UN.GIFT
United Nations Global Initiative to Fight Human Trafficking

UN.GIFT B.P.:017

The Vienna Forum to fight Human Trafficking
13-15 February 2008, Austria Center Vienna
Background Paper

017 Workshop: Technology and Human Trafficking

This Background Paper has been reproduced without formal editing.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Its content does not necessarily reflect the policies or views of UNODC and of the donors.

THE VIENNA FORUM TO FIGHT HUMAN TRAFFICKING
13-15 February 2008

Vienna, Austria

BACKGROUND PAPER

WORKSHOP 017
TECHNOLOGY AND HUMAN TRAFFICKING

As globalization accelerates, the range of information and communication technology expands, becoming more accessible to more people, ultimately impacting the way that humans interact. The same is as true for human trafficking as it is for legal business enterprises; technology offers traffickers more creative and complex ways to commit their crimes while at the same time, presenting the global anti-trafficking community with more opportunities to respond to it.

TECHNOLOGY: PART OF THE PROBLEM

Using technology for communications and transactions among traffickers

"Traffickers in [some] countries are no longer uneducated, "paan-chewing" men, but carry cell phones, video cameras, and speak cultured English instead, allowing them to exploit women and children more efficiently and effectively than ever before".[1]

Traffickers are as diverse as the countries in which they operate. Some are poorly educated individuals who have few skills but those they learn in crime, while others are respected members of the community as well as clandestine members of well-resourced, highly sophisticated crime syndicates who can afford to remain on the crest of technological advances. Regardless of which end of the 'sophistication' spectrum traffickers are operating and regardless of where in the world they are committing their crimes, all of them are benefiting in their criminal activities through advances in technology which make it faster, easier cheaper (and ultimately more profitable) to conduct transactions.[2]

The increase in the use of technology for exploitative purposes (from sexual or pornographic, to trafficking in persons or a combination of offences) has been attributed to:

- More generalised access to internet
- Increased number of internet users each year
- Increased affordability of technology and services
- Anonymity of users
- Speed – it is fast (leaving only digital traces)
- Criminals can work from home (although the crime itself can affect victims and have consequences in several countries)
- Difficulty to trace (criminals can operate in many countries)
- The high profitability of the sale of pornography relative to the investment required

[1] Skinner, Robyn., and Maher, Catherine. "Child Trafficking and Organized Crime: Where have all the Young Girls Gone?" Youth Advocacy International (YAPI) Resource Paper, www.yapi.org., p.2.

[2] Skinner, Robyn., and Maher, Catherine. "Child Trafficking and Organized Crime: Where have all the Young Girls Gone?" Youth Advocacy International (YAPI) Resource Paper, www.yapi.org., p.4.

- Lack of appropriate legislation or State policy to respond to the phenomenon.[3]

Region	Population (2007)	% of world population	Internet usage	% population (penetration)	Usage growth (2000-2007)
Africa	941,249,130	14.2%	44,234,240	4.7%	879.8%
Asia	3,733,783,474	56.5%	461,703,143	12.4%	303.9%
Europe	801,821,187	12.1%	343,787,434	42.9%	227.1%
Middle East	192,755,045	2.7%	33,510,500	17.4%	920.2%
North America	334,659,631	5.1%	237,168,545	70.9%	119.4%
Latin America / Caribbean	569,133,474	8.6%	122,384,914	21.5%	577.3%
Oceania / Australia	33,568,225	0.5%	19,243,921	57.3%	152.6%
World TOTAL	6,606,970,166	100%	1,262,032,697	19.1%	249.6%

Source: Internet World Stats, Usage and Population Statistics, November 30, 2007 www.internetworldstats.com/stats.htm

The two main areas where organised crime groups can advance and facilitate their criminal activities in the area of trafficking in persons are:

- Communication, and
- Financial Transactions

Communication

The use of new information technologies for communication purposes among traffickers is not extensively documented. However, it is known that criminal generally use new technologies to avoid police interception of their communications. Trafficking in persons requires extensive coordination throughout the process of planning, recruiting victims, transporting them, meeting and transferring people at various times and locations; it is therefore likely that criminals are using new technologies or old technologies in more complex ways to facilitate their communications and avoid detection. [4] It is not known whether the use of new technologies has increased trafficking in persons, but it is believed that increased use of technologies have made trafficking activities easier to perform. [5]

The use of new technology and increased use of old technology is particularly prevalent at the exploitation stage of trafficking. People seeking to buy women and children for purposes of sexual exploitation are now able 'shop' online with an ease

[3] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.14.

[4] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.22.

[5] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.22.

that was impossible before the internet.[6] There have also been incidents of the internet being used to advertise the sale of human organs.

Types of Communication Technology

There are various forms of technology which offer organized traffickers arenas in which to convene transmit communications and illegal material to each other. Some of them include;

- Newsgroups: sites for exchange of information.
- Web message and bulletin boards: exchange of information; similar to newsgroups but can be private and password protected.
- Websites and search engines
- Chat rooms: real time communication; no messages are archived or stored, and no log files are maintained.
- File Transfer Protocol (FTP): effective file exchange on the internet, allows users direct access to another's computer hard drive to upload and download files.
- Peer to Peer networks and file swapping programs: used to share illegal material by finding and downloading files on online networks without leaving traceable transmissions.
- Encryption: can be used to disguise the content of files.[7]
- Mobile internet systems.

An enormous advantage criminals are offered by information communication technology is the ease of anonymity and disguise. Criminals are able to send their communications through a series of carriers, each using different communications technologies. In effect, such technologies have enabled criminals to more easily distance themselves from the crimes they commit, and provide a degree of anonymity and/or disguise which allows them to commit their crimes with reduced risk.[8]

Telephone calls may be disguised through the simple use of local or long distance telephone companies and internet services providers and extend to include wireless or satellite networks; cellular and satellite phones and their users can be located far from their home base. Telecommunications companies often offer free or cheap incentives to sign up to their services; criminals often take advantage of such offers and dispose of their phone after a short period of use or after a particular act as been committed.. Mobile phones can be programmed to transmit false identification and traffickers can sign up for mobile phone services. Pre-paid phone cards can also be used easily and anonymously, for both mobile phones and also landline telephone

[6] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.27.

[7] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.18-19.

[8] 'Trafficking in Human Beings: Internet Recruitment' Council of Europe, 2007, pp.25-26.

systems.[9] Another layer of disguise is offered by the use of stolen phone cards which can be replaced on a regular basis or phones which are fraudulently recharged.

Electronic communications can be similarly anonymous. Emails for instance can be routed through different countries and different time zones, hampering attempts to identify sources and recipients of communications. Messages can be simply sent through 're-mailers' who remove identifying information and replace it with false information before sending it one; this system is known to take advantage of chinks in the global law enforcement cooperative community, with re-mailers sending communications through at least one country known for its lack of cooperation with the global community and law enforcement. New technologies such as Web TV allow traffickers to communicate without accidentally leaving illegal materials on a file cache to be discovered be law enforcement. [10]

Financial Transactions

With accelerating globalization, criminals are able to take advantage of the ease of capital movement, increasing mobility of people and commodities, diversity of legal provisions in various jurisdictions, and advances in technology to transfer assets quickly from place to place in such a way that they ultimately appear as legitimate assets. These assets are then available to serious offenders and criminal organizations anywhere in the world to finance further criminal operations.[11]

The spread of e-business is to the enormous benefit of organized crime groups; it offers the possibility of having 'virtual identities' on the internet, facilitates and disguises financial activities and allows the exchange of money and services with a high level of anonymity. Money can be moved very rapidly around the world in a very short time via the internet, and it is increasingly difficult for law enforcers to monitor this movement. Some internet payment options allow the payer a similar anonymity as they are afforded with cash, but with the ability to conduct global transfers and payments. [12]

Electronic forms of business, society and banking are being exploited by organised criminal groups which take advantage of new criminal opportunities afforded in the criminal arena and attack systems or exploit the weaknesses in security systems. The

[9] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.20-21.

[10] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.20-21.

[11] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.39

[12] "EU Organised Crime Threat Assessment 2007" (Europol, June 2007), p.19.

ability of service providers to increase the security of their online services is restricted by market forcers; where security is often sacrificed to user-friendliness.[13]

Counterfeit documentation

Counterfeit documentation has become easier than it was. Significant advances in computer and printer technology has increased the ability of organized crime groups to produce counterfeit documents of various types.

New Technologies

Not only are 'old' technologies being used in more effective and more creative ways by traffickers, but also, the development of new technologies is facilitating transnational crime with more crimes committed across borders through the use of the Internet. The abuse of online technology has created new forms of crime, such as 'spoofing', 'phishing', 'hacking', 'page-jacking', 'mouse-trapping' etc.[14]

USING TECHNOLOGY TO RECRUIT VICTIMS

The relationship between recruitment of victims and technology takes various forms. As the Council of Europe notes, these include:

1. Victims may fall prey to traffickers via websites and other internet services
2. 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.[15]

These methods will be explored below.

Recruitment via communication with potential victims

As more and more people access the internet on a more and more regular basis, the possibility of its use as a means of recruiting victims must be considered. This is particularly so in light of the fact that technological advances brings about the increased necessity of using computers and the internet in both education and work. This, coupled with the falling prices of telecommunications services and technology such as computers, means that it is realistic to assume that the number of internet users (including children and adolescents) will increase over coming years.

In 2006, the Serbian NGO 'Astra' conducted a study of secondary school students from six Serbian towns (Belgrade, Novi Pazar, Novi Sad, Vranje, U`ice and Šabac) to assess the likelihood of the Internet as a means of recruiting victims of trafficking. That report highlights the need to pay increased attention to risks posed to children and adolescents by the online community; the ASTRA SOS hotline receives dozens of calls expressing concerns about the security of meeting people who callers

[13] "EU Organised Crime Threat Assessment 2007" (Europol, June 2007), p.18.

[14] "EU Organised Crime Threat Assessment 2007" (Europol, June 2007), p.18.

[15] 'Traficking in Human Beings: Internet Recruitment', Council of Europe, 2007, p.33.

have made contact with via the Internet, who have ultimately invited them to undertake joint traveling, opportunities for further studies or work. [16]

This research showed that 38% of secondary school pupils used the Internet as a means of communication, and more than half of those reported using chat (instant messaging) over the Internet. Of the 460 respondents who reported to using chat to communicate with other people,

- 170 reported unpleasant experiences (including sexual harassment)
- 220 received offers (to meet in person, date, marry, travel, work, study, etc)
- 284 reported that their friends had received similar offers
- 174 reported that they met in person with someone they met online.[17]

Of all the girls who chat over the Internet, 57% had received offers at least once, compared with 38.6% of boys.[18]

Respondents who participated in this study were asked whether they thought that recruitment into human trafficking was possible through the internet.

- 12.6% of respondents thought that this would be impossible
- 87.4% of respondents believed that this would be possible; they felt that the Internet could be misused in this way through offers to meet in person, attractive job offers, false promises of a better life or other invitations as well as through online advertisements.[19]

Recruitment via Advertisements

There seems to be some evidence that traffickers use the Internet to recruit women into trafficking situations. Chat rooms and advertisements are the two principal methods used by traffickers to recruit such victims. The types of sites used by traffickers for the recruitment of victims can include:

- sites of marriage agencies (that could act as mail-order bride agencies or dating clubs)
- escorts' sites
- dating clubs
- various job offering sites including:
    - home assistance
    - waitressing / bartending
    - au pair / care
    - modeling
    - entertainment industry (dancers / hostesses)
    - construction / factories / agriculture

[16] "Human (Child) Trafficking: A Look through the Internet Window" Astra anti-trafficking Action, (Belgrade, Serbia, 2006), p.61.

[17] "Human (Child) Trafficking: A Look through the Internet Window" Astra anti-trafficking Action, (Belgrade, Serbia, 2006), p.50.

[18] "Human (Child) Trafficking: A Look through the Internet Window" Astra anti-trafficking Action, (Belgrade, Serbia, 2006), p.52.

[19] "Human (Child) Trafficking: A Look through the Internet Window" Astra anti-trafficking Action, (Belgrade, Serbia, 2006), p.53.

- educational courses
- matrimonial offers
- tourism
- work in the sex industry.[20]

A report by the Danish Police notes suspicious advertisements for nannies, waitresses and dancers on Web sites in Latvia and Lithuania. The traffickers used Internet sites to post job advertisements for jobs in Western Europe just as they do in magazines and newspapers. The magazine ads give mobile phone numbers for contacts, while the Internet sites give email addresses.[21] The danger posed by the internet has also been highlighted by the La Strada Foundation in Poland, which reported that 30% of its clients (trafficked women) were recruited through the Internet.[22]

The significance of these Internet advertisements in the recruitment of women was disputed. Some thought that so few girls and women have Internet access in Latvia and Lithuania, especially in the poor, rural areas from which many girls/women are recruited, that this could not be an effective recruitment tool. Others thought that almost all girls or women would have access to the Internet through schools and libraries, where they may go to search for work abroad. In Latvia, according to police sources, the women most vulnerable to recruitment were young women, aged 19 to 22, living in extreme poverty primarily in the southern and Russian part of Latvia where unemployment is high and the prospects for the future are poor. The destinations for the women from Latvia are primarily Germany and Scandinavia, but also include Great Britain, the Netherlands, Spain, Italy, Greece, Cyprus, Switzerland and Iceland. For the women from Lithuania, Poland is a transit country and Germany is considered to be the primary destination country, although many women are distributed to other European countries, especially Spain, the Netherlands, and Israel. Law enforcement sources believe there is a national network of recruiters in Lithuania with connections to international trafficking for the purpose of sexual exploitation networks.[23]

It should also be noted that the internet can be used to recruit victims into trafficking for purposes other than sexual exploitation. For instance, in 2006 the Polish and Italian police jointy dismantled a network of trafficking men for the purpose of forced labour; an employment agency website was identified as the primary means of recruitment.[24]

[20] 'Trafficking in human beings: Internet Recruitment' Council of Europe, 2007, pp.31-32.

[21] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.22.-23. The report can also be downloaded at www.coe.int/T/E/human_rights/Trafficking3_Documents/Reports/#p473_60876.

[22] Garnier, Joanna, at 'Misuse of the Internet for the recruitment of victims of trafficking in human beings' Strasbourg, 7 – 8 June 2007, Seminar Proceedings, p.36.

[23] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.22.-23.

[24] For more information on Operation 'Terra Promessa' visit www.policja.pl/portal/pol/90/2363/Polish_Police_and_Italian_Gendarmerie_Carabinieri_have_freed_119_Polish_citizens.html

Mail order brides (International Matchmaking Organizations)

'Marriage agencies' operating online can be a front for the recruitment and exploitation of victims of trafficking. It has been suggested that some sites may be mail-order bride sites which involve the sale of trafficked victims online by credit card, while marriage agency sites may be offering sexual services.[25]

The 'mail order bride' industry is almost completely unregulated. Businesses advertise for adults (and sometimes minors) for marriage and require the women and young girls they attract to disclose sometimes highly personal details, while failing to screen the mail clients or scrutinize their backgrounds at all. Women who participate in such programmes often make the erroneous assumption that governmental agencies in the countries of the men participating in the programme have the technological capacity to access information about the men and that men with criminal records would not be able to able to bring a spouse or fiancé into their country. The industry however, does not screen its male customers; no check for a criminal record is conducted, and there is no formal means of ascertaining whether male clients are already married. [26]

A United States Senate hearing heard that the 'mail order bride' industry (or international matchmaking organizations) have been linked to trafficking in persons. 'Mail order bride' agencies online can be fronts for trafficking organizations in which adults and girls are offered as 'brides' but sold privately into sexual exploitation, forced into marriage with men (some of whom will then prostitute them) or held in domestic slavery. [27] The senate report listed the following incidents[28]:

- An organized criminal gangs from Russia, the former Soviet Union and the Balkans were using the Internet to advertise women for sale to brothels in Western Europe and also to men as 'Internet Brides'[29]
- A study by the Global Survival Network (GSN) found that most mail-order bride agencies in Russia have expanded their activities to include trafficking for prostitution
- European embassies have reported that a number of international matchmaking agencies conceal organized prostitution rings victimizing newly arrived Filipina women
- Asian organized crime groups have used fiancée visa and marriage to bring women across the US border for purposes of sexual exploitation, often with the help of US nationals.[30]

[25] 'Trafficking in human beings: Internet Recruitment' Council of Europe, 2007, p.40.

[26] "Human Trafficking: Mail Order Bride Abuses" Hearing before the Committee on Foreign Relations United State Senate, Tuesday 13 July 2004, Testimony of Suzanne H. Jackson, Associate Professor of Clinical Law, George Washington Law School, p.2.

[27] "Human Trafficking: Mail Order Bride Abuses" Hearing before the Committee on Foreign Relations United State Senate, Tuesday 13 July 2004, Testimony of Suzanne H. Jackson, Associate Professor of Clinical Law, George Washington Law School, p.2.

[28] "Human Trafficking: Mail Order Bride Abuses" Hearing before the Committee on Foreign Relations United State Senate, Tuesday 13 July 2004, Testimony of Suzanne H. Jackson, Associate Professor of Clinical Law, George Washington Law School, p.2.

[29] Miller, *Sex Gangs Sell Prostitutes over the Internet*, The Guardian (U.K.), July 16, 2000, p.13

[30] Amy O'Neill Richard, Center for the Study of Intelligence, International Trafficking in Women to the United States: A Contemporary Manifestation of Slavery and Organized Crime (Nov. 1999), p. 8.

Indeed, there have been numerous cases in Western Europe and the United States of women who have become victims of domestic violence, sexual slavery or even murder after meeting men through marriage agencies.[31]

Case Study: Recruitment of victims by use of Technology
In 2006, the Helsinki District court found eight people guilty of trafficking 15 Estonian women (one of whom was mentally handicapped) to Finland and forcing them to work in the sex industry between October 2005 and March 2006. The two leaders of the gang who ran the scheme were already serving prison sentences, but managed to use mobile phones and the internet to recruit victims and advertise sexual services on a popular website, while they were in prison.[32]

USING TECHNOLOGY TO EXPLOIT VICTIMS

Technology can be used for the purpose of exploitation, particularly sexual – either by individuals for their own private use or by organized criminal groups or other entities using the Internet as a commercial tool to general profit by selling images or services.[33] Types of online technology which can be exploited for such purposes include the following:

- Newsgroups: sites for exchange of information can be misused to find women and children for the purpose of exploitation, and to upload and download illegal pornography.
- Web message and bulletin boards: exchange of information misused by sexual perpetrators; similar to newsgroups but can be private and password protected.
- Websites: can be misused as venues for distribution of pornography, maintained recreationally or for profit. Can now offer streaming videos.
- Chat rooms: real time communication can be misused by predators to abuse children or recruit potential victims. No messages are archived or stored, and no log files are maintained.
- File Transfer Protocol (FTP): effective way of exchanging files on the internet, is misused to exchange child pornography. Allows users to have direct access to another's computer hard drive to upload and download files.
- Search engines: powerful indexes of cyberspace, can be misused by criminals to find illegal content.
- Peer to Peer networks and file swapping programs: used to find and download files on online networks, misused to share illegal material. Transmissions are not logged or traceable.

[31] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.41.

[32] 'Trafficking in human beings: Internet Recruitment', Council of Europe, 2007, p.35

[33] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.13.

- Encryption: can be used to disguise the content of files.[34]

Unethical practices are also used, such as 'page-jacking' and 'mouse-trapping' to misdirect internet users to pornographic sites and trap them there.[35] (See counter-response to this; Operation PIN, below)

Sexual Assault online

One very real phenomena which is occurring through the world world web (which may be but is not necessarily related to trafficking in persons) is the stalking by adult predators of children for the purpose of engaging in inappropriate online communication for the sexual gratification of the predator. This has in some cases lead to actual meetings between predators and their child prey, and the sexual abuse of the child.[36] In addition to this, the internet has been used as a means of stalking adult victims; crimes of this nature have ranged from online harassment to physical stalking and physical assault. [37]

Pornographic images featuring trafficked persons

Web pages have advertised women for sexual exploitation who may be trafficked victims. The web is increasingly featuring pornographic websites or websites advertising sexual services. Some photos contained therein may never have been intended by their subjects for such purposes. Some of the women may not even know their photographs are on Web sites.[38] The global trend seems to be an increase in the number of pornographic material appearing online, though Sweden has been cited as an exception; since the passage of law criminalizing buyers of prostitution there has been a decline in web advertisements for brothels and sex clubs.[39]

There have been incidents where trafficked women have been used for the purpose of producing online pornographic material; often such cases highlight the ease with which technology can be used to transcend state borders.

[34] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.18-19.

[35] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.20.

[36] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.22.-23.

[37] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.22.-23.

[38] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.27.

[39] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.27.

Case Study: Technology and Transnational Trafficking

In 2000, Japanese women were trafficked to Hawaii in the USA for the purposes of sexual exploitation. Their traffickers intended to use their victims to do live performances which would be shown to Japanese audiences via the internet; laws in Japanese concerning pornography encouraged the traffickers to conduct their operation in Hawaii. The traffickers advertised in Japan for "nude models"; the women were used to make pornography and perform live Internet sex shows upon their arrival in Hawaii. The operation was entirely aimed at a Japanese market with all website material written in Japanese. The traffickers used digital cameras to capture material, and transmitted it to an Internet Service Provider in California, which Japanese viewers would then access through the Californian server. This case study showcases how technology can be used to circumvent both borders and national laws; women were trafficked from Japan into the United States and exploited for viewers in Japan.[40]

Child Pornography

Though little research has been conducted into the full extent of the nexus between online child pornography and trafficking in children, the link may be in the service it provides to increasing demand. The demand is believed to come through some 50,000 to 100,000 paedophiles involved in organized pornographic rings around the world. The supply is represented by an estimated 14 million pornography sites, containing 1 million pornographic images of children, with some 200 new images posted daily.[41]

The internet is a popular means of distributing child pornography among paedophiles for reasons of its ease and anonymity; where once a paedophile would have to physically seek out material away from his usual community he is now able to access it within minutes. Further to this; the evolution of online payment systems offers anonymity to both purchasers of material and the webmasters who supply it. This makes the internet an attractive market for organized crime groups, and strong incentive for international police organizations to strengthen their cooperative relationships with internet service providers.[42]

Information sharing platforms enable the rapid exchange of materials. Basic technology can be used to create numerous still images from footage, and small files (both images and short movie clips) can be traded on the internet. Alternatively, child pornography will be advertised on the Internet and distributed through the mail.[43]

The internet enables sex offenders to engage children on many levels, from sexual chat to enticing them into physical contact. Often pornographic images are created through the online stalking of children. Stalkers befriend children in chat

[40] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, pp.28-29.

[41] Lewis, Gary., UNODC Representative, India, speech at Cyber Crime Training Programme, Kerala, India, 17 January 2007, available at http://www.unodc.org/india/cyber_crime_kerala_gary_speech.html

[42] EUROPOL Annual Report 2006, (Europol, May 2007), p.11.

[43] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.16.

rooms, and ask them to take pictures of themselves.[44] The many ways of disguising a person's identity has allowed many child sex stalkers to commit sex crimes against children with impunity.

TECHNOLOGY: PART OF THE SOLUTION

It is impossible to halt the advance of technology or to stem the tide of its proliferation around the world, and to do so would be an enormous loss to the majority of people who benefit in legitimate ways from its use.

In fighting transnational organised crime which is facilitated by the use of technology, rather than repressing technology, it becomes necessary to harness its potential to interfere with organized criminal activities and to combat trafficking and assist its victims. There are numerous examples around the world of this being done.

Cooperation is key to efforts to investigate, interrupt and prosecute traffickers; this is all the more so now with the acceleration of globalized technology. The international mobility of offenders and their use of advanced technology makes it more necessary than ever that law enforcers and judicial authorities coordinate their responses to be able to follow crimes and criminals across borders.[45]

USING TECHNOLOGY TO INVESTIGATE TRAFFICKING

Law Enforcement Cooperation through Technology

Article 27(3) of the Transnational Organized Crime Convention calls upon States to:

> "…endeavour to conduct law enforcement cooperation in order to respond to transnational organized crime committed through the use of modern technology."[46]

This provision calls upon States to endeavour to conduct law enforcement cooperation in order to respond to transnational organized crimes committed through the use of modern technology.[47]

There are several promising examples of such cooperation. The work of Interpol particularly highlights the potential offered by technology as a medium of global law enforcement cooperation against trafficking in persons.

[44] Council of Europe document EG-S-NT (2002) 9, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.16.

[45] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.217.

[46] United Nations Convention against Transnational Organized Crime, adopted by the General Assembly in its resolution 55/25 of 15 November 2000 and entered into force on 29 September 2003, Article 27(3).

[47] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.237

The Convention on Cybercrime

The Council of Europe's Convention on Cybercrime (CETS No 185) was signed in Budapest on the 23rd of November, 2001 and came into force on the 1st of July 2004. Though the Cybercrime Convention does not directly address trafficking in persons, it provides procedural and investigative tools to enable law enforcers around the world to cooperate to prevent and combat all types of crime committed on or through the internet, including trafficking. This is particularly so in light of the interaction between this Convention and the Convention on Action against Trafficking in Human Beings (CETS No 197).

"I-24/7 system" Interpol

Interpol is the largest international police organization in the world, with 186 member counties. Its purpose is to support law enforcement agencies to fight crime globally, with combating trafficking one of its five key priority areas of action. Among its key activities towards this end, Interpol provides an intelligence clearing house on traffickers, to facilitate the identification of international links in trafficking investigations. Human resources are also linked globally, with crime intelligence officers establishing international networks of contacts in conjunction with Interpol National Central Bureaus (NCBs) and Sub-Regional Bureaus (SRBs).[48] In 2006, Interpol created the Human Smuggling and Trafficking Message to provide a standardized format for easy information exchange. The message is accessible to all authorised member countries via Interpol's global communications "I-24/7" system.

G8 Sub-group on High-Tech Crime

The Group of 8 countries (Canada, France, Germany, Italy, Japan, Russia, the United States and the United Kingdom) established various subgroups to achieve forty recommendations adopted by G8 Heads of State. One of the those is the 'Subgroup on High-Tech Crime', originally mandated to strengthen the ability of G8 countries to prevent, investigate and prosecute crimes involving computers, networked communications and other new technologies.[49]

The Virtual Global Taskforce (VGT) [50]

The Virtual Global Taskforce (VGT) aims to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse. VGT is currently comprised of law enforcement agencies from around the world, including the Australian High Tech Crime Centre, the Child Exploitation and Online

[48] For more information about INTERPOL, visit: www.interpol.int (http://www.interpol.int/Public/NCB/1247/default.asp0)

[49] More information about the G8 Sub-group on High-Tech Crime is available at http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html

[50] Source: http://www.virtualglobaltaskforce.com/

Protection Centre in the UK, the Royal Canadian Mounted Police, the US Department of Homeland Security and Interpol. The key objectives of this cooperative group are:

- to make the Internet a safer place;
- to identify, locate and help children at risk; and
- to hold perpetrators appropriately to account.

The VGT delivers low-cost and high impact initiatives to prevent and deter paedophiles from exploiting children online.[51]

The Internet Watch Foundation (IWF)[52]

The United Kingdom's Internet Watch Foundation (IWF) is an internet 'Hotline' for internet-users to report their exposure to potentially illegal contect online. The aim of the IWF is to minimise such content, including child sexual abuse images anywhere in the world, criminally obscene content hosted in the UK and incitement to racial hatred content hosted in the UK.

Case Study: Child Sex Abuse Image Database

"ICAID" (Interpol Child Image Database) operates as a stand-along system housed at the Interpol General Secretariat. Images are contributed from the image banks of law enforcement agencies around the world, to facilitate global investigations of child sexual exploitation. In 2006, police were able to identify and rescue 131 victims of child sexual abuse using ICAID; in five years, more than 500 victims have been rescued in 29 countries.[53] The International Child Sexual Exploitation Database will be available to member countries directly through I-24/7.

Such image databases showcase effective international law enforcement cooperation as the database is strengthened through contributions made by law enforcement agencies around the world. For instance, the Image Analysis Resource Centre (funded by the US National Center for Missing and Exploited Children from a U State Department grant) was initiated in 2006. As part of this initiative, investigators from the Centre from nine countries worked at Interpol to help specialized officers at Interpol's General Secretary identify children from their home regions depicted in abuse images. This collaboration resulted in the rescue of several children and the identification of several locations. The Image Analysis Resource centre also created an 'Expertise Reference Database' to facilitate identification of locations, including the names of more than 500 experts in various fields to assist in the translating clues contained in photographs to information about victims, perpetrations and locations.[54]

[51] See for instance, Operation PIN as a means of using technology to interrupt trafficking.

[52] For more information about the Internet Watch Foundation, see www.iwf.org.uk

[53] INTERPOL, Annual Report 2006, www.interpol.int, p.11.

[54] INTERPOL, Annual Report 2006, www.interpol.int, p.24.

Case Study: Private Sector Assistance with law enforcement cooperation

Advances made in technology by the private sector are invaluable to the law enforcement sector In investigating transnational crimes. In January 2003, the Toronto Police made a personal appeal to Bill Gates for software that could track transnational pedophilia.

Microsoft responded with the "Child Exploitation Tracking System (CETS)", which enables law enforcement officers from different departments in different countries to collaborate in the pursuit of pedophiles and in the rescue and repatriation of abused children. International input into the system will ensure that the system will function across various jurisdictions where children are trafficked for exploitative purposes. The US Department of Justice and the International Criminal Investigative Assistance Training Program (ICIATP) helped Indonesia to launch CETS in June 2006, and will soon launch in other Asian countries and beyond.[55]

Computer based Training for Law Enforcement

A key means by which technology has been harnessed to strengthen law enforcement response against trafficking, has been through the use of training resources which use a technological platform. Key examples of such resources include the following;

Learning Human Trafficking modules *(UNODC)*

Computer-based training (CBT) is a form of e-learning, involving training presented on interactive CD-ROMs and lessons delivered via interactive television. In this way, students who are located in remote areas throughout the world can learn practical skills at their own pace. This training package has been designed to enable law enforcement officials to enhance their skills, knowledge and awareness at their own pace and in their own language using state of the art interactive computer-based law enforcement training packages. Programmes are tailored for domestic legal circumstances, but also emphasise the regional and global impact of transnational organized crime.

A training module on human trafficking has been designed for law enforcement personnel with the overall objective of providing basic understanding of human trafficking to enable law students to better detect and respond to the crime.[56]

Law Enforcement Best Practice Manuals *(UNDP, Romania)*

A UNDP Romania project implemented between November 2001 and January 2004 in cooperation with the Romanian Ministry of Administration and Interior

[55] Source: 'Human Trafficking in Asia', Microsoft, 17 April 2007, http://www.microsoft.com/about/corporatecitizenship/citizenship/giving/programs/up/casestudies/asia.mspx

[56] A demonstration of the Human Trafficking module is available at http://www.unodc-elearning.org/index.php?option=com_wrapper&Itemid=43
eLearning home: http://www.unodc-elearning.org/index.php?option=com_wrapper&Itemid=33

with funding from USAID lead to the training manuals for law enforcement. These training manuals were launched in December 2003 in Vienna as part of a comprehensive Anti-Trafficking Training Strategy for South-East Europe.[57]

Crime Reduction Toolkit *(United Kingdom)*

The Policing Organised crime unit of the UK Home Office established an online crime reduction toolkit as a practical measure to address trafficking in the United Kingdom. The toolkit is intended for use by police, immigration officials, prosecutors, victim support and social services, local authorities, non-governmental organisations and other agencies who come into contact with human trafficking issues.[58]

NATO Advanced Distributed Learning *(ADL) through the NATO School*

The NATO School and ISN in Zurich has produced two courses covering different dimensions of human trafficking. The courses are available to anyone, free of charge via the Learning Management System hosting the Advanced Distributed Learning (ADL) program. The self-paced courses are undertaken independently without the support or involvement of any tutor or professor. Advanced Distributed Learning (ADL) courses offered in relation to TIP are:

- Human Trafficking: Causes, Consequences, Counter-strategies
- Combating Trafficking in Human Beings.[59]

USING TECHNOLOGY TO INTERRUPT TRAFFICKING

Security and Control of Documents

Article 12 of the Trafficking in Persons Protocol concerns *Security and control of documents.* That article states that
Each State Party shall take such measures as may be necessary, within available means:

(a) To ensure that travel or identity documents issued by it are of such quality that they cannot easily be misused and cannot readily be falsified or unlawfully altered, replicated or issued; and

(b) To ensure the integrity and security of travel or identity documents issued by or on behalf of the State Party and to prevent their unlawful creation, issuance and use.[60]

[57] The manuals can be consulted at: www.undp.ro/governance/Best%20Practice%20Manuals/

[58] The UK Home Office Crime Reduction Toolkit can be accessed at www.crimereduction.gov.uk/toolkits/tp00.htm

[59] More information about the NATO courses is available at: http://www.ndc.nato.int/courses/adlcourse.html#cthb. The course specific to anti-trafficking can be accessed via http://pfp.ethz.ch/.

[60] Trafficking in Persons Protocol, Article 12

Around the world, falsification of all kinds of legal documents is occurring on a large scale. New technologies mean that false documents can be more easily produced and criminal networks are able to provide trafficking victims with false passports and other travel documents such as visas. Technical measures are required to make documents more difficult to falsify, forge or alter. Administrative and security elements are required to protect the production and issuance process against corruption, theft or other means of diverting documents.

Several kinds of technology that are new or in the process of being developed offer considerable potential for the creation of new types of document that identify individuals in a unique manner, can be rapidly and accurately read by machines and are difficult to falsify because they rely on information stored in a database out of the reach of offenders rather than information provided in the document itself.[61]

One concern raised during the negotiation of Article 12 of the Trafficking in Persons Protocol was the cost and technical problems likely to be encountered by developing countries seeking to implement highly technological systems; the development of systems and technologies that minimize the amount of sophisticated maintenance and high-technology infrastructure needed to support and maintain such systems will be critical to the success of deployment in developing countries.[62]

"False and Authentic Document" FADO

One example is the European image archiving system called "False and Authentic Documents" (FADO). FADO makes the efficient and effective verification of documents possible, and enables prompt and comprehensive notification of relevant law enforcement or immigration authorities in participating States when misuse of a document or a fraudulent document is detected.[63] Intended to combat organized crime, the FADO database contains:

- images of false and forged documents
- images of genuine documents
- summaries on forgery techniques; and
- summaries of security techniques[64]

High-technology Passports

In 2004, Kyrgyzstan updated its passport format in compliance with international standards set by the International Civil Aviation Organisation (ICAO). Previous passports contained information written in by hand,

[61] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.299.

[62] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.299.

[63] Source: http://europa.eu.int/comm/justice_home/fsj/freetravel/documents/printer/fsj_freetravel_documents_en.htm

[64] Source: http://ec.europa.eu/justice_home/fsj/freetravel/documents/printer/fsj_freetravel_documents_en.htm

facilitating the commission of misuse of document in the commission of transnational crime. There were reports that human traffickers would fly victims from Uzbekistan and Tajikistan via Kyrgyzstan using forged Kyrgyz passport, before transporting them onwards to destinations in the region or beyond. The new passports contain modern technology, including special dye, a particular seal, and data imprinting, making such document forgery substantially more difficult. Passports contain identify numbers repeated on each page by laser, a machine-readable code and a digital image of the passport holder. Special paper has been used to make the passports, containing fibres only visible by ultraviolent light. Further to this, a new system was introduced to make passports issued only from a centralised centre where information is stored in a database which can be checked at borders.[65]

Another example of passport security is evident in the use by the Australian government of biometric technology in Australian passports. Biometric technology measures physical characteristics of a person to verify their identity; common biometrics include fingerprints, iris, hand geometry, voice recognition and face recognition. Face recognition technology uses a formula to determine whether a live image of a face matches the electronically stored image of that person.[66]

Border Security

"Operation Paludin Child" (United Kingdom)

'Operation Paludin Child' was conducted in the United Kingdom in 2004. This initiative involved the recording of the personal details of every child arriving at border posts throughout the United Kingdom who was assessed as possibly being at risk or trafficking or exploitation.

Each child was issued with an identification number, had his or her photograph taken and was asked to say where he or she would be living in the United Kingdom. If the child could not be located at the address given during subsequent visits of social services staff, an investigation would be opened. Details of the adults welcoming unaccompanied children at airports or ports were also recorded.[67]

"Frontex"

Frontex is the European Union's border security agency. Frontex has undertaken many collaborate initiatives with Interpol to ensure border

[65] Source: http://www.irinnews.org/report.aspx?reportid=24471

[66] Source: http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Budgets_Budget2005_InformationSheets_ProtectingAustraliasborders-InformationSheet5

[67] Source: The Job, Volume 28, Issue 953, 13 May 2005. More information about the work of the Metropolitan Police can be found at www.met.police.uk

integrity, and will be increasing its collaboration with respect to undertaking more joint initiatives against specific border-related crimes including trafficking in persons. Some of the projects collaboratively undertaken by Frontex in 2006 include the following:

- Mediterranean Transit Migration (MTM) focused on the establishment of migration-governance guidelines, including safeguards for the protection of migrants, to be developed by the International Centre for Migration Policy Development (ICMPD), Europol and partner countries in Europe and North Africa.
- Project JAWA (Joint Action Western Africa) examined criminal networks involved in smuggling people from Western Africa to Europe, and was carried out jointly with Europol, the United Nations Office on Drugs and Crime and ICMPD.
- Operation Amazon, in which Interpol co-chairs the intelligence unit, tackled air routes from South America to Europe used to smuggle people.[68]

Creative approaches to preventing trafficking using technology

Rapid advances in technology hail new potential and new capacity for creative solutions to creative problems. Some such measures are showcased below:

Case Studies: Creative Law Enforcement Responses

"Operation PIN" (Virtual Global Taskforce)

In December 2003, The Virtual Global Taskforce[69] launched Operation PIN. Operation PIN created a website that purports to contain images of child abuse but which is in fact a law enforcement site.

Anyone who enters the site will be confronted with an on-law law enforcement message, informing the individual that s/he has entered a law enforcement website, has committed an offence and that his/her details have been captured and provided to relevant national authorities. The two key aims of Operation PIN are:

- the capturing of details of individuals who actively seek images of child abuse
- deterring individuals from seeking images of child abuse, by reducing their confidence in the Internet as an anonymous, risk-free arena

Through Operation PIN, details of a number of individuals have been captured and will continue to be caught as the Virtual Global Taskforce works with industry experts to refine aspects of the operation to make the internet a dangerous place for those seeking images of child abuse.[70]

"Operation Pentameter" (United Kingdom)

[68] INTERPOL, Annual Report 2006, www.interpol.int, p.31.

[69] See p.11 above.

[70] Source: http://www.virtualglobaltaskforce.com/

Operation Pentameter was a multi-agency, victim-focused initative aimed at combatting human trafficking for sexual exploitation. Operational activity involved 55 police forces, as well as immigration and serious crime agencies and non-governmental organizations. The Operation also appealed directly to clients of sex workers to help combat trafficking by providing information on women who were possibly forced to work in the sex industry. Evidence gathered from web sites catering for clients of prostitutes suggested that users were becoming more aware of trafficking and urging others to be on the lookout for trafficked women and share such information with the police. The Crimestoppers number (0800 555 111) which allows informants to remain anonymous was central to the provision of such information. During three months of operation, 84 trafficked women and girls were rescued an 232 arrests were made.[71]

Case Study: Creative reduction of demand

Camel Jockeys in the UAE

For many years, young boys have been trafficked primarily from Bangladesh, Pakistan and Sudan to serve as camel jockeys in the United Arab Emirates. After years of campaigning by governments, international organizations and NGOs, a particularly innovative approach to curtail demand emerged in 2005. Alongside legislation banning the use of young boys, camel owners started using remote-control operated robots of comparable size to the young boys formerly used.[72]

Case Study: Creative prevention through empowerment

Microsoft involvement in preventing trafficking

Microsoft is supporting a number of anti-trafficking initiatives in the Asia-Pacific region in a bid to raise awareness of the dangers of trafficking in persons through a range of target groups.

- In Thailand Microsoft hosted local NGO Mirror Foundation's informational video on human trafficking on the Microsoft MSN Search Internet site
- Microsoft also sponsored a prominent Vital Voices' 2007 conference in Asia, to mobilize the engagement of the private sector in combating trafficking in persons.

Through a community investment initiative, Microsoft is acting to reduce vulnerability to trafficking:

- Through the Microsoft 'Unlimited Potential' program, Microsoft is trying to improve the employability in various communities by teaching them how they can benefit from basic information and communication technology skills.

[71] More information about Operation Pentameter can be found at www.pentameter.police.uk, as well as www.ukhtc.org. Also see 'Trafficking in human beings: Internet Recruitment', Council of Europe, 2007, pp.38-39.

[72] For more information on this issue, see www.ansarburney.org/human_trafficking-children-jockeys.html. To learn the perspective of Anti-Slavery International on the UAE's response, visit: www.antislavery.org/archive/briefingpapers/ilo2006**uae**_cameljockeys.pdf

- In 2006, Microsoft committed more than US$1.2 million worth of funding and software to projects targeting at-risk populations and to projects helping to reintegrate victims of trafficking.

Microsoft is also contributing to effort to support law enforcement responses to trafficking.

- In addition to software applications aimed at tracking missing children and uncovering trafficking networks,[73] Microsoft is assisting in law enforcement and NGO capacity building initiatives in developing countries, but training officials in internet and technology analysis techniques which can assist them in locating and prosecuting traffickers.[74]

USING TECHNOLOGY TO PROSECUTE TRAFFICKING

The evolving nature of crime was anticipated by the drafters of the Trafficking in Persons Protocol. Previous treaties listed offences, thereby remaining weak against crime types which evolved through the advancement of technology. More recent treaties are based on the principle of dual criminality, which applies when the same conduct occurs in both the requesting and the requested State and when penalties are above a certain threshold.[75]

Because human trafficking is an offence that frequently occurs across borders, States must take steps to ensure that they can cooperate and assist each other in the investigation of trafficking offences and the prosecution and punishment of offenders. The international mobility of offenders and the use of advanced technology, among other factors, make it more necessary than ever that law enforcement and judicial authorities collaborate and assist the State that has assumed jurisdiction over the matter. In order to achieve this goal, States have enacted laws to permit them to provide such international cooperation and have entered into treaties on mutual legal assistance in criminal matters.

Such cooperation has been greatly advanced by means of information communications technology, which rapidly enables actors in one state to identify those they need to contact in other jurisdictions for the purpose of extradition of persons (under Article 16 of the TOC Convention), transfer of sentenced persons (under Article 17) and making requests for mutual legal assistance (under Article 18). Some of those tools are showcased here:

[73] For more on this, see p.12.

[74] Source: 'Human Trafficking in Asia', Microsoft, 17 April 2007, http://www.microsoft.com/about/corporatecitizenship/citizenship/giving/programs/up/casestudies/asia.mspx

[75] Legislative Guides for the Implementation of the United Nations Convention Against Transnational Organized Crime and the Protocols thereto, UNODC, October 2004, p.196.

"Online Directory of Competent National Authorities" *(UNODC)*

The Online Directory enables competent national authorities to easily access updated contact information of their counterparts in most countries of the world, as well as means of communication and information on the legal requirements for cooperation.

The online directory was initially established in relation to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988. As at 20 November 2007, contact information for competent authorities of more than 150 States or dependent territories (more than 600 authorities) had been provided to UNODC, including information on specific procedures to be followed in urgent cases.

Following decision 3/2 (18 October 2006) of the Conference of the Parties to the TOC Convention, UNODC – as the Secretariat to the Conference of the Parties - has extended the Directory to include authorities designated under that Convention, and now provides information in accordance with Article 16 (extradition requests), Article 17 (transfer of sentenced persons) and Article 18 (mutual legal assistance requests).

Access to the on-line Directory is reserved for competent national authorities designated in accordance with the 1988 Convention or the TOC Convention. The on-line Directory has also been upgraded to allow for external update of the data by the users (CNAs) themselves; users need to simply request a password for the directory, which will permit full access almost immediately.[76]

"UNODC Mutual legal assistance Request Writer Tool" *(UNODC)*

UNODC has developed a mutual legal assistance request writer tool to help practitioners streamline the process of lodging requests. The computer-based tool is user friendly, easily adjustable to a State's substantive and procedural law and practices and requires virtually no prior knowledge of or experience with mutual legal assistance. It also does not require internet access.

The request writer tool guides the user step by step through the request process for each type of mutual assistance, using on-screen templates. The tool prompts users when they have omitted to include vital information, before they progress from one screen to the next in order to avoid incomplete requests and minimize risks of delay or refusal. When data entry is finished, the tool consolidates all data and then automatically drafts a correct, complete and effective request (in Microsoft Word) for final proofing and signature. The tool also provides contact details of where to send your request in other states, and includes useful links to the legislation of other countries. The tool is available free of charge in English, French, Russian, Spanish and Portuguese.[77]

[76] For more information on the Competent National Authorities on-line Directory, visit: http://www.unodc.org/unodc/en/frontpage/upgraded-directory-of-competent-national-authorities.html and www.unodc.org/compauth/index.html

[77] For more information about UNODC's Mutual Legal Assistance Request Writer Tool visit www.unodc.org/mla/index.html

Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition *(Organization of American States)*

During the third Meeting of Ministers of Justice and Attorneys General of the Americas in early 2000, it was decided to improve information exchanges between member states of the Organization of American States (OAS) in the area of mutual legal assistance in criminal matters. A working group was established and developed a pilot project focusing on the creation of a criminal justice information exchange network. The project is a site to enable citizens of OAS member countries to become familiar with their own justice systems, and those of the States they are working with. The site includes a general description of legal systems of countries of the Americas and posts laws, bilateral and multilateral agreements in force concerning extradition and mutual legal assistance in criminal matters. The information is available in the four official languages of the OAS; English, French, Spanish and Portuguese.[78]

European liaison magistrates *(European Union)*

At the European Union level, a framework has been created for the exchange of liaison magistrates to improve judicial cooperation between the member States of the Union. The tasks of the liaison magistrates comprise any activity designed to encourage and accelerate all forms of judicial cooperation in criminal matters, in particular by establishing direct links between relevant departments and judicial authorities in order to facilitate mutual legal assistance. Under arrangements agreed between the home and the host member States, the tasks of liaison magistrates may also include any activity connected with handling the exchange of information and statistics designed to promote mutual understanding of the legal systems of the States concerned and to further relations between the legal professions in each of those States.

USING TECHNOLOGY TO ASSIST AND SUPPORT VICTIMS

Ensuring the Physical Safety of Victims

The requirements of Article 6(5) of the Trafficking in Persons Protocol supplement the provisions of the Organized Crime Convention concerning the provision of assistance and protection to victims. This provision requires that States Parties "shall endeavour to provide for the physical safety of victims of trafficking in persons while they are within its territory."[79]

[78] For more information about the OAS Information Exchange Network, visit: www.oas.org/juridico/mla/en/index.html

[79] Trafficking in Persons Protocol, Article 6(5).

Article 24 of the TOC Convention refers to the dangers represented by "retaliation or intimidation" for those who cooperate with authorities, whereas Protocol article 9(1)(b) also refers to protection from the risk of "revictimization", a significant problem in trafficking cases.

The fears of victims are often fully justified by the very real prospect of retaliation if they assist the competent authorities. It is therefore essential that programmes to protect victims both during and after they have cooperated are implemented and adequately resourced. Subject to domestic legal principles an the rights of the defence, Article 24(2) of the TOC Convention allows the adoption protection measures such as:

a. Physical protection, such as relocation and permitting limitations on the disclosure of information concerning identity and whereabouts;
b. Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as videoconferencing or other adequate means.

Such protection measures are particularly important where witnesses are testifying against organized criminal groups.

Technology for Physical Protection

Protecting of victims, witnesses and victim witnesses can be significantly aided by the use of technology. Measures can range from simple low-cost measures (such as giving witnesses a mobile phone with some credit and relevant emergency telephone numbers) to highly complicated resource-intensive measures (such as domestic or foreign relocation of witnesses or changing the identity of witnesses.)

Technology during Witness testimony: Testimony via video-link

Video-link testimonies, or teleconferences as they are sometimes called, allow witnesses to testify in a location other than the courtroom. Their statement is transmitted in actual time via video-link to the courtroom, where the judge, the defendant, the defence counsel and the public prosecutor watch and listen to the transmission and can ask questions of the witness. The room where the witness is testifying can be a separate room in the court building or in a different location.

This method protects the witness from direct confrontation with and intimidation by the accused. It creates physical distance between the witness and the accused and thus an environment where the witness feels secure enough to testify. It does not, however, prevent the accused from recognizing the witness, as she or he is fully visible to the audience. In cases where it is necessary to guarantee the anonymity of the witness, video-link testimonies can be combined with techniques allowing for the distortion of the image or voice, or both, of the witness.

Providing assistance to victims

There is a clear role for information communications technology in facilitating the safe return of a victim to their place of origin. Beyond this there are creative ways which technology can be used to assist victims of trafficking in persons. A very basic one is the access provided by the internet to numerous service providers who can assist victims. For instance, the International Organization for Migration's Counter-Trafficking Division has an operation tool, the Counter-Trafficking Module (CTM) database which it uses to support the management of victim return and reintegration, with a view to improving services and facilitating coordination between IOM missions.[80]

Case Study: Asia Foundation

Building anti-trafficking linkages in isolated areas

The Asia Foundation seeks to build linkage between isolated anti-trafficking actors and facilitate anti-trafficking efforts by sharing valuable information among counterpart organizations. For instance, many NGOs in rural areas maintain lists for missing persons, some of whom are likely to have been trafficked while many NGOs in cities which are often trafficking destinations, have information on victims currently seeking help. By linking this rural and urban information, victims could be identified and put in touch with their families and outstanding issues could be resolved.

One of the goals of The Asia Foundation's initiative is to build linkages between isolated anti-trafficking groups across the region. Many of these groups maintain information that could be of tremendous value if shared with counterpart organizations. For example, many NGOs in rural areas will maintain a list of missing persons, especially those who are likely to be victims of trafficking. In cities that tend to be destinations of trafficking, several NGOs and authorities maintain information on victims who are currently seeking help. If the NGOs and authorities across the region (rural and urban) could share information, the victims could be put in contact with their families, and many of the cases on missing persons could be resolved. [81]

Facilitating return of victims

The Asia Foundation is also supporting the development of a web-portal on trafficking in persons, which supports information sharing and dissemination throughout anti-trafficking networks so that arrangements can be made for the safe return of victims through strong NGO collaboration. The portal will have a secure intranet space for sharing sensitive information as well as a public space for information dissemination. Missing persons who are likely victims of trafficking and mechanisms to assist them will also be provided on this website, as well as law and regulations to assist in the cooperation between NGOs working in different jurisdictions.[82]

[80] For more information about IOM's Counter Trafficking Module Database, see http://www.iom.int/jahia/Jahia/pid/1

[81] "Utilizing Information Technology to Address Human Trafficking", The Asia Foundation, http://www.asiafoundation.org/ICT/trafficking.html, p.1.

[82] "Utilizing Information Technology to Address Human Trafficking", The Asia Foundation, http://www.asiafoundation.org/ICT/trafficking.html, p.1.

Human Trafficking Database

Protection services are hampered by lack of reliable data and access to information and inadequate coordination between service providers. NGOs must raise awareness among policy-makers and the public through the provisions of reliable statistics on the scope and nature of trafficking in persons. The Asia Foundation will support the Cambodian Women's Crisis Center (CWCC) to develop a database to store and analyze thousand of victim records for the purpose of facilitating better coordination and support advocacy and public education efforts.[83]

This paper has been prepared to provide some broad background material for the workshop. Please note that fuller materials, including speaker summaries and workshop conclusions, will be included in the official report of the Vienna Forum.

If you have any further information regarding this topic, please contact:

Anti-Human Trafficking Unit
United Nations Office on Drugs and Crime
P.O. Box 500
1400 Vienna
Austria

tel: +43 1 26060 5687
fax: +43 1 26060 5983
email: ahtu@unodc.org
website: www.unodc.org

[83] "Utilizing Information Technology to Address Human Trafficking", The Asia Foundation, http://www.asiafoundation.org/ICT/trafficking.html, p.2.