol on trafficking.

The Criminal Code contains various anti-trafficking in human beings provisions.

Slovak law on electronic communications and provider liability is harmonised with that of the European Union.

Slovakia has adopted a national action plan against trafficking for 2006-2007. The measures covered are essentially preventive, and include the provision of information by police and NGOs on possible Internet misuse.

According to its reply to our questionnaire, Slovakia is still a source country, from which mainly young women are trafficked to various countries. Traffickers most commonly recruit their victims by offering them lucrative employment abroad, chiefly through the traditional channels. The actual extent of the problem is not known, since only a few victims are willing or able to testify. Police statistics are extremely revealing here. In 2001, only 6 cases of trafficking in human beings were recorded – a figure which rose to 17 in 2002 and 2003, and 18 in 2004. It must be emphasised that police statistics do not record the number of victims, but only cases in which charges were brought, and that each of those cases may have involved several victims.

Sweden

So far, Sweden has ratified neither of the two Council of Europe conventions, but has merely signed them.[61]

However, the Criminal Code prohibits trafficking in persons (particularly women and children) for purposes of sexual exploitation (Article 1a, Chapter 4 of the Code, introduced on 29 May 2002). This provision applies to anyone who, by using unlawful force or deception, exploiting another person's vulnerability, or employing any similar improper means, recruits and gains control over that person, with a view to subjecting him/her to certain sexual offences, casual sexual relations or other forms of sexual exploitation. It also covers recruitment of victims of trafficking in human beings via the Internet. If the victim is below the age of 18, improper means need not have been used for it to apply. A person found guilty of trafficking in human beings is sentenced to at least two and at most ten years' imprisonment. Sweden has also transposed the European Union Directives on electronic commerce.[62]

Swedish law, which treats those who buy the services of prostitutes as criminals, has discouraged public advertising of those services. As mentioned in the 2003 report, Sweden is the only country where Web advertising of brothels and sex clubs is declining. On a large public site, used by men to exchange information and comments, there had been only a few messages concerning prostitution in Sweden since 1999 – all of them were warnings about the new law.[63] However, it appears that the Government is considering decriminalising the use of prostitutes' services.

United Kingdom

The United Kingdom has ratified neither of the Council of Europe conventions, but has merely signed them.

Until recently, there were no specific trafficking offences in United Kingdom law.[64] Other offences, such as facilitating illegal entry, kidnapping, unlawful imprisonment and living off immoral earnings applied instead.

On 10 February 2003[65] a new series of offences involving "trafficking in prostitution" were introduced under Section 145 of the Nationality, Immigration and Asylum Act 2002. These were simply a stop-gap

[61] More details of Swedish law can be found in the proceedings of the Council of Europe seminar on *Action against trafficking in human beings: prevention, protection and prosecution,* Riga, 21-22 September 2006 at `http://www.coe.int/t/dg2/trafficking/campaign/Source/eg-thb-sem2_2006_Proceedings.pdf`.

[62] There has been one reported case of victim recruitment for trafficking via the Internet, but we have been sent no details.

[63] 2003 report, p. 30.

[64] Arabella Thorp and Ross Young, House of Commons, Human Trafficking, Note SN/HA/3753, 17.3.2007.

[65] SI 2003/1.

measure, and were soon replaced by broader offences involving "trafficking for sexual exploitation", introduced by Sections 57-60 of the Sexual Offences Act 2003, which came into force on 1 May 2004.[66] The wording of the new offences is similar to that in the 2002 Act – they cover trafficking into, within or out of the United Kingdom, for purposes of sexual exploitation, and carry a maximum sentence of 14 years' imprisonment. Some examples of how the new offences might work are given in the Government's Explanatory Notes on the 2003 Act.[67]

These sections do not apply to Scotland, but Section 22 of the Criminal Justice (Scotland) Act 2003 created a similar offence of trafficking for purposes of prostitution.

Unusually, these offences cover not only anything done in the United Kingdom by anyone, regardless of their nationality, but also anything done *outside* the United Kingdom by a British person or company.[68] The current United Kingdom Borders Bill contains provisions that would extend the extra-territorial scope of these trafficking offences still further, to cover acts committed outside the United Kingdom by non-British nationals as well – making them applicable to acts committed anywhere by anyone.

Conviction for any of these offences will disqualify the guilty person from future work with children,[69] and the court may confiscate their assets.[70]

Neither the 2002 Act nor the 2003 Act included any provisions on trafficking for labour or other exploitation. Other, more general offences were sometimes used, such as "assisting unlawful immigration", which carries a maximum sentence of 14 years' imprisonment,[71] but the Home Office considered this legislation difficult to apply, since illegal entry can be hard to ascertain.[72] Other offences of sexual and physical violence, and those concerning fraud, forgery of documents and false imprisonment, were also available, but were considered inadequate.

Section 4 of the Asylum and Immigration Act 2004 (Treatment of Claimants, etc.) introduced new offences of trafficking for labour and

[66] *Sexual Offences Act 2003 (Commencement) Order* 2004, SI 2004/874.

[67] Paras. 104-113: http://www.legislation.hmso.gov.uk/acts/en2003/03en42-b.htm.

[68] Section 146.

[69] Criminal Justice and Court Services Act 2000 Schedule 4, as amended by Schedule 6 of the 2003 Act. The Safeguarding Vulnerable Groups Bill 2005-06 will repeal these provisions and replace them with new measures: see Library research paper 06/35 Safeguarding Vulnerable Groups Bill at http://www.parliament.uk/commons/lib/research/rp2006/rp06-035.pdf.

[70] Proceeds of Crime Act 2002 Schedule 2, as amended by Schedule 6 of the 2003 Act.

[71] Sections 25-25B of the *Immigration Act 1971*, as amended.

[72] Home Office *Setting the Boundaries* (2000), p. 105.

other exploitation. It is couched in similar terms to the sexual trafficking offences, and covers trafficking to, within or out of the United Kingdom. Like the other trafficking offences, it attracts a maximum penalty (on conviction on indictment) of 14 years' imprisonment and/or a fine. Following a Sewel motion debated by the Scottish Parliament on 12 February 2004, the new offence now applies in Scotland, as well as England, Wales and Northern Ireland[73] (came into force on 1 December 2004).[74]

The Government's explanatory notes on the Act describe this offence as follows:

A person commits an offence if he arranges for a person to arrive in or depart from the United Kingdom and he intends to exploit that person or believes that another person is likely to do so. The offence is also committed if a person arranges travel within the United Kingdom by a person if he believes that the person has been brought into the United Kingdom to be exploited, and he intends to exploit that person or believes that another person is likely to do so.

For the purposes of the offence, a person is exploited if he is:

- the victim of behaviour contravening Article 4 of the ECHR (slavery or forced labour);
- encouraged, required or expected to do something which would mean an offence is committed concerning organ removal;
- subjected to force, threats or deception designed to induce him to provide services or benefits or enable another person to acquire benefits; or
- requested or induced to do something, having been chosen on the grounds that he is ill, disabled, young or related to a person, in circumstances where a person without the illness, disability, youth or family relationship would be likely to refuse or resist.

Again, the offence can also be committed outside the United Kingdom. Offenders may be considered unsuitable to work with children, and their assets may be seized.[75]

This offence remains separate from the offence of trafficking for sexual exploitation in the Sexual Offences Act 2003. While the two offences are broadly similar (and have identical penalties), there are some minor differences. The two offences together meet the minimum requirements of the UN Protocol.[76]

[73] Motion S2M-838, Scottish Parliament Official Report 12 February 2004 col 5817-28: it can be downloaded at `http://www.scottish.parliament.uk/plenary/or-04/sor0212-02.htm`.

[74] SSI 2004/494, Article 2 (Scotland) and SI 2004/2999, Article 2, Schedule (England, Wales and Northern Ireland).

[75] 2004 Act, s5.

On 5 January 2006 the Home Office and Scottish Executive launched a national consultation exercise on proposals for a United Kingdom Action Plan on human trafficking.[77] Comments were invited on this plan, which was to address all forms of human trafficking (consultation ran for three months and closed on 5 April 2006).[78]

Definitional features of the crime of trafficking in human beings via the Internet – comments

The crucial question is: what are the elements which define the crime? Deception of the victim, or actual recruitment and transfer of the victim to the country where exploitation takes place?

Normally, and according to the definition given in Article 4 of the Council of Europe's Anti-Trafficking Convention, the crime of trafficking is committed when one of the following acts is involved: "recruitment, transportation, transfer, harbouring or receipt of persons", regardless of the specific mode of commission (threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person), or the specific means used (Internet, press, personal contact, etc.).

However, some countries seem to differ on this point.

The Greek example

The special feature of Greek law on trafficking is that the definition of the crime also refers to the means used.

Under Article 351 (1) of the Criminal Code, the crime of trafficking for purposes of sexual exploitation is committed when a person is recruited, transported or transferred inside or outside Greece, detained, harboured or delivered to, or received from, another person, using violence, threat or other coercive means, or abusing power. Under Article 351 (2) 2,[79] however, trafficking for purposes of sexual exploitation is also committed:

[76] United Nations, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, United Nations Doc. A/55/383 at 53 (2000).

[77] http://www.dti.gov.uk/consultations/page37726.html.

[78] In total they received 206 responses from individuals and organisations both within and outside the United Kingdom. In March 2007 a new Action Plan was drafted.

[79] The same conditions are also required by Article 323 A of the Criminal Code

- if the perpetrator, in order to achieve his purpose (sexual exploitation), extracts a person's consent by fraudulent means; or
- by taking advantage of that person's vulnerable position, induces compliance by promising gifts, money or other benefits.

In such cases, the legislator does not seem to make recruitment, transportation or transfer inside or outside Greece, or detention, harbouring, delivery to/receipt from another person part of the offence's definition, but expressly refers only to deception by fraudulent means or the making of promises to the victim, and to the purpose of the crime (sexual or labour exploitation of the victim, or, in the case of Article 323 A, removal of organs). As in the Council of Europe Convention, it is not necessary that the victim should actually have been exploited.

According to the Convention, traffickers are guilty of using fraudulent advertising to defraud and deceive victims, when the latter "are led to believe that an attractive job awaits them rather than the intended exploitation".[80] Thus, it is enough that the victim should have been subjected to one of the acts referred to in the definition, using one of the specified means, "for the purpose of" exploitation. Trafficking in human beings is consequently present before the victim has actually been exploited.

This means that, in Greek law, the crime of trafficking for purposes of sexual exploitation via the Internet, can be seen as having been committed from the moment when the victim is convinced by the perpetrator's promises, i.e. s/he does not need to have been actually recruited, transferred, harboured, etc.

Article 4 of the Council of Europe Convention, on the other hand, does not state that the crime is committed only when certain means are used. Although it refers to various means (threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, or of the giving or receiving of payments or benefits, to achieve the consent of a person having control over another person), the crime of trafficking is always present when one of the following acts, "recruitment, transportation, transfer, harbouring or receipt of persons", is committed, regardless of the mode of commission (force, deception, etc.) and the specific means used (Internet, press, personal contact, etc.).

This is an important point, since, if a victim is persuaded, e.g. by a fraudulent promise made on an Internet site or chat-room, to leave her/his home country, and if her/his belief in that promise is enough to substantiate the crime of trafficking, then s/he will be able to prosecute the

[80] Para. 82 of the Explanatory Report on the Convention.

offender, instead of simply going home, as if nothing had happened. In trafficking in human beings cases, the issue is not just the promise, but its possible repercussions for a vulnerable victim, possibly living in miserable conditions, who may be induced by that promise to leave her/his home country, with all the hardship that entails.

Drawing conclusions from what we have so far said about legal measures taken by Council of Europe member states against victim recruitment via the Internet, we can say that:

- laws on trafficking in human beings can generally be considered satisfactory. Though only seven members have so far ratified the Anti-Trafficking Convention, they do have anti-trafficking provisions in domestic law, while some have transposed the Palermo Protocol, and European Union states have transposed the Framework Decision on trafficking in human beings.
- Although only two member states (Albania and Romania) have ratified both the Anti-Trafficking and Cybercrime Conventions, half have ratified the Cybercrime Convention, and the European Union states have also transposed the relevant European Union legislation.
- However, we should not underestimate the importance of the fact that laws are not uniform – which is not conducive to efficient prosecution of offenders. Most member states have still to address the question of providers' liability and their obligations concerning retention of data (the European Union states have not yet transposed its relevant legislation).

Administrative measures

Administrative measures chiefly involve the setting-up of special bodies to combat trafficking in human beings. Equally important, however, are the technical measures which these bodies then take to prevent and/or prosecute trafficking, and these will also be examined below.

It must be emphasised that many European countries have established special computer units to take specific measures against cybercrime. However, there are no such units in countries regarded as source countries, one reason for this being the state of their Internet infrastructure.

The following are some examples of such units:

Germany

The police have set up special units to detect computer-related crime. The Central Service for Research on Data Networks (CARD) has power to conduct Internet searches *ex officio*. Known as "Internet patrolling", this involves collecting evidence on all types of Internet-based crime – which is then passed to the relevant authorities. Special attention is paid to monitoring and exploiting technical data.

Greece

The Police Security Division's Computer Crime Unit was established only in 2004 (by Presidential Decree 100/2004), with offices in Athens and Thessalonika. It has scored numerous successes in dismantling Internet-based pornographic networks. Its experience of trafficking in human beings recruitment via the Internet is still limited, however, to a few cases (described in Part I above, page 37). According to the Unit, some 2 trillion dollars were trafficked electronically in 2006 in 700 000 transactions.

Poland

In August 2006 a national team (at National Police Headquarters), and also provincial teams, were established to fight trafficking in human beings. Co-ordinators were also appointed to monitor the Internet – communicators, chat-rooms, forums, discussion lists, etc.

The problem with these units is that they normally intervene only on receiving information concerning a suspect activity. They do not investigate Web sites *ex officio*. I believe that, primarily for preventive purposes and eventually, of course, prosecution, the police should have a separate unit to monitor the Internet *ex officio* (even if it cannot do this exhaustively), in an effort to locate sites which recruit (or at least attempt to recruit) victims of trafficking in human beings, or offer their services on the Web.

Technical measures

Criminals are often quicker to exploit new technologies than law-enforcers who, to some extent, always seem "behind the game". Certainly, criminals are staggeringly ingenious in using the Internet to purvey child pornography, arrange payments, and escape detection.[81]

According to the 2003 report, technical aspects are crucial to the development of sites which exploit all the Internet's possibilities. In many cases, the server's geographical location (possibly in a country with little or no legislation in this area) neutralises the law. For example, some operations are prohibited in Europe, but allowed in the United States – so a hyperlink from a European to an American site is all it takes to circumvent the law.[82]

I believe that we should make a distinction between technical measures which:

- can contribute to prevention;
- can effectively facilitate prosecution in cases of recruitment of victims of trafficking in human beings via the Internet, and
- can do both.

[81] Nick Garlick, Europol, presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking, Strasbourg, 7-8 June 2007.

[82] 2003 report, p. 14.

Technical measures to prevent recruitment of victims of trafficking in human beings via the Internet

Technical measures taken by governmental organisations

Greece

In May 2006 the status of the special committee established to co-ordinate enforcement of Act 3064/2002 and the introduction of legislative or other measures to combat trafficking in human beings was upgraded,[83] giving it power to propose such measures itself.

One of the committee's immediate priorities was promotion of a 24-hour help line (197), operated by the National Centre for Social Solidarity (EKKA), with adequate, multilingual staff.

In June 2007, the Ministry of Finance set up a new body, the DART (Digital Awareness and Response to Threats).[84]

Its chief aims are to increase public awareness, avert and protect against the dangers inherent in the new technologies, and provide advice on safe Web surfing, particularly for children and parents.

Poland

As part of the National Anti-Trafficking in Human Beings Programme 2005-2006, the national and provincial teams responsible for combating trafficking in human beings set up a Web site[85] to provide comprehensive and, as far as possible, up-to-date information on trafficking.

The Web pages of police departments and social organisations, such as La Strada and the Foundation against Trafficking in Women, provide advice for people going abroad to work:

"1. Accept job offers from employment offices only.

2. Do not accept offers from strangers, or people casually met.

3. Collect as much information on the intermediary as possible, and make sure that he operates lawfully.

4. Ask the intermediary for information on the employer – address, phone number, etc.

[83] *Official Gazette* B-493/18.4.2006 and addendum *Official Gazette* No. 581/9.5.2006.

[84] More information can be found at `http://www.dart.gov.gr/`.

[85] `http://www.mswia.gov.pl/portal/pl/166/2000`.

5. Preferably take with you the address and phone number of the Polish embassy or consulate in the country you are going to. You can turn to them for assistance."

The following information is also disseminated in leaflets, the press and on the Internet:

"Distrust anyone who proposes:

- illegal work,
- travel to an "attractive" destination,
- attractive work for women only,
- work which requires no knowledge of the language, qualifications, etc.,
- departure at short notice, leaving you no time to think or consider the proposal,
- help with obtaining documents (e.g. passports) and crossing borders,
- coverage of all costs connected with the journey (transport, accommodation, documents, board), deductible from future earnings".

Preventive measures taken by private entities

Sites (supposedly) offering protection against scam marriage agencies

There are sites which claim to offer such protection, but there is no guarantee that they themselves are safe.

One such site[86] carries a list of "honest" and "dishonest" marriage agencies in Ukraine and Russia, as well as a list of blacklisted sites.

Its creator claims to be American,[87] and to have spent many years looking for a wife in Ukraine and Russia (!). "I have used just about every major agency. I have taken my experiences and added American business ethics to create Kherson Girls". The site advertises its services as follows: "Your love is true … Is your loved one real? – Order Scam Check to find out. We will deliver one red rose to the address you provide us with. Our couriers will personally visit the address, and report back with their findings. This includes a description of whether the address or the recipient was found, and a photograph of the delivery, in the event that the person exists. This option includes a check in local telephone directories, in the event that we are unable to find the recipient. We accept all

[86] http://www.honestmarriageagencies.com/honest.html.

[87] Kevin Hayes (kevin@khersongirls.com).

major credit cards, PayPal and United States check/money order. Visit this page to learn about acceptable payment methods."

Points to ponder

- This site offers fee-paying scam-check services ($44 for normal services and $59 for an "advanced scam check", which includes passport verification – a rather large sum for Ukraine and Russia. At the very top of the site, the founder declares "this site does not accept money from sponsors or agencies" and adds that he pays for it "out of his pocket" – although he takes money for "normal" and "advanced" scam checks!
- The site also carries a database of scammers, but gives only the supposed scammers' names, and no details of the sites. In other words, it does not give potential victims the information they need to avoid existing scammers.
- Obviously, a site which charges for its services, while claiming not to, should be treated with great caution. The founder's faulty English also raises doubts concerning his claim to be American.

Protection against scam modelling agencies

There are, however, sites which – unlike the above – are serious, provide free advice on scam modelling agencies, and help to alert would-be models to possible dangers.

In the United Kingdom the NGO "Safe Modelling" has set up such a site, which gives detailed advice on avoiding fake agencies.[88]

"Safe Modelling" provides a free service for models and aspiring models. It describes itself as a private site, which is not government-run and is not itself a modelling agency (which suggests that it has no vested interests). It declares: "This site has been set up to make life easier for photographic models and to make life more difficult for the conmen, scam artists and timewasters who try to rip off models".

It carries links to other sites, but warns that it cannot necessarily guarantee that all of them are honest and trustworthy. "Unlike some other advice sites, we will not recommend any modelling agencies or photographers". Since November 2006, it has also carried an on-line petition to the Prime Minister, asking the government to prohibit the charging of up-front fees by modelling agencies, model management and promotion services, etc. and subject them to yearly licence review.

It gives three reasons for the large number of victims:

[88] http://www.safemodelling.org.uk.

- Most would-be models are young and find it hard to spot the crooks;
- People believe the lies because they want to believe them; and
- The rogues are easier to find, because they advertise (most genuine agencies do not).

It lists typical features of scam modelling agencies, and offers advice on avoiding and checking on them. For example:

"Some scams may be illegal, but it may be reasonable to also include the better-organised 'agencies' that act within the law (they are licensed as model agencies).

How to check: Don't rely on identification, business cards or whatever, they could be fake. Don't assume that it must be OK if the person who approaches you happens to be the same sex as you. Rely on your common sense and on the presence of a large, male friend. Never go to a hotel room and don't accept anything to drink. Make it clear to the person that you'll be bringing your boyfriend/father with you – no reputable agent or scout will have a problem with that."

It also describes situations in which dishonest "agencies" pass themselves off as something else. There are a few famous names in modelling – highly respectable and successful agencies, known to nearly everyone. Crooks have been known to use their names, or very similar names, to deceive their victims. Alternatively, they may claim to be talent-scouting for those agencies.

"How to check: Look the famous-name agency up in the phone book, ring them up and ask them."

The following is the site's advice on scam-spotting:

"Not all modelling scams are easy to recognise because many of the advertising claims and practices are very similar to methods used by some genuine modelling agencies.

However, below are some common advertising claims that should make you suspicious:

- 'No Fees'. Genuine agencies don't charge any upfront fees they only charge commission on the work that they actually find their models.
- 'Earn £50 per hour or £300 per day.' Only experienced models can expect to receive large salaries.
- 'Work full or Part Time.' The hours of a model are uneven and sporadic. You will not have the flexibility to choose your own hours.
- 'Male or female, no age limits.' Some ads encourage people of all shapes, sizes, and ages to apply for commercial modelling work. Opportunities do sometimes exist for 'real people' models, but they are rare.

- The single biggest giveaway – they accept you! In fact they accept almost everyone, although, if they're clever, they'll try to make you think that you've been specially chosen!
- And always remember that it is very unusual for genuine agencies to advertise, so the fact that you even saw the advert is a very good indication that it's just a scam!"

Concerning photographers, the site warns that "nothing in life is completely safe", and that potential models should remember that not all supposedly commercial photographers are genuine, that photography gives sexual predators a unique opportunity to meet new victims, and that some may set up "businesses" for this very purpose – in much the same way as paedophiles who look for work in children's homes. Some of the advice given:

- "Make it clear from the outset that someone will be going with you. No reputable photographer will object to this.
- Always make sure that you know where the photography will take place and that you have a landline phone number there, not just a mobile.
- Arrange with a parent or friend (parents are usually more reliable) that you will ring them both when you arrive and leave, and will ring them at prearranged times, such as once per hour on the hour. You will probably get absorbed in the modelling work and may forget to ring, so make it clear to this person that s/he must ring you if you don't ring in as arranged.
- Have a prearranged codeword in case you find yourself in a situation that you're a bit unhappy about, so that your contact can go to the studio immediately to prevent a possible situation from getting out of control.
- Have another prearranged codeword for emergency use. If you use the emergency codeword your friend/parent must phone the police immediately and tell them exactly where you are and that you need immediate help. We have only ever heard of one situation in which a model had to get help – the contact was her mother, who rang the police immediately. Apparently there was some confusion because the police thought that she had told them that her daughter was a police officer – anyway, whatever was said, the police arrived in less than 1 minute! Of course, none of this will be any help to you unless your contact is 100% reliable AND knows exactly where you are".

The site also warns interested people that working abroad can be especially risky.

"Young, attractive girls could end up being forced into prostitution. Here are some sensible precautions:

- Never give your passport to anyone, always keep it safely with you and check into airports and hotels yourself, keeping your flight tickets, money, credit cards, mobile phone and passport with you at all times. If anyone puts pressure on you to hand over any of these items, say that you've lost them – and then get some help!
- Always make sure that your family or a trusted, reliable friend knows you are leaving the country, where you are going, how you can be contacted and when you should be back.
- Make sure that you have a mobile phone that will work in the country you are going to, in case you need to call home in an emergency. Make sure it has plenty of credit.
- Make sure you have the details of the British Embassy in the area you are going to, so that if necessary you can contact them or go to their offices. They will protect you. If there isn't a British Embassy (or equivalent) in your destination country ask the Foreign Office (before you leave the United Kingdom) who you should go to if you need help – there will be an arrangement with another foreign embassy. In cases of desperation, any embassy will protect you. In some countries an embassy may be the safest place to go to.
- Never leave home without either having a return ticket, or the funds to buy a return for yourself if things don't work out."

It also explains how "chaperones" can protect vulnerable people, and mentions two types of danger which their presence helps to avert.

- "Physical assault, including rape;
- Emotional pressure (to do something that you're not happy about) is another possibility. Bear in mind that when you are being photographed in someone else's environment you may not feel as confident about asserting yourself as you would be if you were in your own home. Bear in mind too that most photographers are older and have much more experience of life than most of the models they photograph, and they can be very persuasive."

It notes that children must be chaperoned at all times – this is a legal requirement.

Initiatives on the "Safe Modelling" pattern should be taken up and expanded worldwide, since prevention holds the key to reducing trafficking in human beings, particularly when victims are recruited via the Internet – which makes counter-action harder.

Preventive measures taken by European Union institutions

The European Union has a forum on organised crime prevention,[89] comprising national law enforcement authorities, business and professional groups, academic researchers, non-governmental organisations and civil society in general. It was set up 2001, to discuss new approaches to preventing organised crime. Subjects covered at its first meeting,[90] in May 2001, included trafficking in human beings, fraud and the counterfeiting of non-cash means of payment, the private sector's role in preventing economic and financial crime, etc. The European Union has also set up a financial programme, *Hippokrates*, to fund European Union-wide prevention projects.

According to the European Commission, crime prevention must be addressed, first and foremost, at local level.[91] The subsidiarity principle must be applied. At the same time, there are enough similarities between crime problems in various countries to make a common approach both possible and useful. Moreover, many European Union policies can have direct impact on crime, e.g. the regional development programmes, which set out to improve the urban environment, or reinforce social and economic cohesion.

Technical measures for effective prosecution in cases of victim recruitment via the Internet

Measures taken by national authorities

Measures for the effective prosecution of traffickers who recruit their victims via the Internet have been taken at both national (by governmental or non-governmental institutions) and international level.

Most national measures target child pornography, although a few countries have specific measures on Internet-based trafficking for other purposes.

[89] `http://ec.europa.eu/justice_home/fsj/crime/forum/wai/fsj_crime_forum_en.htm`.

[90] The latest Safer Internet Forum, on "Safer Internet and online technologies for children", took place on 20-21 June 2007 in Luxembourg, and comprised three workshops: online-related sexual abuse of children, in particular grooming; assessing the need for awareness-raising for creating a safe online environment for children; and the impact and consequences of convergence of online technologies for online safety.

[91] See the point made by the European Commission at `http://ec.europa.eu/justice_home/fsj/crime/forum/wai/fsj_crime_forum_en.htm`.

Measures taken by governmental organisations

As we have said, most of the measures taken so far focus on Internet child pornography, but some can be extended to other forms of sexual exploitation via the Internet.

Albania

In co-operation with all the parties involved, the Anti-trafficking in human beings Authority is in the final stages of setting up a country-wide, toll-free "help line", which can be used to report cases of trafficking. The Authority is also setting up a database, where representatives of the Ministry of the Interior, the Ministry of Foreign Affairs, the Ministry of Labour and the Protection Centres for Victims of Trafficking will record cases of victims returned, referred, dealt with and protected in Albania.

Belgium

In Belgium the -eCops system[92] was created mainly to fight child pornography, but it also addresses other Internet-related crimes, and can be used to report offences committed via or against the Internet.[93]

Italy

In connection with Act No. 38/2006 on child pornography online, the Polizia Postale has recently adopted Microsoft's CETS (Child Exploitation Tracking System) – a management and investigative tool for police use only, which allows them to "trace" all attempts to download and share child pornography. CETS was developed jointly by Microsoft Canada, the Royal Canadian Mounted Police (RCMP) and the Toronto Police Service, and was officially launched on 7 April 2005.[94]

Measures taken by NGOs

Belgium

Childfocus has set up a site[95] with a hotline which the public can use anonymously to report crimes connected with child pornography.

Childfocus was also the source of an initiative, taken in June 2000, to bring together, at European level, various NGOs dealing with the dis-

[92] http://www.ecops.be/.

[93] Information concerning the Federal Computer Crime Unit in Belgium can be found at http://www.polfed-fedpol.be/presse/presse_detail_fr.php?recordID2=1157.

[94] See more details at: http://www.microsoft.com/presspass/features/2005/apr05/04-07CETS.mspx.

[95] http://www.childfocus-net-alert.be/.

appearance and/or sexual exploitation of children (the European Centre for Missing and Sexually Exploited Children). Its site was created with the support of the European Commission, as part of its Action Plan for a Safer Internet. Childfocus works with the police and judicial authorities, under a co-operation agreement concluded with both.

Italy

Some Italian NGOs and local authorities have already started to use the Internet as a tool to prevent trafficking and assist trafficked persons and potential victims already in Italy.[96]

NGOs like On the Road and Gruppo Abele have set up comprehensive Web sites, which are increasingly used by "friends" and "partners" of victims to find information, put them in touch with help centres, and eventually launch social assistance and integration programmes for them.

The Province of Lecce is modifying its Web site to increase its impact and make it more user-friendly. It will be publicising the site:

- alongside "sexual service" classified ads in newspapers and periodicals;
- on jobs offered/sought Web sites;
- at Internet points;
- in money-transfer agencies.

The last two types of venue have been chosen because they are widely used by migrants and those whom the social services are trying to help.

The indoor outreach units of the Segnavia – Padri Somaschi project (Milan)

The indoor outreach units are a good example of how the Internet can be used to identify potential cases of trafficking. Noticing that Web sites offering sexual services had proliferated in Milan in the previous three years, they decided to:

- map and analyse the main Web sites;
- make a selection;
- set up a special team (outreach workers and cultural mediator);
- contact the numbers posted on the Web sites, and
- meet some of the contacted persons directly, in the apartments where they work (152 persons were met in 2006).

[96] Isabella Orfano, *The role of civil society in preventing and combating the misuse of the Internet for the recruitment of victims of trafficking in human beings*, Presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beingstrafficking in human beings, Strasbourg, 7 June 2007.

In this way, two cases of trafficking were detected, and the victims assisted.

It is worth noting that the nationalities of the prostitutes (mainly Hungarian and Brazilian) who appear to recruit clients via the Internet are not the same as those of the victims (mainly Romanian, Nigerian, Moldovan, etc.) generally assisted by the anti–trafficking organisations.

The Headway online transnational database[97]

This database is operated under the European Union's EQUAL Community Initiative by the Development Partnerships of Headway – Improving Social Intervention Systems for Victims of Trafficking (of which On the Road is part), with ten other Italian private and public organisations and institutions, and other European partners.[98]

The Headway database covers organisations and institutions working on trafficking, and is intended to facilitate contact between them and other interested bodies. In the last decade, many Web sites and databases on trafficking and related issues have been set up throughout the world. None of these, however, is specially designed to connect, and provide up-to-date information for, professionals who need to contact their counterparts in other countries, so that they can better serve the needs of the people they assist.

Its main objectives are:[99]

- To facilitate rapid identification of, and contact between, institutions and organisations active in the anti-trafficking sector:

– in European Union countries and non-European Union countries;

– of different kinds (NGOs, local authorities, government bodies, universities, etc.);

– working on different forms of trafficking (sexual exploitation, forced labour, begging, criminal activities, organ trafficking, illegal international adoptions, mail-order brides);

[97] http://www.osservatoriotratta.it/headway/.

[98] The transnational partnership consists of six national DPs which represent, not only very different national and regional contexts (of origin, transit and destination), but also various types of public and private agency engaged in the anti-trafficking field: Estonia: Integration of Women Involved in Prostitution into the Labour Market; Germany: Reintegration of Victims of Trafficking – Strengthening of National Supporters; Italy: Osservatorio e Centro Risorse sul Traffico di Esseri Umani; Lithuania: Integration and reintegration of victims of human trafficking into working society; Poland: IRIS – Social and Vocational Reintegration of Women Victims of Trafficking; Portugal: Cooperação-Acção-Investigação-Mundivisão.

[99] C. Bellini, A. Gratti, "The Headway database: An on-line transnational tool for anti-trafficking service providers", in AA.VV., *Headway – Improving Social Intervention Systems for Victims of Trafficking*, Warsaw, pp. 216-219, referred to by Isabella Orfano in her presentation, loc. cit.

- addressing different target groups (male minors, female minors, men, women, transgender people, communities, social and health workers, educators, teachers, law enforcement officers and judicial personnel);
- taking different types of action (assistance and associated activities directly aimed at trafficked persons);

- To facilitate the exchange of up-to-date information on organisations, projects, activities and services concerned with trafficking;
- To encourage networking and co-operation between organisations working on trafficking.

Information on the Headway database is public-access: users do not need passwords, and there are no other restrictions on access.

The database was officially launched in Rome on 25 June 2007.[100]

Monaco

Action Innocence Monaco[101] is an NGO established on 20 October 2002. Its chief aim is to protect children on the Internet (mainly against paedophile and pornographic sites). It has the support of Prince Albert II and the co-operation of the Directorate of National Education and Public Security of the Principality of Monaco. It sets out to: mobilise public institutions and authorities; provide preventive information for parents and children; work with education and health professionals; co-operate with computer professionals in devising and up-dating comprehensive technical means of filtering and blocking Web sites, chat-rooms and discussion forums used by predators.

In Monaco psychologists from the organisation talked to over 800 school classes, i.e. 10 000 pupils, between 2003 and 2007, alerting them to the dangers.

Action Innocence's slogan neatly summarises the aim of prevention: "*Prévenir, c'est éviter le pire. Ne pas lutter, c'est l'encourager*" (To prevent is to avert the worse. Not to fight is to encourage it).

Action Innocence regularly produces preventive items aimed at young people and parents: mouse pads carrying advice on security, the "Your Child and the Internet" guide, the Kiloo CD-Rom,[102] cartoons illustrating the dangers, etc.

Action Innocence Switzerland set up a preventive technologies department in 2003, mainly to devise filtering techniques:

[100] http://www.osservatoriotratta.it/headway/.

[101] http://www.actioninnocence.org/.

[102] http://www.kiloo.org/.

- www.filtra.info: responds to intense demand by users, principally parents worried about their children's safety. This site sets out to provide clear, detailed information on the various filters available on the market. New software is regularly tested, and the site updated twice a year;
- www.logprotect.net: offers free downloads of Logprotect software, which prevents children from providing personal data (e.g. address, phone number, etc.) on the Internet;
- AntiPedoFiles: is an investigative database, mainly used by the police and, secondarily, the private sector;
- LogP2P: Develops specialised software to locate paedophile sites on "Peer-to-Peer" (P2P) networks, and introduces this product to the judicial authorities.

Poland

The NGO *La Strada* runs awareness campaigns, but also monitors Internet forums containing suspect job offers.

It operates an advisory phone service (hotline) and a Web site providing information on work abroad, missing persons and violence. It also takes part in chat and discussion sessions on work abroad, warning against the possible dangers of trafficking.

United Kingdom

The Internet Watch Foundation (IWF)[103] runs the United Kingdom's only authorised Internet hotline, which the public and IT professionals can use to report potentially illegal content encountered online. Its brief covers:

- child abuse images hosted anywhere in the world;
- criminally obscene content;
- content which incites to racial hatred;
- inappropriate chat or behaviour with or towards children online.

IWF works in partnership with British Government departments, such as the Home Office and the Department of Trade and Industry, in promoting initiatives and programmes to combat online abuse. This dialogue extends beyond the United Kingdom and Europe, the aim being to ensure greater awareness of global issues and responsibilities.

Over 70 leading Internet, IT and mobile phone operators and media organisations are already members of IWF and working with it to minimise availability of potentially illegal content online.

IWF has a wide range of supporters, public and private, including:

[103] http://www.iwf.org.uk/.

- ISPs, CSP, host companies
- Portals
- Mobile operators
- Search providers
- Filtering and software vendors
- Financial sector – to disrupt activity
- CSR reasons

It also has international partnerships with the European Union Safer Internet *plus* Programme, the INHOPE Association, and 28 hotlines in 25 countries worldwide.

Measures taken at international level

Virtual Global Taskforce (VGT) is an international partnership of law enforcement agencies, which was set up to fight online child abuse, and could serve as a model for combating the recruitment of victims of trafficking in human beings. It comprises the Australian High Tech Crime Centre, the United Kingdom's Child Exploitation and Online Protection Centre (CEOP), the Royal Canadian Mounted Police, the United States Immigration and Customs Enforcement authorities, the Italian and French law-enforcement authorities, Europol and Interpol.

The VGT was set up as a global response to child exploitation, and operates a round-the-clock hour alert system seven days a week, allowing it to respond instantly to reports of children at serious risk. Young people all over the world can, if they have been abused, make a virtual complaint simply by clicking on an icon, and the police can respond immediately. This is based on a secure information-sharing infrastructure, and time zones are covered by the countries involved. The VGT alert system protects children on and offline at low cost with high impact. International co-operation is crucial, and this model is an effective way of achieving it. The VGT has scored some successes over a short period, and been able to stop ongoing abuse within two hours of a complaint's being made. There are clearly significant differences between child-abuse and victim recruitment online, and counter-measures effective for the first are not necessarily so for the second; however what the VGT does show is that international co-ordination of action on the Internet can work. "The criminals work globally, then so should we."[104]

[104] According to Nick Garlick, Europol, at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7-8 June 2007.

Measures for prevention and prosecution taken at regional level

Measures taken by the European Union

The work of the two European Union law-enforcement institutions, Europol and Eurojust, can be seen as contributing to the prevention and prosecution of trafficking, since trafficking in human beings is a major priority for both.

Europol

Since 2001[105] Europol has extended its range to cover all forms of serious transnational crime. Its core activity is to support member states in their efforts to prevent and combat serious and organised crime, including trafficking in human beings.

Europol has contributed to many successful anti-trafficking in human beings operations by helping member states with information exchange, co-ordination and intelligence analysis.[106] These operations have resulted in the dismantling of numerous criminal networks, and the arrest and imprisonment of many traffickers.

The Analytical Work File (AWF) is one example of the support that Europol can provide.

The AWF was set up in 2001 to help participating member states to prevent and combat the activities of criminal networks involved in the production, sale or distribution of child pornography, and associated types of crime within Europol's mandate, e.g. sexual exploitation of children. So far, it has been immensely, and increasingly, successful.

Its investigations have led to the identification of numerous suspects and saved many children from further abuse. In 2005, it supported two major investigations[107] – "Operation Icebreaker" Nos. 1 and 2, involving fourteen European Union and non-European Union countries, and leading to the identification of over 200 suspects. So far, it has helped to identify a total of some 400 suspects belonging to various criminal networks involved in offences related to child-abusive material on the Internet.

[105] Decision of the European Union Council of 6.12.2001 on the extension of Europol's competences, OJEC, C 362 of 18 December 2001.

[106] See Part 1, page 46, examples of successful Europol operations.

[107] Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet, January 2006.

Europol also provides training for police officers and the judiciary on measures to combat sexual exploitation of children on the Internet, the aim being to help them develop the knowledge and skills they need to attack and dismantle paedophile networks. Thoroughly practical in its approach, this training also sets out to build fundamental skills relevant to investigating child abuse on the Internet, and harmonise police investigative standards. Another aim is to introduce/disseminate the latest investigation techniques and methods, and promote the pooling of lessons learned. Opening the courses to members of the judiciary, e.g. prosecutors, magistrates and judges, helps to give them a better understanding of the crime, the methods used by investigators, and the constraints they may have to contend with. In combating crime, Europol co-operates closely with Eurojust, the European Union's judicial instrument.

Eurojust

A total of 32 cases of trafficking in human beings were referred to Eurojust in 2006.[108] From January to April 2007, 37 cases were already registered, which shows, as a Eurojust official put it, that "this issue is getting more and more important, because there is still a growing market, where a lot of money is earned".[109]

Eurojust operates on three levels. The first is the Plenary Meeting of all 27 national members; the second is co-operation involving only members working on specific cases; the third is co-operation between investigators and prosecutors working on a specific case, plus co-operation with Europol, providing access to all European Union police authorities and data.

Measures taken by the Council of Europe

In addition to the work which the Council of Europe has been doing for a long time on action against trafficking in human beings, with numerous training and awareness seminars, we should like to focus in this section on the possibilities offered for prevention and prosecution by GRETA – the monitoring mechanism provided for in the Convention on Action against Trafficking in Human Beings (CETS No. 197, Chapter VII, Articles 36, 37 and 38). GRETA's purpose is not simply to monitor implementation of the Convention, but also to put pressure on the member

[108] According to Benedikt Welfens, German Desk Deputy, in his presentation at the Council of Europe Seminar on the misuse of the Internet for the recruitment of victims of trafficking in human beings, Strasbourg, 7 June 2007.

[109] Benedikt Welfens, loc. cit.

states to take all the measures needed to prevent the crime, prosecute perpetrators and protect victims.

Under Article 36 (4), the procedure for electing members of GRETA is determined by the Committee of Ministers. This procedure is an important part of implementing the Convention, and the drafters of the Convention understandably felt that the Committee of Ministers should be left to define it, with the Parties themselves electing the members.[110] Before deciding, however, the Committee of Ministers is to consult all the Parties and obtain their unanimous consent. This requirement recognises that all the Parties to the Convention should have an equal say in determining the procedure.

Article 38 describes how the monitoring procedure works, and how GRETA and the Committee of the Parties interact.

Article 38 (1) indicates that monitoring will be organised in cycles, and that GRETA will autonomously decide, at the beginning of each cycle, which provisions are to be monitored.

GRETA will also decide how monitoring is to be effected (Article 38 (2)). It may include a questionnaire or other requests for information. Parties are required to supply any information requested.

GRETA may also receive information from civil society (Article 38 (3)).

As a further aid, GRETA may organise country visits to obtain more information (Article 38 (4)). The drafters stressed that these visits should be a subsidiary means, carried out only when necessary. They must be organised in consultation with the relevant authorities in the country concerned and the “contact person” it appoints.

Paragraphs 5 and 6 describe the drafting phase of both the report and GRETA’s conclusions, and make it clear that GRETA is required to engage in dialogue with the Party concerned when preparing the report and its conclusions. Indeed, such dialogue holds the key to proper implementation of the Convention. GRETA then publishes its report and conclusions, with any comments by the Party concerned, and sends them simultaneously to the latter and to the Committee of the Parties – thus completing its task in respect of that Party and the monitored provision(s). Its reports are published as adopted, and may not be altered or amended by the Committee of the Parties.

Article 37 sets up the monitoring system’s other pillar – the “Committee of the Parties”, which is more political in character. This ensures equal participation of all the Parties in the decision-making process and

[110] See para. 358 of the Explanatory Report.

monitoring procedure, and also strengthens co-operation between them, and with GRETA, on effective implementation of the Convention.

Article 38 (7) deals with the Committee's role in the monitoring procedure, stating that it may adopt recommendations indicating action which the Party concerned must take to implement GRETA's conclusions, setting a date (if necessary) for submission of details of the action taken, and promoting co-operation to ensure the proper implementation of the Convention. This machinery will ensure that the independence of GRETA's monitoring function is respected, while giving the dialogue between the Parties a "political" dimension.

There are plans for a conference in Strasbourg on 8 and 9 November 2007, at which member and observer states, international governmental organisations and non-governmental organisations will be invited to contribute to setting-up of the Convention's monitoring system (GRETA and Committee of the Parties).

Great hopes are vested in GRETA and its work. It is a promising tool, and effective implementation of the Convention depends on it.

Other measures

Another technical measure which might be considered is "legislative theatre"[111] – a method devised by a theatre group in Rio, which involves putting pressure on governments to introduce new laws in areas where society faces problems, and legislation is generally needed.

The Rio group produces plays for various audiences, and prepares interactive mailing lists for consultation of people who may be useful in preparing laws.

In 2006, the group was invited to present a play on marriage agencies in Munich. The interesting plot runs as follows:

"Once the bridegroom has chosen his wife, the agency imports her, promising her marriage and the wonderful lifestyle of a European princess. Obviously, the young women involved are very poor and full of hope – also very naive. When they arrive, one of the agency's promises is redeemed: they marry. Once married, most – though not all – husbands treat them like purchased slaves, in the kitchen and in bed. More often than not, they do not speak a word of German, and have difficulty learning the language. They have no friends, and are sometimes forbidden to go out without their husbands, who keep them under strict control (masters and slaves). A wife who decides to leave her husband can do it, but

[111] See *Legislative Theatre*, Routledge, London/New York 1999.

not easily – the only problem is that she automatically loses her German nationality, and is sent back to her own country by the police. She is punished: not him!"

The group has scored numerous successes with this method, reportedly paving the way for approval of 13 new laws in 4 years. This is certainly an original way, not only of raising public awareness, but also of putting pressure on public authorities.

Evaluation of the current situation

The problem is that trafficking for sexual exploitation is not as obvious as child pornography – so that detecting sites which offer sexual services based on exploitation is not easy. Creating filters, of the kind used to counter child pornography, seems to be rather difficult technically. The same applies to sites involved in exploitation. To protect potential victims, countries should set standards (preferably harmonised at international level) for various types of site, e.g. job or marriage agency sites. However, since no standards can be set for sites offering sexual services, constant surfing by the police authorities, combined with action to alert potential victims and clients, is the only way of fighting exploitation in this area.

Action to prevent recruitment of victims of trafficking in human beings via the Internet is impeded by:

- Shortcomings in legislation;
- Shortcomings in technical means and infrastructure, mainly concerning telecommunications;
- Both the above.

The present situation regarding anti-trafficking in human beings legislation is generally more satisfactory than it was at the time of the 2003 report. All the member states have laws making trafficking in human beings a crime.

Most have either incorporated the Additional Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children (the Palermo Protocol) to the United Nations Convention against Transnational Organised Crime in domestic law, or added provisions on trafficking in human beings to their criminal codes. In doing so, most have also adopted the definition given in the Protocol.

Some countries have adopted a definition which covers trafficking in human beings either as a national or transnational crime (e.g. Romania, in Section 12 of Act 678/2001). Others have adopted a broader definition (e.g. Bulgaria in Articles 159b and 159c of the Criminal Code), extending it, via aggravating circumstances, not only to cases where the victim is trafficked from one country to another, but also to cases where an organised criminal group is involved. There are also countries, however, which use a narrower definition than that given in the UN Protocol. Greece, for instance, has a rather limited definition of exploitation, since the provision which makes trafficking a crime (Article 323A of the Criminal Code) does not cover all forms of exploitation, but only sexual and labour exploitation, as well as organ removal, and recruitment of minors to commit terrorist acts. Some countries do not specifically state that the consent of the victim to exploitation should have no bearing on the means used by the exploiters, as required not only by Article 4 (b) of the Council of Europe Convention, but also by Article 3 (b) of the Palermo Protocol.

In defining the crime of trafficking of minors, some national laws assume use of the same means as those used for adults (e.g. Greece). National definitions of the crime also vary, depending on the means used. In Greece, for example, if promises have been made to win the victim over, recruitment or transfer – normally necessary elements in definition of the crime – are not required.

Some countries make the victim's age a factor in penalty-setting. In general, trafficking – not only of children – carries a broad range of penalties. This may encourage traffickers to "shop around" for the country where they face the lowest sentence. One of the main shortcomings in national law is failure to punish (as required by Article 19 of the Anti-Trafficking Convention) "consumers" who knowingly use the services of victims of trafficking in human beings. Only Greece does this, while Sweden has criminalised the use of prostitutes. Croatia now intends to introduce a new provision, making it an offence to use a victim's services, in accordance with Article 19 of the Convention.

These problems are mainly due to the fact that not all the member states have ratified the Convention.

The existence of two different levels of telecommunications infrastructure and Internet use is another problem. There is a net legislative discrepancy between Council of Europe member states which are also European Union members, and the others; only those within the European Union have satisfactory laws on Internet-related crime and provider liability.

The overall impression is that there are countries which have adequate legal and technical infrastructure to fight Internet-based trafficking, and countries which, even if they have the laws, lack the technical capacity to do so.

The majority of the countries which have ratified the Cybercrime Convention are not among the most advanced technically. In other words, there are countries which have the laws, but not the technical means, to fight and punish Internet-based crime, and countries which have the technology, but not the laws. Some countries have infrastructure which allows them to detect and react to computer crime rapidly; some have infrastructure which allows them to detect fairly well, but not react; and some have no adequate infrastructure at all. Obviously, the two last are most at risk from victim recruitment via the Internet, and the fact that such recruitment has not so far assumed large proportions is, as we have said, to some extent due to their low levels of the Internet use and poor telecommunications infrastructure.

Even though considerable progress has been made since the 2003 report, there are still – alas – countries which do not oblige providers to monitor information they transmit or store, or look actively for signs of illegal activity.

The Cybercrime Convention is far from being implemented in Europe, since fewer than half the member states have ratified it. Nevertheless, there has been net progress, at least in the European Union member states, which have extensive legislation on Internet-related crime, and on providers' liability and obligation to retain data.

Best practices against trafficking in human beings via the Internet

In general, quite enough anti-trafficking in human beings practices have already been developed. Many handbooks are available on prevention, and on effective investigation and prosecution of trafficking in human beings.[112] All of them deal with good practice principles. Some of the

[112] Just some of the existing publications: International Centre for Migration Policy Development (ICMPD), (2004), *Regional Standard for Anti-trafficking training for judges and prosecutors in SEE*; can be downloaded at http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=249&cHash=445c9d8c56; International Centre for Migration Policy Development (ICMPD) (2003), *Development of an Anti-trafficking Training Module for Judges and Prosecutors*; can be downloaded at http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=187&cHash=1663ddae57; International Centre for Migration Policy Development (ICMPD) (2005), *Elaboration and Implementation of Anti-Trafficking Training Modules for Judges and Prosecutors in European Union Member States, Accession and Candidate Countries*; can be downloaded at http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=174&cHash=7813ce8d84; International Centre for Migration Policy Development (ICMPD) (2005), *Strengthening Law Enforcement Capacities for Fighting Human Trafficking in South-Eastern Europe – Joint ICMPD/UNDP Romania Follow-up on Regional Training*; can be downloaded at: http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=184&cHash=b3157d6dac; International Centre for Migration Policy Development (ICMPD), (2005), *Awareness Training on Trafficking in Human Beings for Police, Border Guards and Customs Officials in European Union Member States, Accession and Candidate Countries – Development of a European Curriculum*; can be downloaded at http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=181&cHash=3c47116e25; International Centre for Migration Policy Development (ICMPD), (2005), *Combating the Forced Labour Outcomes of Human Trafficking*; can be downloaded at http://www.icmpd.org/758.html?&tx_icmpd_pi2[document]=175&cHash=ada7314bbb; ICRC (2004), *Inter-agency Guiding Principles on Unaccompanied and Separated Children*; can be downloaded at http://www.unicef.org/protection/files/english_guiding_principles.pdf; International Labour Organisation (ILO) (2005), *A Global Alliance against Forced Labour, Report of the Director-General, Geneva: ILO*; can be downloaded at http://www.ilo.org/dyn/declaris/DECLARATIONWEB.DOWNLOAD_BLOB?Var_DocumentID=5059; International Labour Organisation (ILO), *Trafficking for Forced Labour; How to Monitor the Recruitment of Migrant Workers, Training Manual*, 2006.; International Labour Organisation (ILO), *Guide to Private Employment Agencies, Regulation. Monitoring and Enforcement*, 2007.

above-mentioned technical measures taken by governmental organisations and NGOs at national or international/regional level could also be regarded and adopted as good practices against trafficking in human beings committed via the Internet. In this connection, we would remind readers of the hotlines for information and online reporting of crimes set up in the United Kingdom by the "Internet Watch Foundation" for sexual-content sites, and by "Safe Modelling" for scam modelling agencies. Systems akin to the comprehensive Web sites operated by NGOs like On the Road and Gruppo Abele in Italy; or systems that promote international co-operation, such as the Headway online transnational database, which targets various forms of trafficking, can be useful in the fight against victim recruitment via the Internet.

Systems already established to combat child pornography, such as the filtering systems adopted by Action Innocence – Monaco, the CETS (Child exploitation tracking system), or the Virtual Global Taskforce (VGT), might also be adapted to cover recruitment and exploitation via the Internet. VGT is an international partnership of law enforcement agencies, which was set up to fight online child abuse. A body similar to the Taskforce, which comprises the Australian High Tech Crime Centre, the United Kingdom's Child Exploitation and Online Protection Centre (CEOP), the Royal Canadian Mounted Police, the United States immigration and customs enforcement authorities, the Italian and French law enforcement authorities, Europol and Interpol, might be useful in identifying recruitment Web sites worldwide, and then leaving the relevant law-enforcement agencies to act.

We also hope strongly that implementation of GRETA (the monitoring structure provided for in the Council of Europe Convention) will play a major role in prevention and in putting pressure on governments.

Other practices that have proved useful in fighting trafficking in human beings via the Internet include:

ILO's principal approach to preventing abusive forms of recruitment

In the wake of the Global Report on Forced Labour (2005), a business alliance against trafficking and forced labour has been formed. This involves employers in a strategy against human trafficking and forced labour, and tackles the problem on the demand side.

ILO has developed training tools on recruitment and trafficking for various target groups:

- The *Training manual: How to monitor the recruitment of migrant workers* (2006), which focuses on recruitment of migrants into highly exploitative working situations, which may amount to forced labour. It provides information on abusive recruitment practices and trafficking, and on socio-economic factors which encourage trafficking. The main emphasis, however, is on policy measures, skills and techniques to eliminate these practices.

- The *Guide to Private Employment Agencies Regulation, Monitoring and Enforcement* (2007), which gives national legislators guidance on drafting laws in line with ILO Conventions. It includes examples of national legislation, and collates specific provisions from developed and developing countries. It helps national legislators and the social partners to identify any gaps in their legislation, and find appropriate solutions.

The ILO is currently developing *Training modules for labour inspection* on the various aspects of forced labour:

- Identifying illicit recruitment practices;
- Identifying victims of trafficking for forced labour and protecting their rights;
- Collecting evidence against traffickers and investigating them;
- Co-operating with criminal law enforcement agencies.

International Organisation for Migration

The IOM's Counter-Trafficking Division has an operational tool, the Counter-Trafficking Module (CTM) database, which is uses to support management of the victims of trafficking in human beings whom it assists directly.[113]

The CTM is used to manage return and reintegration of victims of trafficking in human beings. Its database makes it possible to reconstruct the trafficking process for each victim, and centrally monitors direct IOM assistance, movement and reintegration, with a view to improving services, on the basis of further research, advocacy, information and evaluation. The CTM has many different functions: it stores information collected from assisted victims, thus providing a better picture of their background, experience of trafficking and assistance needs. It is also a tool for effective co-ordination between IOM missions, allowing them to follow individual cases, track activities, and also monitor and evaluate programme effectiveness. It serves as a knowledge-bank, containing statistics and detailed reports which can be used in research, programme development and policy-making on counter-trafficking. The database stores information from two questionnaires completed for victims referred to IOM: the Screening Interview, which assesses their eligibility for assistance under one of IOM's CT projects, and the Assistance Interview, which provides fuller information on the trafficking process.

[113] IOM Counter-Trafficking Module Database, 2007.

International Centre for Missing and Exploited Children

In an effort to support the international community's increased efforts to tackle the growing problem of child safety on Internet, the International Centre for Missing and Exploited Children,[114] Interpol[115] and Microsoft[116] have set up an international training programme for law-enforcement personnel worldwide, who investigate computer-facilitated crimes against children. The Centre runs eight to ten intensive training programmes per year[117] around the globe. The Conference on Computer-Facilitated Crimes Against Children brings together law-enforcement operatives from all parts of the world for four days of extensive training on investigating online child predators, collecting evidence and forensic data on computer, and seeking private sector support in investigating child exploitation. Microsoft's involvement in the conference is one of many initiatives the company is taking to help ensure safety on the Internet. It provides financial support for various conferences on this question.[118]

[114] `http://www.icmec.org/`.

[115] `http://www.interpol.int/`.

[116] `http://www.microsoft.com/`.

[117] The first training session involved representatives of 33 countries and took place in Lyons, France, in December 2003.

[118] In 2004 Microsoft financed an INHOPE conference in Berlin on "The Internet in 2004: Safe or Just Safer?" INHOPE is the co-ordinating body for the Association of Internet Hotline Providers in Europe and is funded under the European Union Safer Internet programme. It works closely with the International Centre in exchanging reports and facilitating international dialogue.

Recommendations on legal and technical measures to fight trafficking in human beings via the Internet effectively

To fight trafficking based on computer or other communication systems, it is imperative that the member states ratify both the Council of Europe instruments: the Cybercrime Convention and the Convention on Action against Trafficking in Human beings. There is no need for a new instrument specifically devoted to trafficking in human beings via the Internet, since these are already effective tools for counter-action.

What is needed is close co-operation and co-ordination – and also harmonised arrangements for effective prosecution of transnational traffickers.

As noted in the 2003 report, effective law enforcement requires "sufficient resources to finance law enforcement units trained and dedicated to fight cybercrimes".[119]

The specific measures taken should reflect the potential victim's profile and the form of trafficking involved. Different measure are needed to prevent child pornography (e.g. software to ensure safe chatrooms), sexual exploitation of adults, and exploitation of labour. One problem is that filters for adult sex sites will not work in countries where prostitution is legal.

In such cases, awareness campaigns are needed to alert potential clients; starting at local level, they are also needed for people in danger

[119] 2003 report, p. 75.

of being lured into sexual or labour exploitation by fraudulent job advertisements.

Awareness campaigns should be mounted in European Union regions where unemployment is relatively high. The public should also be warned against agencies which demand fees for providing work. As long as wages and employment opportunities remain unequal within the European Union, there will be people who seek to exploit, and people who are vulnerable to exploitation. In the long term, the only way to deal with this effectively is to level out living standards.

The development of methods and tools to provide information and assistance for (potential) victims of trafficking in human beings via the Internet by NGOs and other agencies active in the anti-trafficking field must be supported.

To gauge the Internet's effectiveness for recruitment of victims of trafficking in human beings, we need surveys of Internet infrastructure, and of the use made of the Internet in finding employment or partners, in the potential victims' countries of origin.

Once we know the sites, gateways and other Internet services through which people are recruited, we can monitor them. This will allow us to assess and address risks connected with the use of sites which have certain features. An early warning system could be set up, and warnings flashed to users who hit certain links or type in certain words or phrases, following the marketing techniques employed by various businesses (spam-like messages).

Further research is also needed on other unexplored areas of Internet-based trafficking, e.g. illegal adoptions or trafficking of pregnant women (even though, in these cases, the Internet is likelier to be used to attract clients, or facilitate transactions with them.[120]

Prospects for co-operation with computer experts, and businesses which operate Internet gateways and search engines, should be explored. There are already examples of codes of conduct, which have been introduced online to tackle the problem of child pornography. The use of advertising filters might be another option.

Resources and appropriate equipment are needed to be able to act and keep pace with the skills and technical equipment of abusers.

[120] Illegal adoption is not covered, as such, by the definition of trafficking in human beings given in the Convention on Action against Trafficking in Human Beings (CETS No. 197). Nevertheless, "where an illegal adoption amounts to a practice similar to slavery as defined in Article 1 (d) of the Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices similar to Slavery, it will also fall within the Convention's scope". See para. 94 of the Explanatory Report on the Convention.

In Recommendation 1663 (2004) on domestic slavery: servitude, au pairs and mail-order brides, the Council of Europe's Parliamentary Assembly recommended that agencies active in this field be regulated and monitored by appropriate authorities via an accreditation system, which would commit them to respecting certain minimum standards, e.g. charging reasonable fees, ensuring that persons responsible for Internet agency sites are clearly identifiable and that site users are required to identify themselves, following up marriages, and providing an emergency contact number. When couples are considering marriage, agencies should also be required to carry out background checks on prospective bridegrooms, to ensure that they do not have criminal records (e.g. for domestic violence or procurement).

It is therefore important that law-enforcement agencies should monitor use of these marriage bureaux and modelling agencies, and set up databases of suspect agencies, for use by visa-issuing authorities in source countries. Those involved in running marriage bureaux and modelling agencies should also be checked for any links with trafficking for purposes of sexual exploitation. According to Europol, there seem to be close links between people who operate online marriage bureaux and people who make money from pornographic and exploitative PPV Web sites (if indeed they are not the same).

There should also be systematic monitoring of sites that offer sexual services, whether or not prostitution is legal in the country concerned.

It is important to remember that we must not confuse prostitution with sexual exploitation, which is a form of trafficking in human beings, although we should be aware of their possible connections.

To help prevent labour exploitation, government job sites, and sites operated by ministries of employment and embassies, should provide information on rights and obligations, as well as risks and how to avoid them. More coherent and comprehensive systems are needed to disseminate primary preventive information in areas where risks have been clearly identified.

We should increase the capacity of workers' organisations to identify recruitment malpractices, co-operate with labour inspectorates, and monitor the recruitment sector, with a view to eliminating illegal and exploitative practices; co-operation between labour inspectorates and criminal law enforcement agencies should also be intensified.

A broad policy framework is needed to help private employment agencies to develop and enforce self-regulation and good business standards. National laws and regulations should tackle shortcomings and gaps in the current role of private employment agencies on the national labour market, taking due account of their main activities and services. Legislators should have information on the (estimated) number of recruitment agencies, their type, the services they offer, and the economic sectors in which they predominate. Reports of malpractice and abuse by agencies should be analysed. Representatives of employers and trade unions should be actively involved in drawing up regulations for private employment agencies. Labour ministries and inspectorates have a key role to play in ensuring compliance with the rules on employment of persons locally or overseas.

A self-regulation system should be introduced. Self-regulation is based on three key elements: first, involvement of all the interested parties (government, industry, service and access providers, user associations) in producing codes of conduct; secondly, implementation of these codes by the industry concerned; thirdly, evaluation of the measures taken. Experience has shown that law-abiding private employment agencies have an interest in self-regulation based on codes of conduct, rating systems, etc., if it helps to reduce unfair competition, and if they can expect favourable government treatment in return for applying it. Other regulatory and promotional measures to ensure compliance with basic standards by private recruitment agencies include registration, licensing, professional certification, rating and partnerships between public employment services and private employment agencies.

Self-regulation can be backed by clear legal regulation – this is what the term "co-regulation" means. A co-regulatory system is one in which the public authorities accept that protection of societal values can be left to self-regulatory schemes and codes of conduct, but reserve the right to intervene, if self-regulation fails to work.[121] The European Union Commission is up-dating the 1998 Recommendation on protection of minors in the online environment – the new text is now close to adoption by the European Parliament and Council. It builds on the original Recommendation, which remains valid, with adjustments to meet the challenges presented by new technologies. The topics covered include media literacy and media education programmes, and co-operation and pooling of know-how and good practices by regulatory and self-regulatory bodies responsible for rating or classifying audiovisual content. The ICRA system may very well become an accepted co-regulatory system of this

[121] Communication by Viviane Reding, Member of the European Commission responsible for Information Society and Media, "Freedom of the media, effective co-regulation and media literacy: cornerstones for an efficient protection of minors in the European Union", ICRA Round Table, "Mission Impossible" Brussels, 14 June 2006, at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/06/374&format=HTML&aged=0&language=EN&guiLanguage=en.

kind. As long ago as November 2004, the German Commission for the Protection of Minors decided to test the "ICRA Deutschland" system for an 18-month period.

In case the regulatory system does not work, states should also consider severe penalties for users. For instance, the landowners who illegally hired exploited Polish workers in Italy (operation Terra Promessa) were merely fined, although they had also committed a trafficking offence by exploiting their labour directly.

For the purpose of prosecuting offenders, we should use: local, regional and national co-ordination and information-sharing mechanisms; national liaison officers posted overseas or links with liaison officer networks; Europol and its Liaison Bureaux; Interpol's National Contact Bureaux; Eurojust; the Schengen Information System; and direct bi-lateral contacts. Channels that already exist for other purposes should be activated and adapted. To ensure that investigators use them effectively, these must be well-publicised and easily accessed.

We should also consider adding use of the Internet and other new technologies to commit trafficking in human beings to the list of aggravating circumstances which determine the penalty for the offence, since traffickers who employ these means address an indefinite number of people, and so can do incalculable harm. In French cybercrime law[122], the use of electronic means (i.e. the Internet) to commit a crime involving sexual exploitation (including trafficking in human beings) is an aggravating circumstance and makes the penalty more severe.

Concerning recruitment, states should consider revising their laws on trafficking in human beings to make enticement through promises (actually the case on the Internet) enough in itself to constitute the offence, without its being necessary for the victim to have been actually "recruited, transported, transferred, harboured or received".

GRETA should play an active role in monitoring implementation of the Council of Europe Convention on Action against Trafficking in Human Beings, and put pressure on states to take appropriate action against all forms of trafficking, regardless of the means they employ.

Finally, since 55% of sexual content sites appear to be hosted in the United States, the measures taken should first target this market, to which no binding international instrument applies. As some experts have said, simply "wringing one's hands" is not enough...

[122] See 2003 report, p. 74.

General conclusion

“Men think that by ill-treating others they make their own superiority the greater” – Aristotle*

* This is Aristotle’s explanation of *hubris* in his *Rhetoric,* 1378b.

The Internet is still very largely *terra incognita*, and that leaves plenty of scope for criminal activity.

There is an intrinsic link between the Internet and the provision of sexual services, and it is essential to make monitoring of the Internet an integral part of any action taken against trafficking in human beings. As the cases examined here and many others show, traffickers no longer need to install their victims in old-style "red light areas" or put them on the streets, when covert arrangements can be made anonymously online, allowing clients to go to nondescript addresses in towns not previously associated with the sex trade. In such settings, victims are less likely to attract police attention, and can be strictly controlled at all times. This clearly has implications for law enforcement, which is no longer just a matter of trawling the well-known areas, arresting traffickers and rescuing victims – unfortunately, things are now a great deal more complicated. Traffickers have a commodity whose full value can be realised only by making victims available to clients, to whom their services are advertised on the Internet.

The problem with sexual exploitation of adults is that it is less obvious than child pornography and child prostitution. Both these crimes against children are obviously banned throughout the world and, because their character is clear, technical measures against them can be more easily devised and implemented – even if new technological developments are daily creating fresh challenges. However, with sexual exploitation of adults – unless someone chances on a really obvious site, e.g. one that sells women as slaves online – there is never enough certainty as to where exploitation, and thus victimisation, of an adult person starts (unless the case is being investigated, and that person is identified as a victim). At least, we should all be clear on one thing: the fact of prostitution's being legal in a given country does not dispense the authorities from investigating to establish whether the people concerned have been exploited.

At the same time, sexual exploitation is not the only kind practised via the Internet. Increasingly, victims of labour exploitation are being lured by fraudulent job offers online or by spam mail. People looking for employment, friends, husbands, etc., can all be deceived in this way.

Certainly, the Internet is not evenly used in all the member states. We must not forget that equipment availability and infrastructure differ between states, chiefly for economic reasons. However, we should not underestimate the speed at which Internet use is increasing. Unless suitable action is taken, this may lead on to an increase in victim recruitment. Technology moves fast, and criminals are always the first to exploit new developments.

Since the 2003 report, all the member states have introduced legislation against trafficking in human beings, and at least half of them – mainly European Union members – have also introduced specific provisions on use of the new information technologies, and are taking steps to enforce them, even if progress is still needed on provider liability and data retention. On the positive side, rapid progress has been made on legal measures, law enforcement, and technical counter-measures. On the negative side, we should not underestimate the speed with which criminals seize on new technologies, or forget that they will always be a step ahead. Crime can never be eradicated. Anyone who believes that it can is living in a fool's paradise. Our aim should be to narrow the gap between crime and response, so that we can limit the former's effects.

If crime is increasingly organised today, then we need to be organised too. We need to create a network which is strong, well-trained and dedicated to fighting trafficking in human beings.

Effective prosecution in this area depends, not just on strict, detailed and harmonised international law, but also on a rapid, co-ordinated response by law enforcement agencies. Success depends on know-how – and on the investigating authorities' reacting fast. It takes only a minute to erase all the incriminating evidence from an Internet or computer system.

There are regular reports of action taken against traffickers by police throughout Europe, and the sentences given are now quite severe. Many measures have also been taken at international and regional level. In the case of labour exploitation, however, the response is not generally so effective. Since most convictions result from the detection of offences related to trafficking, such as violence or money laundering, the more cunning traffickers may well get away – which scarcely serves as a deterrent.[1]

I do not believe that we need specific laws connecting trafficking in human beings with the Internet or other means employed – whether based on the new technologies or not – since the Council of Europe's Conventions on Action against Trafficking in Human Beings and on Cybercrime already cover this issue comprehensively.

I do believe, however, that the use of the Internet for trafficking should constitute an aggravating circumstance, since it can affect an indefinite number of people, and do this at international level.

A great deal needs to be done before we can claim that we are ready to fight computer-related crime effectively. Countries lack the political will to ratify and implement conventions. But even if they had, they might still lack the technical means to tackle this kind of crime, i.e. the funds to keep pace with the march of technology.

In a consumer world, whose main value is money and whatever it can buy, and where liberty is given a negative twist, and taken to mean liberty to satisfy one's every instinct, we cannot fight the whole sex market without changing the values of Western societies. When we have done that, we may begin to understand why the Spartans thought money the root of evil, and tried so hard to do without it. We must continue to fight exploitation of every kind, and by every means. In no circumstances must exploitation, however practised, be tolerated, because it is an act of *"hubris"*[2] against humanity.

[1] According to Nick Garlick, Europol, "It is the murky area of subcontracting, and in particular gangmaster activity in the food and agricultural sectors, that continues to be the most vulnerable to criminal activity. Often major companies will hide behind their use of subcontractors to avoid taking responsibility towards their employees. A recommendation from me would be that legislation should be introduced that addresses this and can find the companies 'upstream' liable for the maltreatment of workers in the supply chain". Presentation at the Council of Europe seminar on the misuse of the Internet for the recruitment of victims of trafficking, Strasbourg, 7-8 June 2007.

[2] In classical Athens, *hubris* (ὕβρις) was a crime. Hubris against the Gods is often a character flaw in the heroes of Greek tragedy, and the cause of the "nemesis", or destruction, which overtakes them. For the most part, hubris refers to offences committed by mortals against other mortals; things done to shame the victim, and so make the doer seem superior. Violations of the law against hubris ranged from what might today be termed assault and battery, through sexual assault, to the theft of public or sacred property. Cairns, Douglas L., "Hybris, Dishonour, and Thinking Big", Journal of Hellenic Studies 116 (1996), 1-32.

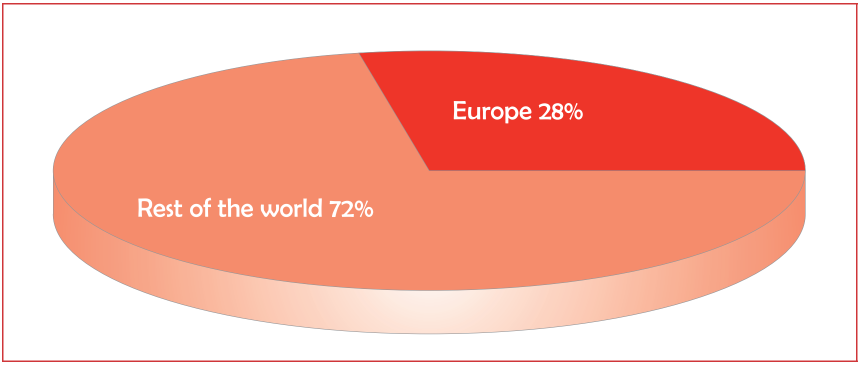
Appendix 1: Internet statistics

Internet user statistics and population for 52 European countries and regions

Internet usage in Europe and the world[1]

	Europe	Rest of world	Total world
Population (2007 est.)	809 624 686	5 765 041 731	6 574 666 417
% pop. of world	12.3%	87.7%	100%
Internet users, latest data	321 853 477	832 505 301	1 154 358 778
Penetration (% population)	39.8%	14.4%	17.6%
% usage of world	27.9%	72.1%	100%
Use growth 2000-07	206.2%	225.3%	219.8%

Europe Internet users[2]



[1] Source: http://www.internetworldstats.com/stats4.htm. (1) European Internet Statistics were updated for June 30, 2007. (2) Population is based on data from world-gazetteer.com. (3) The usage numbers come from various qualified sources, mainly from data published by Nielsen/ /NetRatings, ITU, and other trustworthy sources. (4) Data may be cited, giving due credit and establishing an active link back to Internet World Stats. Copyright © 2007, Miniwatts Marketing Group. All rights reserved worldwide.

[2] Copyright © 2007, internetworldstats.com.

Internet usage in Europe by country[3]

	Population (2007 est.)	Internet users, latest data	% population (penetration)	% users Europe	Usage growth 2000-07
Albania	3 087 159	188 000	6.1%	0.1%	7 420.0%
Andorra	69 524	21 900	31.5%	0.0%	338.0%
Austria	8 213 947	4 650 000	56.6%	1.5%	121.4%
Belarus	9 678 864	3 394 400	35.1%	1.1%	1 785.8%
Belgium	10 516 112	5 100 000	48.5%	1.6%	155.0%
Bosnia-Herzegovina	4 672 165	806 400	17.3%	0.3%	11 420.0%
Bulgaria	7 673 215	2 200 000	28.7%	0.7%	411.6%
Croatia	4 468 760	1 472 400	32.9%	0.5%	636.2%
Cyprus	971 391	326 000	33.6%	0.1%	171.7%
Czech Republic	10 209 643	5 100 000	50.0%	1.6%	410.0%
Denmark	5 438 698	3 762 500	69.2%	1.2%	92.9%
Estonia	1 332 987	690 000	51.8%	0.2%	88.2%
Faeroe Islands	49 760	33 000	66.3%	0.0%	1 000.0%
Finland	5 275 491	3 286 000	62.3%	1.0%	70.5%
France	61 350 009	32 925 953	53.7%	10.2%	287.4%
Germany	82 509 367	50 426 117	61.1%	15.7%	110.1%
Gibraltar	26 268	6 200	23.6%	0.0%	287.5%
Greece	11 338 624	3 800 000	33.5%	1.2%	280.0%
Guernsey & Alderney	63 908	36 000	56.3%	0.0%	80.0%
Hungary	10 037 768	3 050 000	30.4%	0.9%	326.6%
Iceland	299 076	258 000	86.3%	0.1%	53.6%
Ireland	4 104 354	2 060 000	50.2%	0.6%	162.8%
Italy	59 546 696	31 481 928	52.9%	9.8%	138.5%
Jersey	89 485	27 000	30.2%	0.0%	237.5%
Latvia	2 279 366	1 030 000	45.2%	0.3%	586.7%
Liechtenstein	35 622	22 000	61.8%	0.0%	144.4%

	Population (2007 est.)	Internet users, latest data	% population (penetration)	% users Europe	Usage growth 2000-07
Lithuania	3 403 871	1 221 700	35.9%	0.4%	443.0%
Luxembourg	463 273	315 000	68.0%	0.1%	215.0%
Malta	386 007	127 200	33.0%	0.0%	218.0%
Man, Isle of	75 530	—	—	—	0.0%
Moldova	3 727 246	550 000	14.8%	0.2%	2 100.0%
Monaco	33 443	18 000	53.8%	0.0%	157.1%
Montenegro	665 734	117 000	17.6%	0.0%	n/a
Netherlands	16 447 682	12 060 000	73.3%	3.7%	209.2%
Norway	4 657 321	3 140 000	67.4%	1.0%	42.7%
Poland	38 109 499	11 400 000	29.9%	3.5%	307.1%
Portugal	10 539 564	7 782 760	73.8%	2.4%	211.3%
Romania	21 154 226	4 940 000	23.4%	1.5%	517.5%
Russia	143 406 042	28 000 000	19.5%	8.7%	803.2%
San Marino	31 500	14 300	45.4%	0.0%	472.0%
Serbia	10 087 181	1 400 000	13.9%	0.4%	250.0%
Slovakia	5 379 455	2 500 000	46.5%	0.8%	284.6%
Slovenia	1 962 856	1 090 000	55.5%	0.3%	263.3%
Spain	45 003 663	19 765 033	43.9%	6.1%	266.8%
Svalbard & Jan Mayen	2 274	—	—	—	0.0%
Sweden	9 107 795	6 890 000	75.6%	2.1%	70.2%
Switzerland	7 523 024	5 097 822	67.8%	1.6%	138.9%
"The Former Yugoslav Republic of Macedonia"	2 056 894	392 671	19.1%	0.1%	1 208.9%
Turkey	75 863 600	16 000 000	21.1%	5.1%	700.0%
Ukraine	45 833 977	5 278 100	11.5%	1.6%	2 539.1%

[3] Source: http://www.internetworldstats.com/stats4.htm. (1) The European Internet Stats were updated for June 30, 2007. (2) The population numbers are based on data contained in world-gazetteer.com. (3) The usage numbers come from various sources, mainly from statistics published by Nielsen//NetRatings, ITU, C-I-A, and local NICs. (4) Data may be cited, giving due credit and establishing an active link back to InternetWorld Stats. © Copyright 2007, Miniwatts Marketing Group. All rights reserved worldwide.

	Population (2007 est.)	Internet users, latest data	% population (penetration)	% users Europe	Usage growth 2000-07
United Kingdom	60 363 602	37 600 000	62.3%	11.7%	144.2%
Vatican City State	767	93	12.1%	0.0%	0.0%
TOTAL Europe	809 624 686	321 853 477	39.8%	100.0%	206.2%

Sources of spam: worst twelve countries[4]

Position	Country	Percentage
1	**United States**	21.6%
2	**China (incl. Hong Kong)**	13.4%
3	**France**	6.3%
3	**South Korea**	6.3%
5	**Spain**	5.8%
6	**Poland**	4.8%
7	**Brazil**	4.7%
8	**Italy**	4.3%
9	**Germany**	3.0%
10	**Taiwan**	2.0%
11	**Israel**	1.8%
12	**Japan**	1.7%
Others		24.3%

[4] European Commission's Communication on spam published at: http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/communic_reports/index_en.htm. The latest Sophos figures (from 6 November 2006) show where action is most needed: http://www.sophos.com/pressoffice/news/articles/2006/11/dirtydozq306.html.

Appendix 2: Bibliography

A full bibliography of sources and references used for this study can be found on the Council of Europe's anti-trafficking Web site: http://www.coe.int/trafficking/.

Trafficking in human beings: Internet recruitment

The rapid development in the use of information technologies, in particular the Internet, has given a new dimension to trafficking in human beings. The Internet is a fast, convenient and inexpensive way of connecting people between cities and across borders, but it also possesses the potential to be misused by criminals. Traffickers now have, literally at their fingertips, an effective, unrestricted and often anonymous means for recruiting their victims. Online employment agencies, in particular model or artist agencies and marriage bureaux, can all be ploys to lure potential victims. Internet chat websites are often used to befriend potential victims. The risks for young people to fall into the traffickers' net have substantially increased.

This study presents the current methods used by traffickers to recruit their victims via the Internet, and identifies legal, administrative and technical means used to combat this misuse.

Gender Equality and Anti-Trafficking Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

http://www.coe.int/trafficking/