CONTENTS

1. Introduction

International Conference on Trafficking was held in Courmayeur, Italy from December 6-8, 2002. The conference dealt with the following six themes: *The Networks and Logistics of Transnational Organized Crime and Terrorism, The Logistics of Trafficking, Trafficking in Firearms, Small Arms and Light Weapons, Trafficking in Stolen Natural Resources, Cultural Objects, Works of Arts and Endangered Fauna and Flora, Trafficking in Human Beings and Smuggling of Migrants and The Networks and Logistics of Trafficking: Emerging Threats and New Challenges.*

The Conference was opened by the Minister of Justice of Italy, *Roberto Castelli*. The Minister emphasized that despite the respective distinctions between transnational crime and terrorism, both need to be tackled and on the preventive and the repressive plane. Minister *Castelli*, stressed also that these two levels of action, preventive and repressive, both need to be co-ordinated by all countries interested in the fight against transnational crime and terrorism.

The President of the International Scientific and Professional Advisory Council, *Guido Rossi*, said that the globalization have significantly broadened the transnational criminal market and criminal organizations have become very active on an international level. It is now common belief that individual countries are unable to fight and defeat transnational organized crime and terrorism. Therefore international cooperation becomes essential and there is a need to enhance forms of cooperated action and information sharing.

The Executive Director of the United Nations Office on Drugs and Crime, *Antonio Maria Costa* made an address on the theme "Business and Crime – Trade and Trafficking". He said that although the line between legitimate business and dirty criminal activity might be sometimes thin, we should be keeping the line between them clear. He also contrasted the legitimate trade with trafficking and stressed the importance of fair trade conducted with integrity, on the basis of accountability and fair play.

The first session dealt with the theme "The Networks and Logistics of Transnational Organized Crime and Terrorism".

Thomas Pietschmann, United Nations Office on Drugs and Crime, made a presentation on the theme "The Evolving Nature of the International Drug Trade and Future Trends". He discussed the global drug market by referring to the various data on drug seizures. He also analyzed the recent trend of the drug trafficking. While most of the trafficking patterns have not changed much in terms of routes and geographical distribution in recent years, there has been a change in the organizational structure, i.e. there seems to be a trend towards smaller organizations which keep a lower profile and are therefore more difficult for law enforcement agencies to detect.

Christopher D. Ram, United Nations Office on Drugs and Crime, addressed the topic "The Relationship between Technological Change and Trafficking", discussing. Firstly, he discussed the effect of modern information and communication technology on criminal activities and elaborated upon high-technology and computer related crimes, such as hacking and dissemination of computer virus. Secondly, he discussed the effect of new technology on smuggling and trafficking. He spoke on the issues of the use of encryption by criminals, child pornography and intellectual. He also spoke on how new

technology had been used for trafficking in tangible commodities, such as drugs and firearms and trafficking in human beings.

The second session dealt with the theme "The Logistics of Trafficking".

J. C. Addison, International Maritime Organization(IMO), on behalf of Captain *H.G. Hesse*, Deputy Director, Head of Navigation Safety and Maritime Security Section, Maritime Security Division, IMO, made a presentation on the theme "IMO Activities to Enhance Maritime Security." He discussed the history of IMO activities to enhance maritime security, as well as recent activities of IMO in the aftermath of the tragic event of 11 September 2001 in the United States. After 11 September, IMO reviewed the existing international legal and technical measures to prevent and suppress terrorist acts against ships at sea and in port, and to improve security aboard and ashore.

Neil Bailey, International Division of National Criminal Intelligence Service, the United Kingdom, spoke on the subject "Boats, Planes, Trains and Automobiles: logistics of the trafficking market". He discussed the difficulties that law enforcement agencies are facing in the fight against trafficking in drugs as well as trafficking in persons. He pointed that a huge profit margin is the driving force of trafficking in both drugs and persons and that the profit is so large that those involved in the logistics of trafficking can afford to be quite generous in the cost of trafficking. He also pointed that the difficulty is that the illegitimate consignments of people or drugs are concealed amongst legitimate consignments which would not in themselves raise suspicion. He stressed the importance of information sharing among law enforcement agencies and the cooperation between law enforcement agencies and private sector, including legitimate transport businesses, trade organizations and people who control data bases of routings and consignments of legitimate goods.

The third session focused on the theme "Trafficking in Firearms, Small Arms and Light Weapons."

Nicolas Florquin, Small Arms Survey, Geneva, addressed the topic "The Nature and Extent of Trafficking in Small Arms and Light Weapons with a Focus on Organized Crime. He overviewed the issue of trafficking in small arms and light weapons, discussing the pathways by which legal weapons move from the legal to the illicit circuits, grey market and black market, features of trafficking in small arms and light weapons (SALW) and impact of trafficking and impact of trafficking in SALW. He stressed the importance of transparency in the legal trade in SALW. Governments need to tighten legislation and regulations governing legal production and trade in SALW.

Christopher D. Ram, addressed the topic of "The Use of Criminal Justice Measures to Prevent and Combat Trafficking in Firearms, Components and Explosives". He overviewed both negotiation process and contents of the "Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition," supplementing United Nations Convention against Transnational Organized Crime. He discussed in detail the difficulties encountered in the negotiation of the Protocol. Those difficulties include the issue of whether explosives should be covered by the Protocol, the definition of "firearms" and the breadth of the requirement to mark firearms and the amount of information such markings would contain. He also referred to result of the study on the illicit manufacturing of and trafficking in explosives by

criminals and their use for criminal purposes conducted by the expert group based on the mandate provided by the General Assembly.

The fourth session focused on the topic "Trafficking in Stolen Natural Resources, Cultural Objects, Works of Arts and Endangered Fauna and Flora".

Jeroen Cuvelier, International Peace Information Service, discussed the theme "Assessing the Aspect of Natural Resource Trafficking in Central Africa", analysing the current situation of natural resource trafficking in Democratic Republic of Congo (DRC). He illustrated how a limited group of powerful businessmen had managed to use its privileged relationship with the ruling elites in the conflict zone to set up smuggling networks.

Malcolm Kenwood, Recoveries Director of The Art Loss Register Limited, London, focused on the theme "Trafficking in Stolen Works of Arts and Cultural Objects", overviewing the illicit trade in stolen works of arts and cultural property. He demonstrated two examples of trafficking in cultural property, namely, a still life of fruits by Paul Cezanne which was stolen in 1978 and an Assyrian relief, valued in the region of €7 million.

John M. Sellar, Senior Enforcement Officer, Convention on International Trade in Endangered Species of Wild Life Fauna and Flora (CITES) Secretariat, spoke on the topic "Illegal Trade and the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES)". He presented the overview on illegal trade in wildlife and on the Convention on International Trade in Endangered Species of Wild Life Fauna and Flora (CITES). He illustrated illegal trade in wildlife by referring to a case study of caviar trafficking. He also referred to the initiatives and works undertaken by CITE Secretariat.

The fifth session dealt with the theme "Trafficking in Human Beings and Smuggling of Migrants".

Bertrand G. Ramcharan, Deputy United Nations High Commissioner for Human Rights, spoke on the topic "Human Rights and Human Trafficking", presenting OHCHR's activities for the elimination of trafficking in human beings. He stressed that human rights must be at the core of any credible anti-trafficking strategy and OHCHR action is essential because trafficking is too often seen not as human rights issue, but in terms of only migration, organized crime, development or public order. He elaborated upon rights-based approaches to trafficking in human beings and emphasized the importance of ensuring protection for and assistance to trafficking victims.

Nancy Ely-Raphael, Director of the Office to Monitor and Combat Trafficking in Persons at the Department of State, USA spoke on the theme "Trafficking in Human Beigns" He stressed the importance of protecting and integrating trafficking victims and said that in this efforts, collaboration between Governments and NGOs should be promoted. He also emphasized the importance of sharing best practices among those who are working to stop all forms of trafficking.

Irena Omelaniuk, Director of Migration Management Services, International Organization for Migration (IOM), addressed the topic "The Nature and Logistics of Trafficking in Human Beings", introducing the database on the trafficking situation in the Balkan countries established by IMO. According to the database, trafficking victims in

the Balkan countries are mostly young, educated, unemployed and literate and the majority of them are induced to got to another country through the lucrative job. He also addressed IMO's activities to assist trafficking victims, including activities to provide shelter and medical assistance to trafficking victims.

Grainne O Hara, Legal Officer of Protection Policy and Legal Advice Section, Department of International Protection, UNHCR, spoke on the theme "Trafficking, Smuggling and Refugees: the Contribution of UNHCR". He referred to the UNHCR's participation in the preparatory work of the two Protocols against smuggling of migrants and trafficking in human beings supplementing the United Nations Convention against Transnational Organized Crime. He also expressed the asylum related concerns of the trafficking issues. Refugee women are vulnerable targets for trafficking and trafficked women may be refugees as a result of the trafficking experience and the inability or unwillingness of their country of origin to provide protection against such harm.

The sixth session dealt with the theme "The Network and Logistics of Trafficking: Emerging Threats and New challenges."

Alex Schmid, Terrorist Prevention Branch of United Nations Office on Drugs and Crime, addressed the topic "Links between Terrorist and Organized Crime Networks: Emerging Pattern and Trends". He analyzed the links between terrorist groups and organized criminal groups based on the empirical data. He also argued the incentive and disincentive for cooperation between terrorist groups and organized criminal groups.

F. Steinhäuser spoke on the theme "Illicit Trafficking in Nuclear and Other Radioactive Materials". He and L. Zaitseva developed the Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources (DSTO). F. Steinäuser analyzed the situation of trafficking in nuclear and other radioactive materials between 1991 and 2002 based on DSTO. He also referred to the possibility of nuclear and radiological terrorist attack.

Michael E.G. Chandler, Chairman of Monitoring Group of the Security, United Nations, focused the topic "The funding of Terror: Al-Qaida's Financial Links". He overviewed the background and activities of Monitoring Group of the Security Council, which was originally established based on the Security Council Resolution imposing sanctions on the Taliban. He also discussed the funding and financing situation of Al-Qaida and pointed out that informal transfer mechanism is used by Al-Quida to move their fund and that charities are used to raise fund by Al-Qaida.

2. Opening Session

Welcoming Address

ROBERTO CASTELLI
Minister of Justice, Italy

Transnational organised crime and terrorism are two global challenges that threaten the security of mankind at large and not merely the exclusively internal affairs of any one country. It follows that they need to be tackled with internationally co-ordinated responses and methods.

With regard to terrorism in particular, and also bearing in mind the tragic events of 11 September, a vigorous response has been given by the European Union, which, *inter alia*, has set out a decision-making framework, within which a common definition of terrorist-based crime has been formulated. The United Nations, for its part, has concluded a series of Conventions addressing various aspects of the phenomenon. Organised crime has also been met with a number of responses, both in Europe and around the world. Special mention in this context should be made of the Palermo 2000 Convention and Protocols. Faced with both threats, the United Nations Convention shows the awareness and political will of its Member States, who, despite wide differences in cultures and juridical systems, have found sufficient elements in common to establish a policy to deal with the ever-growing and increasingly alarming levels of criminal violence. With regard to Italy, I would say that our own system already possesses the instruments of substantive and procedural law to combat transnational organised crime and terrorism. In particular, the basic principles of the Palermo Convention are embodied in our juridical system, whilst new provisions have been promulgated to tackle the forms of terrorism manifested in the outrages of 11 September.

I do not wish to dwell in detail on the question of how transnational crime and terrorism either resemble or differ from each other. This is a matter I leave to the experts of this Workshop. However, while I am sure that there are differences in the causes, and certainly in the objectives of the two phenomena, international vigilance with regard to either of them has undoubtedly had repercussions on the other. Moreover, despite their respective distinctions, both need to be tackled on the preventive as well as the repressive plane. If we consider, for instance, the scourge of illicit trafficking, to which you will be giving specific attention, and especially to the detestable trafficking in human beings, it is impossible to ignore the social conditions in which they originate. This fact, and any form of aetiological analysis, should not reduce but rather, if possible, intensify the determination to wage war against the criminals who conduct this shameless phenomenon. The two levels of action, preventive and repressive, both need to co-ordinate and mobilise action by all countries involved, whether at the starting-point, during the transit or at the destination of such traffic in human beings. I spoke at the outset of global challenges. One might well say that clandestine trade and trafficking in human beings represent, in a way, the dark side of globalization. With their roots, in the fragile social fabric of many countries, and assertions, often distorted, that these areas owe their existence to the conditions enjoyed in the more developed world, these

phenomena, unfortunately, are increasingly prevalent, both as a result of the profits available to the traffickers, which are vast, and of the low risk of apprehension which they currently enjoy. One must add, too, that one cannot fight against what one does not know. So, it is precisely in order to enhance knowledge of trafficking that the Italian Government has made available funds for a monitoring project in the form of an index of cases in this field, which has been sent to every Public Prosecutor in Italy. The results have been collated by the National Anti-Mafia Directorate and will be analysed by a specialised Anti- Mafia Institute at the University of Trento. I should add that our National Anti-Mafia Directorate, which is somewhat unique in today's world, has created an information system and database, which, to a degree, is the envy of other countries. We are constantly requested to provide details of the operation and organization of this database. I believe this should be cause for some pride on our part. I would say that if anyone is interested in examining the operation and organization of our information system, the Management of the Directorate will be only too pleased to demonstrate what we have achieved so far. With regard to our international relationships, I am looking forward in a few days time to welcoming various colleagues from the countries of Eastern Europe at Syracuse.

Concluding my brief message, I would like to reiterate that the challenges we face are enormous. Yet I think that international criminal networks, which are efficient and endowed with great resources and (however misplaced, regrettably) great abilities, can be confronted by suitable resources, efficiency and abilities, so as to establish a genuine international network of co-operation between all the States interested in this fight.

Opening Remarks

GUIDO ROSSI
President of ISPAC

First of all, I'd like to welcome everybody, on behalf of the *Centro Nazionale di Prevenzione e Difesa Sociale*, at this Conference which is devoted to quite a topical theme. A theme which is strictly related to the economic and social changes which occurred in the last few decades all over the world and which has been one of the main areas of focus of the scientific activity promoted by the Centro in collaboration with a number of international organizations.

I wish to express a special welcome to Mr. Antonio M. Costa, Executive Director of the United Nations Office on Drugs and Crime, to Ms. Rodica Mihaela Stanoiu, Minister of Justice of Rumania , to Mr. Roberto Castelli, Minister of Justice of Italy, to the high representatives of national and international Organizations or Universities, and to all Participants. Our deep gratitude goes to the President of the Courmayer Foundation and to the Authorities of the Aosta Valley for hosting this event in such a wonderful place.

The recent liberalization of international trade combined with the improved and greater speed of financial transactions and trade, has removed the barriers to the movement of persons, services and goods, causing a market expansion and a greater social and cultural mobility.

However, the globalization process has greatly affected all aspects of social behaviour (not only the behaviours of business), thus including both traditional and new criminal phenomena, which are increasingly alarming. In particular, the advancements in transportation, communications and technology exchanges have significantly broadened the transnational criminal markets and the migratory flows, increasing, at the same time, the so-called *trafficking*. Aside from a general feature of mobility, *Trafficking* includes many unlawful activities which differ from each other for their peculiarities and the way they are perpetrated (for example, trafficking in persons, drugs, small arms and nuclear materials). Globalization has made all these activities and crimes, such as financial or computer crimes and corruption, much more feasible .

In this framework it is essential, but also quite difficult, to understand the unlawful mechanisms commonly used in different activities, to try to determine the method of operation and the connections of criminal organizations which are active on an international level, to identify similarities and links between traditional criminal *networks* and terrorist organizations that co-operate and avail themselves of each other's competence and specialization.

During these three days of the Conference, we should be able to effectively contribute to the debate and to better identify the phenomena in question.

ISPAC has functioned as a forum to devote special attention to the examination of these phenomenon. In recent years, it has focused on topics such as transnational crimes (1998), countering terrorism through international cooperation (2000), and the ratification of the Palermo Convention on transnational organized crime (2001).

The rationale during ISPAC's activity has been to find appropriate ways to meet the need to understand the new transnational criminality in order to help formulating an equally transnational approach. The traditional approach, based on national responses, has been considered by many as being no longer conducive to facing challenges which are becoming increasingly complex especially in terms of the technology used, or in relation to the interests involved. Until very recently, in fact, the fight against transnational crime and terrorism has been frequently carried out on a national basis by single States, which have at their disposal various *ad hoc* instruments in order to comply with the peculiar nature of these crimes. However, even if certain responses are specific to and must be formulated by individual States, it is now common belief that individual countries are unable to effectively fight and defeat so complex crimes, that go beyond any single national jurisdiction.

Therefore international co-operation becomes essential and, as it has been outlined by ISPAC Conferences, there is a need to enhance forms of coordinated action and information sharing. A search for common legislative responses has also been considered an effective strategy, to be pursued mainly through the mutual acknowledgement of legislative and judicial decisions. A first and fundamental step toward international cooperation has been already taken with the development of the *United Nations Convention against Transnational Organized Crime* and its three Protocols to *Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Against the Smuggling of Migrants by Land, Sea and Air and Against the illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition*. The Convention and its Protocols represent a unified response to *Trafficking*, a phenomenon that can and must be eliminated.

Business and Crime – Trade and Trafficking

ANTONIO MARIA COSTA
Executive Director
United Nations Office on Drugs and Crime

I wish to thank ISPAC and *the Fondazione Courmayeur* for the wonderful hospitality in such a beautiful place, and for the opportunity to address the important issues on the agenda of the Conference.

It is indeed a great intellectual stimulus to be here. The wealth of knowledge on crime and trafficking you all have accumulated is impressive. If we could tally it all up, I believe we could show that in this Hall contains several centuries of individual work on the two topics that underpin today's agenda: (*i*) the ways and the means to preserve *honest practices in business and trade*, and (*ii*) what we all can, and should do to fight *the dirty dealings of crime and trafficking*.

The organizers apparently thought that my professional experience could provide a platform to introduce the debate. I thank them for their trust and will do my best to stimulate discussion in a provocative, though constructive way. My approach will be broad, as my perspective is wide-ranging. I came from the world of economics and banking, having worked at the United Nations in New York (on development issues), then at the OECD in Paris (on structural questions), later on at the European Commission in Brussels (on integration matters), and finally at the European Bank in London (the investment house in transition economies). In May I took office as the Executive Director of the United Nations *Office on Drugs and Crime*, whose name speaks for itself regarding the mandates we address. Given this, I was glad to accept the invitation by ISPAC to address this Conference.

Business and Crime. Keep them apart

I will start with business and crime, asking a rhetorical question: are there sharp borders separating the one from the other?

Yes, I believe that there are clear-cut differences between them, although the borders between them should be harder to trespass and better patrolled. In fact, we cannot honestly claim that all business is honest and all white-collar work clean. Criminals do not always wear dark sunglasses, look smart in crocodile-leather shoes, or sport tightly fitted coats with swollen rear pockets. In this age of greed and cynicism the behavioural boundaries between business activity and dishonest dealings have become blurred. It is our role and responsibility to re-draw them, with more efficient controls and tougher policing.

(*i*) *Honest business prevails*

The vast majority of business is of course healthy in its conduct and correct in its performance. Most countries' national income is the sole result of innovation, inspiration, perspiration and risk-taking. Only a small percentage of earnings have origins in the dark alleys of organized crime: no more than an estimated 2-3 percent of global income. Of course, in some countries this percentage is higher, at times much higher than in others. Worldwide, the absolute magnitude of the illegally earned income is significant, estimated at $800 billion, perhaps up to $1 trillion with a third of it generated in narcotic-related activities. The other major source of criminal income is from the trafficking of human beings (almost one million people trafficked per year, without counting the much more significant scourge of smuggling of migrants). Major money makers are also gambling, loan sharking and commerce in counterfeited goods. The illegal trade in arms and smuggling of other commodities complete the picture of transnational criminal activities.

Today's meeting is about fighting the origins of this criminal income. Before I venture into this territory, which represents an important segment of our work in the *Office on Drugs and Crime* in Vienna, I wish to address a related matter: the importance of fighting business activities that, although formally legal and apparently honest, in effect are neither.

(ii) The grey areas of business

Economic historians have gathered evidence that many of today's respected businesses have been built upon yesterday's corrupt, at times violent practices.

Unfortunately, the trend continues. How many legitimate enterprises are today flourishing supported by market misbehaviours such as restricted business practices, price fixing, inside information, and the like? How many shareholders have been robbed of their equity, how many retired workers lost their pension rights because of dubious, even criminal management? How many countries' assets have been stolen by corrupt leaders, then invested in *bona fide* securities around the world? How often has the financial sector been the conduit for hiding assets illegally acquired, turning them into fully acceptable investment means elsewhere?

Retaliation has often come with a vengeance. It is not rare nowadays to see yesterday's successful business leaders and prominent politicians, photographed in black-and-white striped suits (Europe), orange uniforms (US), or grey kimonos (Japan), sitting handcuffed at court hearings or heading towards public jails.

More of these pictures are yet to come. The recent decline in stock markets, worldwide, was determined by the highly predictable correction of earlier excessive valuations. Nevertheless, serious white-collar crime in the management of some large corporations on both sides of the Atlantic and of the Pacific has caused a concurrent crisis of confidence in the integrity of business, thus exacerbating the plunge of share values.

When unethical business practices are widespread, questions are asked about the integrity of the system, and the robustness of the moral principles that guide the players therein. Should we despair? Not at all. But, as with our personal religious beliefs and ethical principles, we need to work hard to keep the faith.

Churchill once stated: "*democracy is a very bad political system, if it were not for the fact that all others are even worse*." The same is true of the market economy and of capitalism. In this day and age, we have plenty of evidence that all other economic systems have failed: they have either disappeared or have reconverted to the liberal system.

Instead, capitalism has brought wealth -- yes, unevenly distributed wealth, but a lot of it to all societies. Statistics speak loudly. The economies that have been more open and better integrated in world markets have performed better than those that have remained in state hands, unable to reap the benefits of private enterprising and free trade[1]. Capitalism's relative success, empirically verified, has provided the grounds for its legitimacy, most visibly of course in times of economic prosperity.

Yet, from both a moral and an operational viewpoint, all societies need to do something about the frequently heard accusation that the line between legitimate search for profit and criminal greed in too many instances proved to be a thin one. According to Peter Nove, from the Fraud Investigation Department of the City of London"…*many major crimes are committed solely for profit. In this respect, criminals are like businessmen. It is often only the methods employed that set the two apart*".[2]

(iii) Organized crime: the business of greed

Organized crime is a world in itself, with its own operating rules, financial intermediaries, trafficking routes and market sharing arrangements. It is both organization and state of the mind. The former (organization) facilitates the establishment of "families" and clans; it promotes international arrangements, alliances and united fronts. The latter (the mind set) fosters fresh entries and start-ups, launching better products and charting new territories.

If we leave aside the shedding of blood and the raping of moral principles, in analogy to von Clausewitz's definition of war we could define "organized crime" as "*business conducted by other means*"[3]. Indeed, criminals who are interviewed on their motivations, often describe their occupation as "doing business".

---

[1] Havard Hegre, Ranveig Gissinger and Nils Petter Gleditsch. Globalization and Internal Conflict. Forthcoming chapter in Gerarld Schneider, Kathrerine Barbieri and Nils Petter Gleditsch (Eds.) Globalization and Conflict. Boulder, Colo., Rowman & Littlefield, 2002; quoted from World BankResearch – Working Papers, at
<http://www.worldbank.org/programs/conflict/topic/13188/library/doc?id=15099>, 9/22/02.

[2] Peter Nove. Underground Banking Systems. *ICPR*, July-August 1991, p. 7.

[3] Alfred McCoy. Organized Crime in Australia. In: R.J. Kelly. Organized Crime: A Global Perspective. Totowa, N.J., Rowan & Littlefield, 1986, as quoted in Patrick J. Ryan & Robert J. Kelly. An Analysis of RICO and OCCA: Federal and State Legislative Instruments Against Crime. *Violence, Aggression, Terrorism,* Vol. 3, Nos. 1-2, 1989, p. 60.

What then are these "other means", used by organized crime? The two operational features that distinguish organized crime are intimidation and violence used to acquire, maintain and expand market shares.[4]

Before talking about mafia and syndicates activity, let me note that there is plenty of legitimate business that uses intimidation and violence to the advantage of their market shares. Think, for example, of companies with monopoly status or those engaged in price fixing. Aren't their behaviours a form of intimidation against competitors, suppliers or clients? Or think of brokerage firms that exert the psychological violence of false market analysis to salvage themselves from exposed equity positions, or to avoid unbearable margin calls, or simply to protect unworthy business from which they can then extract premiums and commissions. In fact, the credibility of the market system was severely hurt by improper business activity which, during the stock market upswing of 1995-2001, expropriated several hundred billion dollars – yes!, an estimated $240 thousand million worth of income from investors and workers.

Then, what separates organized crime from such white-collar crime? Organized crime usually challenges two prerogatives of a modern state: the right of taxation and the right to use force.[2] When the institutional power is weak, organized crime can establish a state within the state, running a parallel regime for (certain) sectors of society, applying the rule of the strongest. It is gun enforcement, not law enforcement.

Dishonest business, on the other hand, while formally respecting the rule of law and the authority of the state, violates the self-regulating forces of the market. It breaks the rules of trust established by society, including those set by the business community itself. It is a (modern) form of (ancient) seignorage, a hidden taxation on certain segments of society.

Some countries have at times even sanctioned these behaviours, for example by establishing one set of rules for domestic business and another set for foreign business. Until not so long ago, offering bribes or paying secret commissions to foreign officials in exchange for preferential treatment and business contracts was seen as permissible. It was even tax deductible in some countries.[3]

(iv) The United Nations is doing much to help

Honest and legitimate business stands at one side of the spectrum of economic activity. Organized crime stands at the other end. Legitimate, but dishonest business behaviours are in the middle. Corruption is a common denominator. Hopefully, this will come to an end, as ever higher standards and better norms are demanded by voters and taxpayers. The international community is now working on a UN Convention against Corruption, following in the footsteps of the December 2000 Convention against Transnational Organized Crime.

---

[4] cit .C.J. Wiebrens and A .Roeell. Ondernemen in de onderwereld. *Justitiele Verkenningen*, Nr. 2, 1988.
[2] Frank Bovenkerk. Misdaadprofielen. Amsterdam, Meulenhoff, 2002, p.21.
[3] Vincent Cable. Globalization and Global Governance. London,, Royal Institute of International Affairs, 1999, p.116.

Negotiations on a new Convention against Corruption are presently being conducted in Vienna, supported by my *Office*. More than two dozen countries have offered proposals on how to attack public and private corruption. They have also suggested preventive measures and methods of asset recovery. I am happy to inform you that we are making very good progress and hope to complete negotiations on the Convention against Corruption by the end of next year. We also hope that in 2003 the Convention against Transnational Organized Crime will enter into effect. At the moment over 30 countries already ratified it (a minimum of 40 are needed).

The fight against corruption is more than just cleaning up business and making organized crime more difficult. It facilitates the flow of development aid and foreign investment.[1] At the World Summit on Sustainable Development in Johannesburg last August, I stressed that development cannot cruise safely, it cannot even take off unless the problems of good governance and the rule of law are also addressed. These concerns are at the heart of my *Office*'s mandate, which focuses on combating crime, narcotics, terrorism, and trafficking.

My first conclusion can be summarized as follows. *Beauty is in the eye of the beholder. Similarly, the line between legitimate and honest business on the one hand, and dirty criminal activity on the other is difficult to define: yet the line is there and needs to be respected. The capitalist system cannot exist without ethics and integrity. If business leaders cannot guarantee honesty and transparency, the mechanism of checks and balances that governs our democratic society must allow the shares values of companies that do not behave to plunge, into bankruptcy if necessary. Business is built on trust. The Organized Crime and Corruption Conventions negotiated at the United Nations need to enter into effect soon, with teeth to guarantee that business integrity cannot be challenged with impunity.*

Trade and Trafficking: watch the containers

Having discussed the interface between legal and illegal (even criminal) business, let me now turn to the dichotomy between trade and trafficking. Trade is legitimate if (*i*) it concerns licit goods and services; (*ii*) it adheres to the laws of trading (exporting and importing) countries; and (*iii*) it abides by the rules of arbitration bodies such as the World Trade Organization. Trafficking, on the other hand, takes place in criminal markets, and/or for illicit objects, irrespective of any rules.

We can distinguish two forms of trafficking[2]:

1. provision of illegal goods and services such as narcotic drugs, child pornography, even human beings;

[1] UN Conference Calls Attention to World Poverty. CSIS Globalization org, 4/1/2002, as quoted at *http://www.globalization101.org/news.as?NEWS_ID=28*.

[2] Petrus C. Van Duyne. Crime Enterprises and the Legitimate Industry in the Netherlands. In: C. Fijnaut and J. Jacobs (Eds.). Organized Crime and its Containment: A Transatlantic Initiative. Deventer, Kluwer, 1991, pp. 56-57.

2. unlawful trading of goods and services which are, by themselves, not illegal, such as smuggling of cigarettes, diamonds, or arms.

It is the state, and in a growing number of cases, the international community of states which decides whether a commodity or its trading are legal or not.

(i) Drugs, crime and terrorism: the axis of evil

The UN *Office on Drugs and Crime* is very familiar with drugs trafficking and has fought it for a quarter century. We have measured the huge resources it generates, inside (farmers and petty criminals) and outside (traffickers) the countries where the relevant raw and/or semi-processed materials are produced (opium poppies in Central Asia, coca leaves in the Andean region and amphetamines type stimulants, ATS, in South Asia). We have verified that some of the profits are used to wage war, to protract regional conflicts and humanitarian crises, and to foment terrorism. We have learned of efforts by criminal gangs to trade million of dollars in cash and narcotics for arms. There is evidence that even weapons of mass destruction (chemical, bacteriological and nuclear) have been looked for, and negotiated, in exchange for drug money.

Countries like Colombia, Afghanistan and Myanmar have paid, and continue to pay, a terrible price because of the production of cocaine, heroin and ATS. The drugs and the income they generate are harming other societies as well.

From Asia to Latin America, from the Balkans to the Caucasus and Africa, drugs have been traded for arms. In parallel to this Conference, a group of experts are drafting a legislative guide for the promotion of the ratification and implementation of the UN Protocol against Illicit Manufacturing of, and Trafficking in Firearms. This is the third expert group we have managed to put together. Similar meetings have been held in Vancouver and in Paris for the elaboration of legislative guides for the Palermo Convention and the Protocols on Trafficking in Persons and Smuggling of Migrants, respectively. We hope that the work of this expert group will facilitate the ratification of this vital addition to the Palermo Convention.

Guns are used in crime and in armed conflict. Small arms and light weapons are big killers: some 300,000 people are killed by them every year across the globe. There are up to 600 million such arms in circulation worldwide, one gun for every ten persons on earth.

The word 'circulation' is indicative of the trafficking that takes place – when one conflict comes to an end, the weapons are sold to the next conflict to harvest death and destruction in yet other killing fields. Of 49 major conflicts in the 1990s all but two were waged with small arms as the main weapons.[1] Some 4 million people died in these conflicts, the majority of them civilians.[2] The worst killing has taken place in Africa, where natural resources are both the prize and the exchange commodity for arms.

[1] Idem. ADD Stuff on 3rd protocol.
[2] U.S. Department of State. International Information Programs.21 August 2001. UN Small Arms Conference a Success, U.S. Official Says. By Merle D. Kellerhals, Jr., Washington File Staff Writer.

(ii) Boundless Greed

Despicable as the arms trafficking is, more shameful is the trafficking in human beings. It is estimated that up to two million people annually are victims of this modern form of slavery. One million of them, mainly girls, are still children. It is very urgent that the Protocol to Prevent, Suppress and Punish Trafficking, Especially Women and Children is ratified by all states.

Whether it is drugs, arms, or human beings – trafficking often takes place by means of the same containers that carry most of world trade. About 200 million containers cross the seas every year – a figure likely to double in ten years. At present, only about two percent of them are opened to find out whether the cargo meets the description in the bill of lading. Here we face a dilemma: most trade is run on a "just in time" delivery, in order to keep stocks and storage costs low. Intrusive and extensive controls in search of illegal merchandise would slow down world trade considerably.

We therefore need profiling and risk analysis schemes as well as state-of-the-art inspection methods to combine the need for efficient world trade with the imperative of safety and security. My *Office* is currently working together with the World Customs Organization and other agencies to develop a pilot programme for ports, airports and containers control. We will test this pilot in key ports in Asia, Latin America and Africa.

(iii) United Nations against trafficking

Adam Smith spoke of the *invisible hand* of the market. Yet, a market economy also needs the *visible hand* of the state and the community of states, to set and enforce the ground rules for business and trade. The 1990s have been characterized by: (*i*) the transfer of assets from the public to the private sector; (*ii*) a reduced role for the state in regulatory activities; and (*iii*) global market liberalization.

The world economy is benefiting enormously from these changes. Yet, as ever in human behaviours, this has not come without a price. (*i*) The enormous assets privatisation of the recent past was not always carried out in a transparent manner. In some cases – most notably, in Eastern Europe and the former Soviet Union – it has played into the hands of organized crime. (*ii*) The reduced regulatory activities, and the benign neglect of their importance have facilitated white-collar crime. (*iii*) The global lowering of international barriers has brought along ever more insidious forms of trafficking – from narcotics to arms and people.

Criminal markets can be created, but also dismantled by individual government measures. This is welcome, but not efficient. Crime and trafficking tend then to move to neighbouring states, unless measures are undertaken and implemented on an international, preferably global level. This is the essence of the work of the United Nations *Office on Drugs and Crime* in Vienna. This is where the international

community can agree on common standards of behaviour to fight uncivil society. This is where the custody of such agreements is located.

My second final conclusion is easily sketched out. *Business can be the art of the possible, the creation of something out of nothing. I believe that, collectively, we should set our goals for a civil society a bit higher. Good business and fair trade need to be conducted with integrity, on the basis of accountability and fair play. They must serve the private as well as the public interest, in all countries. Let us join forces to accomplish just that.*

3. The Networks and Logistics of Transnational Crime and Terrorism

The Evolving Nature of the International Drug Trade and Future Trends

THOMAS PIETSCHMANN
United Nations Office on Drugs and Crime, Research Section

Extent of drug trafficking

Global drug seizures are dominated by cannabis, reflecting the fact that cannabis is the most widely abused drug worldwide. Close to 5600 tons of cannabis were seized in 2000 (see Figure 1).The largest seizures are for cannabis herb or marijuana (accounting for 80% of all cannabis seizures) and the second largest are for cannabis resin, also known as hashish. Out of 185 million illicit drug consumers worldwide (4.3% of the population age 15 and above), about 80%, or 147 million people (3.5%), consume cannabis according to United Nations Office on Drugs and Crime (UNODC) estimates.

The next largest seizures concern cocaine (339 tons), consumed by slightly more than 13 million people, and opiates, which are consumed by slightly less than 13 million people worldwide: 213 tons of opium, 53 tons of heroin and 24 tons of morphine were seized in 2000.

Seizures of stimulants amounted to 39 tons, and seizures of ecstasy amounted to 5 tons in 2000. Within the category of stimulant seizures, 32 tons, or more than 80%, were accounted for by seizures of methamphetamine. Most of the rest were seizures of amphetamine.

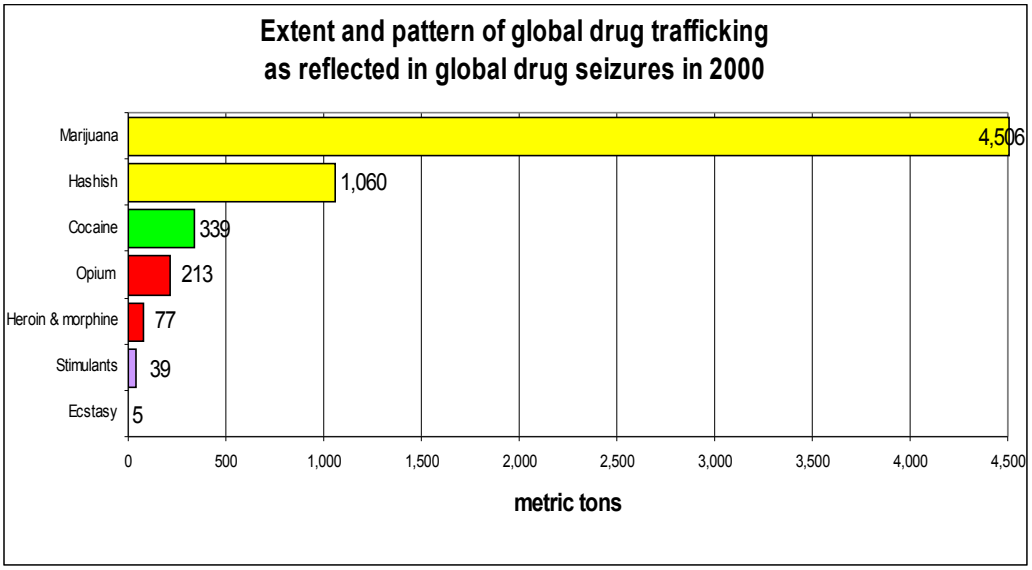


Figure 1
Source: UNODCCP, Global Illicit Drug Trends 2002.

Compared with UNODC estimates of 33 million users of amphetamines (methamphetamine and amphetamine) and 7 million users of ecstasy, seizures of amphetamine-type stimulants are relatively modest. This reflects the difficulties faced by enforcement agencies to seize these substances which – to a large extent – are produced and consumed within the same region. Methamphetamine and amphetamine tend to be produced and consumed within Europe, within North America and within South-East Asia, i.e. they are mainly trafficked 'intra-regionally'. In contrast, heroin, cocaine and, to a lesser extent cannabis, are trafficked 'inter-regionally', offering law enforcement agencies more possibilities to intercept such shipments.

The comparison of production estimates and reported seizures shows that in the year 2000 38% of cocaine production and 21% of heroin and morphine production were intercepted worldwide; interception rates for amphetamine-type stimulants can be assumed to be significantly lower.[1]

Size of the drug markets

The perception of the relative importance of various drugs changes drastically once drug markets are analyzed in economic instead of volume terms. Then cannabis loses its dominant role. In economic terms (i.e. in terms of creating funds that can be laundered and/or used for other criminal purposes, or to corrupt authorities or fuel terrorism) heroin and cocaine trafficking constitutes, by far, the largest threat at the global level. Heroin and cocaine are also the world's most important problem drugs in terms of demand treatment, in terms of related organized crime activity and in terms of drug related violence.

The world's single largest drug market – in economic terms – is the United States of America. Seizures in the USA are dominated by cannabis, mainly marijuana, followed, at lower levels, by cocaine (see Figure 2). In economic terms, however, based on estimates by the US Office of National Drug Control Policy, $36 billion or 57% of the total illicit drug market in the USA is accounted for by cocaine, $12 bn or 19% by heroin and only $10 bn or 17% by cannabis. Synthetic drugs are responsible for most of the rest (less than $5 bn or 7% of the market). Thus according to the US government estimates, cocaine and heroin together account for more than ¾ of the total US market (see Figure 3).

[1] UNODCCP, Global Illicit Drug Trends 2002,

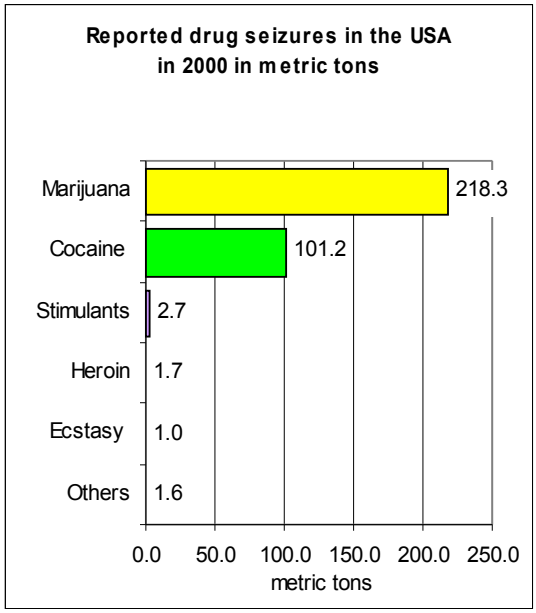


Figure 2

Source: UNODCCP, *Global Illicit Drug Trends 2002*.

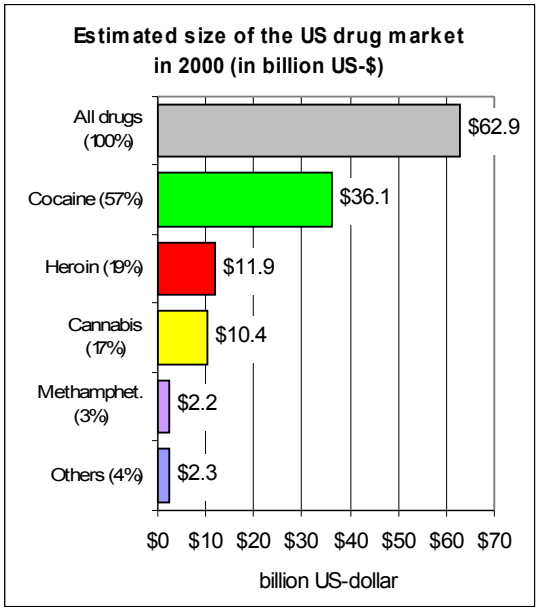


Figure 3

Source: ONDCP, *What America's Users Spend on Illegal Drugs*, December 2000.

Data for the UK show a somewhat similar picture. Seizures in the UK are again dominated by cannabis (See Figure 4). However, in economic terms, the largest drug sales are reported for heroin ($4 bn or 35% of the total drug market), followed by cocaine ($3½ bn or 33%) and only then cannabis ($2½ bn. or 24%) and synthetic drugs $1 bn (8%). Thus, heroin and cocaine – in economic terms – account for more than $^2/_3$ of the UK drug market (see Figure 5).

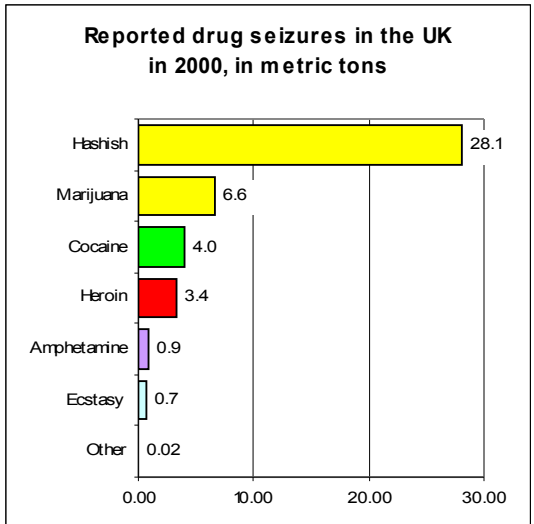


Figure 4

Source: UNODCCP, *Global Illicit Drug Trends 2002*.

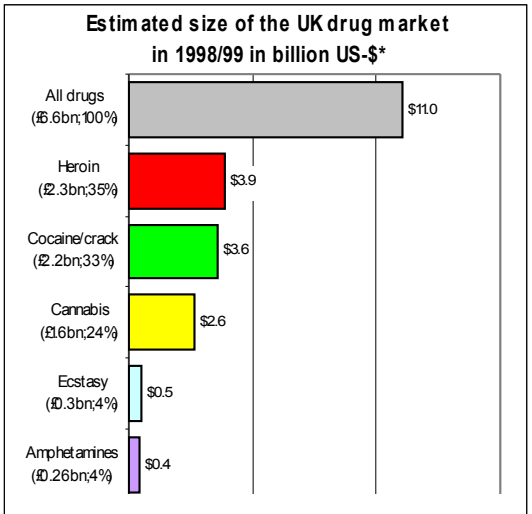


Figure 5

Source: UK Home Office, *Sizing the UK Market for Illicit Drugs*, RDS Occasional Paper No. 74, London 2001.

A similar pattern is also found for Western Europe as a whole. In volume terms, hashish and marijuana clearly dominate overall trafficking and seizures in Western Europe. The next highest seizures – though at far lower levels – are reported for cocaine, heroin, amphetamines and ecstasy (see Figure 6).

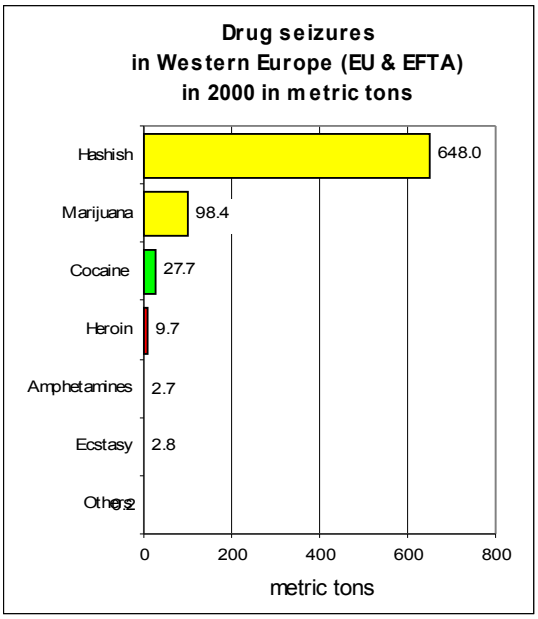


Figure 6

Source: UNODCCP, *Global Illicit Drug Trends 2002*.

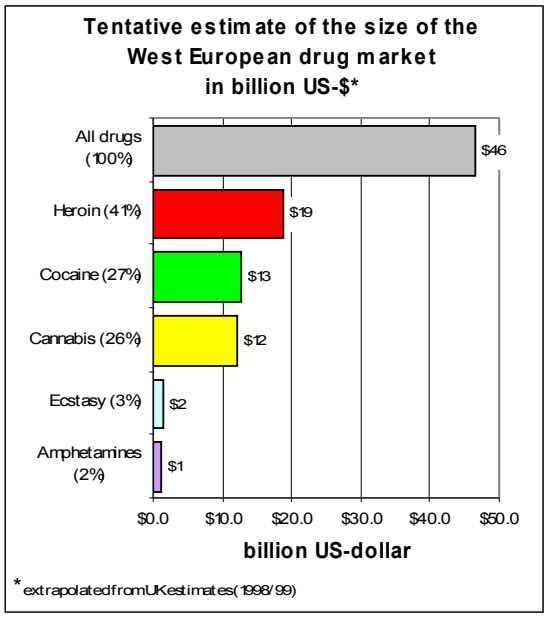


Figure 7

Sources: UN Office on Drugs and Crime, based on UNODC, DELTA and UK Home Office, *Sizing the UK Market for Illicit Drugs*, RDS Occasional Paper No. 74, London 2001.

Yet, in economic terms, the West European drug market is dominated by heroin and cocaine sales. More than $^2/_3$ of the West European illicit drug market – and thus $^2/_3$ of potential trafficking profits – are accounted for by heroin and cocaine. Heroin sales amount to some $20 bn and cocaine sales to some $13 bn (see Figure 7).[1]

Regional distribution and organizational structure of drug trafficking

Almost all countries in the world are affected by drug trafficking. Nonetheless, available seizure data indicate succinct patterns. Seizures – reflecting not only law enforcement successes but also underlying drug trafficking activities – take place primarily in the transit countries in/and around the main countries of production, as well as in 'traditional' consumer countries of North America and Western Europe.

Differences in the global trafficking pattern can be explained, first of all, by differences in location and consumption. The main trafficking route of *cocaine* goes from Colombia to the USA the main *heroin* trafficking routes go from Afghanistan to Western Europe. Both heroin and cocaine trafficking is thus, to a large extent, inter-regional.

There are also differences in the *distribution patterns*. Most *cocaine* is being manufactured in Colombia. Criminal groups from Colombia also play a key role in the distribution of cocaine in the world's largest cocaine consumer market, the USA, notably along the east-coast. The west-coast and the states close to the southern border, in contrast, are dominated by criminal groups from Mexico. Reacting to enforcement pressure, there have been shifts in trafficking routes. While in the early days of cocaine trafficking direct flights from Colombia to the USA served as the main transport route, shipments in later years were organized via the Caribbean, via Central America, via other neighbouring countries of Colombia (such as Venezuela and Ecuador) and via Mexico. Though there are ongoing shifts in trafficking routes across the above mentioned countries, the trafficking routes via these countries, seen in a broader perspective, have not really changed much in recent years. But there have been important changes in the distribution patterns. Much of the cocaine shipments in the 1980s and early 1990s were dominated by Colombian drug cartels. They were hierarchically organised and vertically integrated, i.e. their operations started with the manufacture of cocaine in Colombia (often produced out of coca base imported from Peru), continued with the shipment of the cocaine to the USA, and ended with the sale of the cocaine at the wholesale level, and partly even at the street level, within the USA. Some of these drug cartels (notably the Medellin cartel) used violence systematically as part of their business practices.

This pattern also fits with more recent research by UNODC[2] which found that most violent groups of organized crime are usually those which have a hierarchical

[1] These figures are tentative estimates. They have been derived by extrapolating the UK-results to Western Europe as a whole. The total numbers of estimated heroin, cocaine, cannabis, amphetamine and ecstasy users in Western Europe were multiplied with average expenditure (per drug user) on these drugs reported from the UK. The extrapolation is thus based on the assumption that the consumption patterns of West European drug consumers, on a per capita basis, is similar to that of drug consumers in the UK.

structure, are characterized by strong social or ethnic identity and are involved in narcotics trafficking. In contrast, more loosely organized groups were found to be smaller in size, have no particular social or ethnical identity, and use less violence. Thus, they are seldom seen as posing the same kind of threat to society as traditional hierarchical groups.

Dismantling the hierarchically organized cocaine cartels in the early 1990s was thus positive for society as a whole though it did not stop drug trafficking and *de-facto* enabled an increase in the total number of organizations participating in this business. The new groups usually consist of tightly controlled core groups, assisted by a web of individuals engaged in auxiliary services. While drug trafficking operations in the past were dominated by 10 to 15 major organizations and their subsidiary groups, the illegal trade in narcotics over the last few years was dominated by 150-200 smaller organizations, and many other groups made up of as few as 10 people.[1] In addition, the fragmentation of the Colombian drug trafficking business enabled the rise of Mexican drug trafficking organizations in the 1990s. They supply much of the southern and western parts of the lucrative US market with cocaine. Originally several Mexican groups were only sub-contractors of the Colombian drug cartels, in charge of shipping the cocaine from Mexico across the border to the USA, and handing it back to the Colombian cartels operating within the USA. Following the dismantling of the Colombian cartels, however, they set up their own distribution networks within the USA and became major players themselves.[2] One side-effect of these changes in the market structure was increased competition, and thus an ongoing pressure of cocaine prices to decline even though enforcement efforts in the Americas, and notably within the USA itself, increased strongly.

The *heroin trade* is, in general, far more fragmented than the cocaine trade. Opium is typically produced by Pashtun villages in Afghanistan (and to a lesser extent by Tajik villages in the north). Opium is then sold at the local bazaars and shipped by traders to the borders or transported to local laboratories where it is processed into heroin. Heroin produced in northern Afghanistan leaves the country usually via Tajikistan. Once across the border, Tajik groups take over the business and sell the drugs across the C.I.S. region, notably to Russia. Opium/heroin produced in eastern Afghanistan is trafficked across the border by Pashtun traders. Far more important, in terms of production and trafficking is, however, the opium produced in southern Afghanistan. Once this opium has been shipped to the borders, specialized Baluchi traders usually take over the transport and ship the opium, morphine or heroin to Iran, often via Pakistan. Once in western Iran, Kurdish groups take over and ship it across the border to Turkey. From eastern Turkey opiates are usually shipped to Istanbul. Turkish/Kurdish groups, but increasingly Albanian groups then ship the heroin to Western Europe, sometimes sub-contracting local East Europeans for this purpose.[3] Several depots exist in Eastern Europe. Many of the bulk-deliveries eventually head towards the Netherlands from where they are then distributed, in smaller quantities, across Western Europe. In addition, there are some direct deliveries of heroin

[2] UNODC "Towards a Monitoring System for Transnational Organized Crime Trends: Results of Pilot Survey of 40 selected Organized Criminal Group in 16 Countries", (Draft) September 2002, to be published in *Trends in Organized Crime Journal*.
[1] UNODCCP, "Global Tends in Organized Crime, Internal Report", December 2000, pp. 32-36.
[2] UNODCCP, *World Drug Report 2000*, New York 2000, p. 45.
[3] UNODC, The Opium Economy in Afghanistan - an International Problem, (forthcoming) January 2003, pp. 53-54.

from Pakistan to the UK[1] which may also explain the overall higher levels of purity found in the UK as compared to Western Europe, in general. The actual sales at the street level have in recent years been increasingly taken over by West-Africans and, in some locations, by North Africans[2].

The second largest area of opium production is the Golden Triangle, notably Myanmar and, to a lesser extent, Laos. Much of the heroin manufactured from the opium produced in Myanmar used to leave the region via Thailand. In the past, these shipments were often organized by some of the triads operating from Hong Kong. In more recent years, notably since the mid 1990s, China has emerged as a major outlet of opiates produced in Myanmar. A large number of smaller (Chinese) groups emerged which took over some of the trafficking operations. In parallel, a number of large, hierarchically organised groups continue to operate in the region. They are usually involved in a number of legal and illegal activities, including drug trafficking. Given the strong increase of consumption in China, most of the opium produced in the area of the Golden Triangle is nowadays consumed within South-East Asia,[3] though some is still being shipped to Australia and North America.

A quite different distribution system usually relates to *amphetamine-type stimulants*. In this case, most trafficking is 'intra-regional'. 'Inter-regional' trafficking is usually limited to the supply of the precursor chemicals[4]. (One exception is 'Ecstasy' which in recent years has gained popularity not only within Europe but also outside Europe, though most ecstasy production is understood to still take place within Europe). ATS do not need to be imported into Europe or the USA, but they are - to a significant degree - locally produced. ATS laboratories exist primarily in the Netherlands and neighbouring Belgium (often operated by Dutch groups) as well as, to a lesser extent, in practically all European countries, including East European countries. Production of ATS in Europe is mainly focused on amphetamine and ecstasy (MDMA). ATS production in North America, by contrast, is dominated by methamphetamine. Methamphetamine is also the main ATS produced in East- and South-East Asia[5]. In South-East Asia, organized crime is heavily involved in the methamphetamine trade. This is particularly the case in Japan where the Yakuza is reported to be largely in charge of the highly lucrative methamphetamine business, importing it from other countries in the region, notably from China. In the USA motorcyle gangs used to dominate the methamphetamine business in the 1980s; however, they lost market share to various Mexican crime groups in the 1990s. This shift seems to have been – *inter alia* – related to better controls of the precursor chemicals. As a consequence, good international business connections were required to divert the various chemicals from licit trade. The motor cycle gangs often lacked these connections.

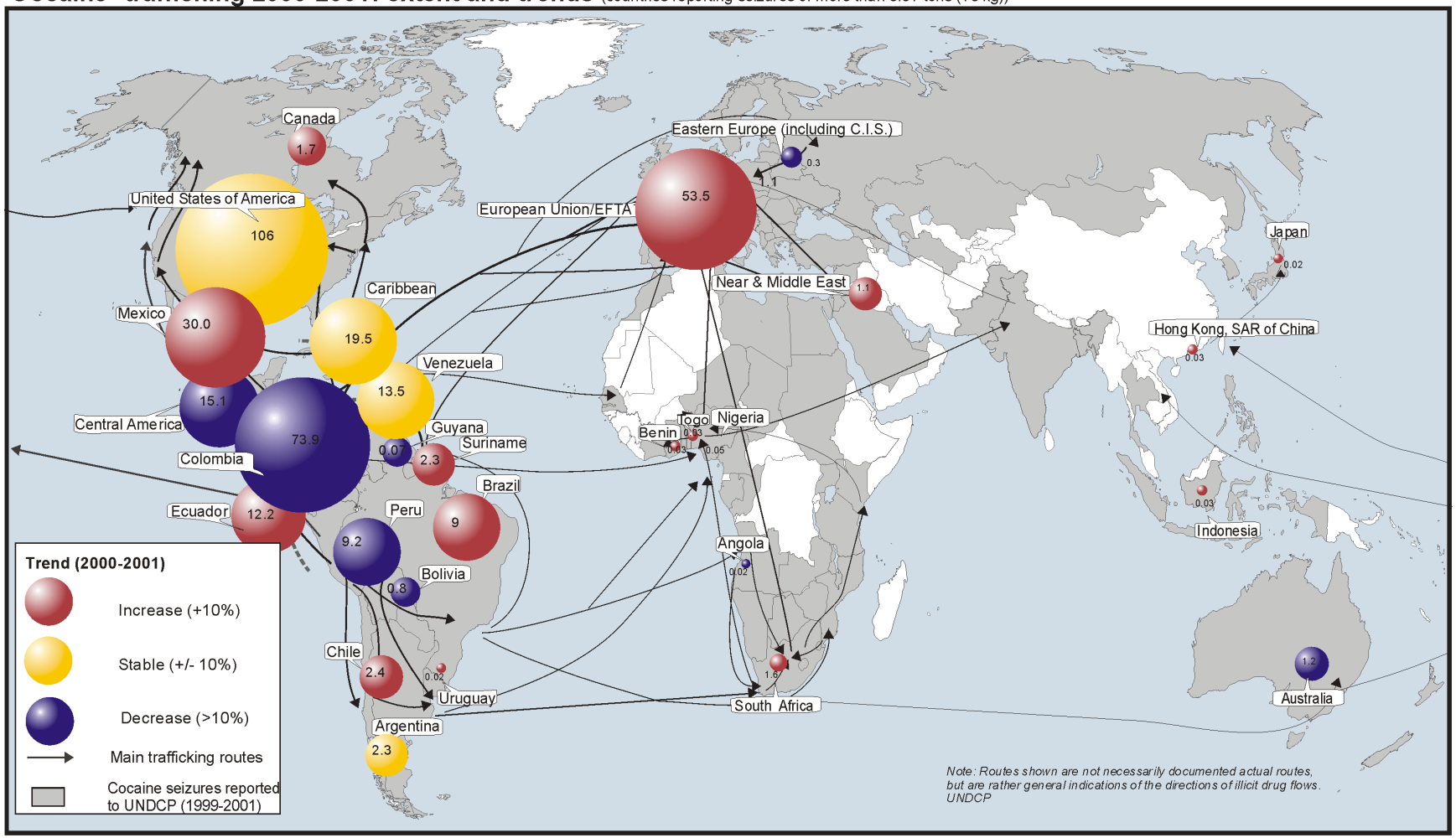
With regard to *cannabis herb trafficking*, there is a focus on Mexico, the United States, South America and Africa, though practically all countries are affected by

[1]UK Forensic Science Service, Heroin Intelligence Database, Heroin Seized from 1 June 2000 to 31 May 2002, London, July 2002.
[2]UNODC, Annual Reports Questionnaire Data.
[31] UNODCCP, Global Illicit Drug Trends 2001, p. 92.
[4] UNDCP, Amphetamine-type Stimulants: A Global Review, Vienna 1996
[5] UNODC, Annual Reports Questionnaire Data.

cannabis trafficking and abuse[1]. *Trafficking in cannabis resin* concerns mainly Europe (notably Spain) as well as Morocco and Pakistan[2].

[1] UNODCCP, Global Illicit Drug Trends 2002, New York 2002, p. 129.
[2] ibid., p. 140.

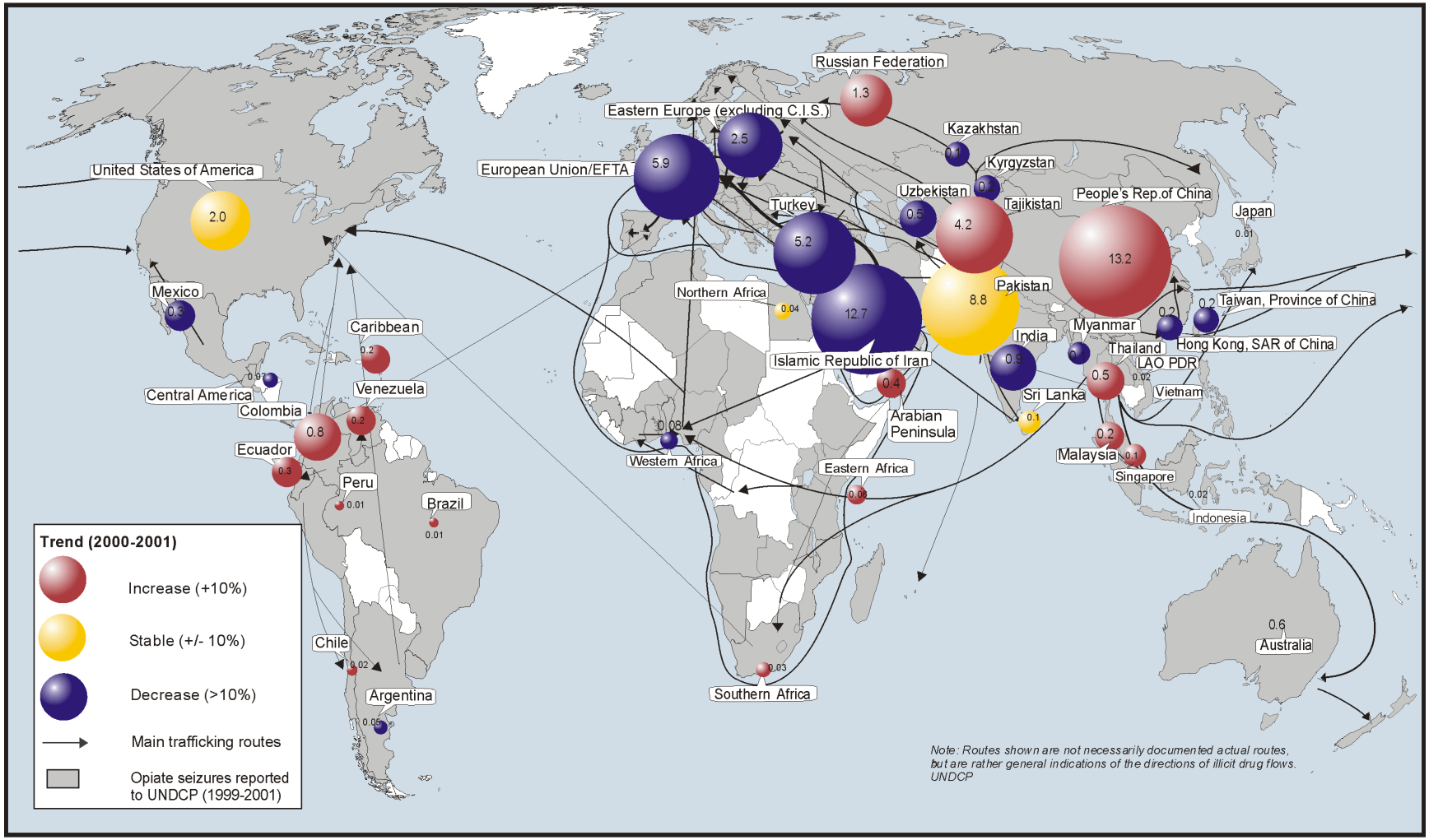
Cocaine* trafficking 2000-2001: extent and trends (countries reporting seizures of more than 0.01 tons (10 kg))



*Cocaine seizures presented in this map do not include seizures in liquid form.

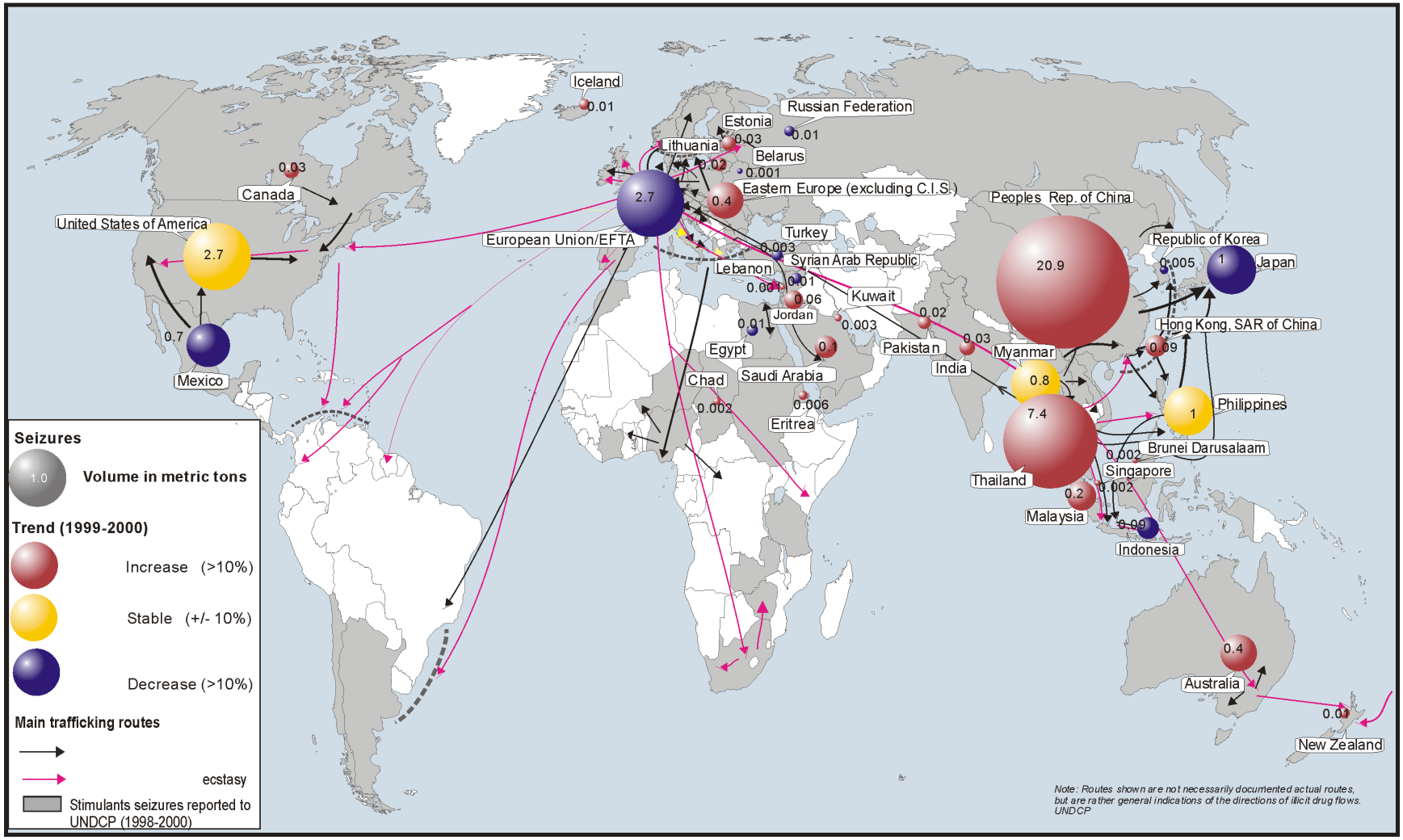
Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Heroin and morphine trafficking 2000-2001: extent and trends (countries reporting seizures of more than 0.01 tons (10 kg))



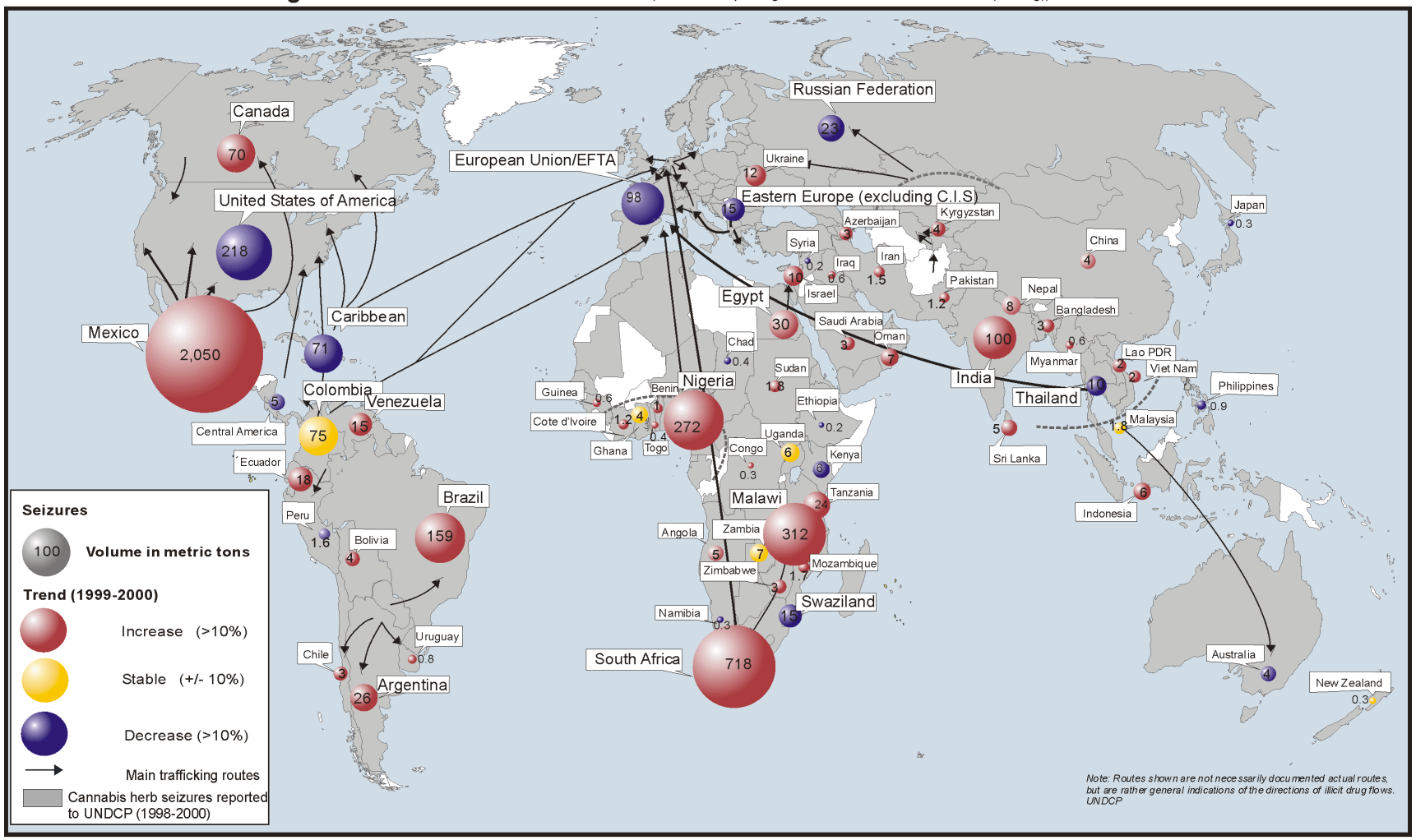
Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Trafficking of amphetamine-type stimulants 1999-2000: extent and trends (countries reporting seizures of more than 0.001 tons (1kg))



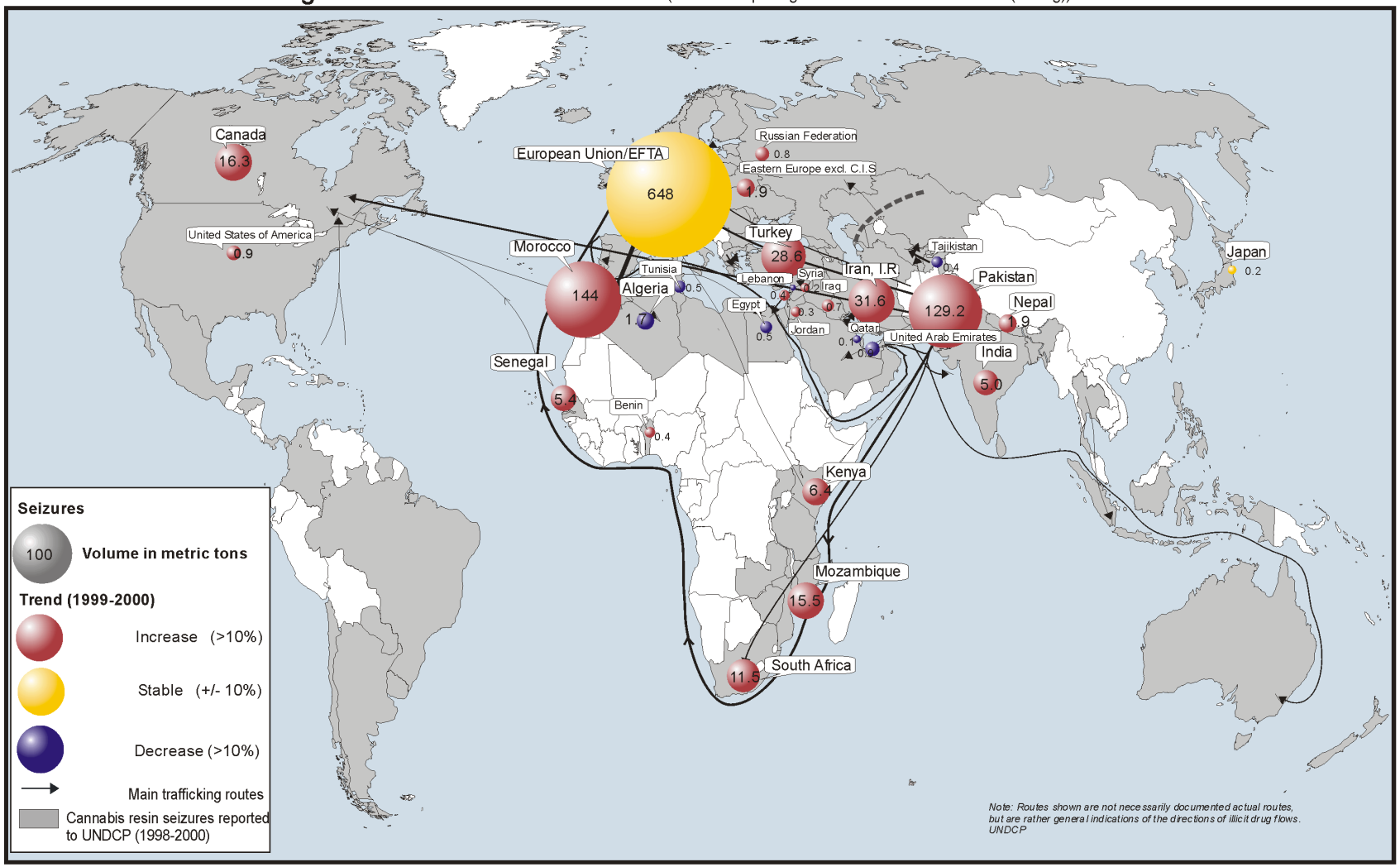
Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Cannabis herb trafficking 1999-2000: extent and trends (countries reporting seizures of more than 0.1 tons (100 kg))



Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Cannabis resin trafficking 1999-2000: extent and trends (countries reporting seizures of more than 0.1 tons (100 kg))



Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations

Trends in Drug Trafficking

The threats arising from drug trafficking should not only be seen in static terms. Time series seizure data (though reflecting enforcement efforts) also provide some valuable information on underlying drug trafficking trends.

Trafficking in opiates

In terms of *heroin and morphine seizures* data show a clear upward trend over the last two decades (see Figure 8). However, the overall upward trend in seizures exceeded increases in opium production (and increases in trafficking), reflecting an overall improved performance of law enforcement. While the interception rate of opiates – calculated on the basis of seizures in heroin equivalents and shown as a proportion of global opium production expressed in heroin equivalents – used to be at around 10% or less in the 1980s, the interception rate rose to 21% by the year 2000.

The peak of heroin and morphine seizures in the year 2000 reflected Afghanistan's record opium harvests of 1999 and the still good harvest of 2000 (and thus record heroin seizures). By contrast, data for the year 2001 indicated a decline in heroin & morphine seizures – a consequence of the Taliban's opium ban which also had an impact on morphine and heroin production. Global opium production fell by 65% in 2001, opium and morphine seizures declined by some 50%. The decline of heroin and morphine seizures taken together was less significant. The existence of huge stocks of heroin in and around Afghanistan and in several of the transit countries guaranteed an ongoing supply of heroin to the main consumer markets in 2001.

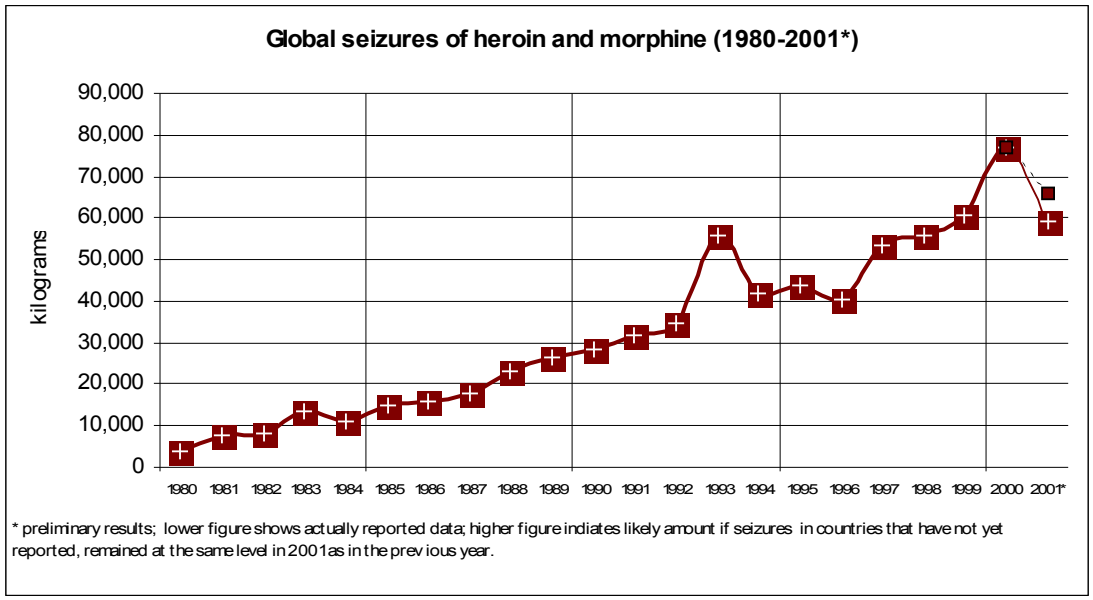


Figure 8

Source: UNODC, DELTA.

Given a delay between opium harvest and the arrival of the bulk of the heroin in the main consumer markets of up to a year, a heroin shortage could have been expected for the year 2002. However, opium production resumed – at a large scale – in Afghanistan in 2002 (3,400 tons as compared to 185 tons in 2001 and 3,300 tons in 2000[1] and so large scale trafficking in opiates resumed as of the second half of 2002. In terms of *heroin* seizures (excluding morphine) data show a strong increase in 2000 and an almost stable trend in 2001 as the market continued to be supplied from heroin stocks accumulated in previous periods (see Figure 9).

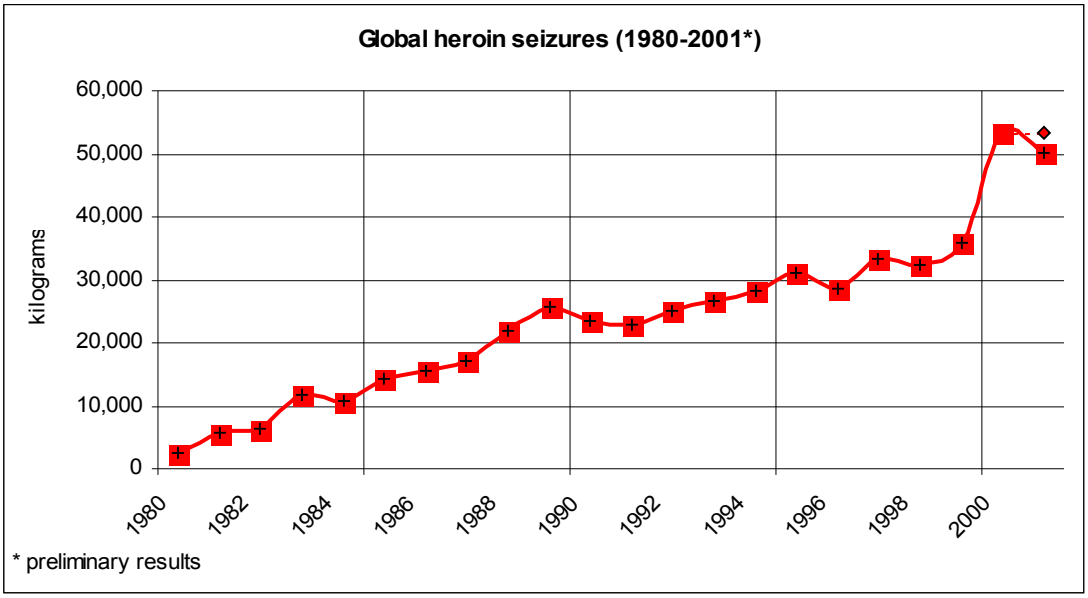


Figure 9

Source: UNODC, DELTA.

The large-scale resumption of opium production in Afghanistan caused, however, important additional problems. Given the opium ban of 2001, opium prices in Afghanistan increased more than 10 fold, from $30/kg in June 2000 to some $300/kg at harvest time in 2001 and $350 per kg at harvest time in 2002.[2] This rise in opium prices also increased the incentives for farmers to get involved in the country's opium economy and makes it difficult, if not impossible, to supply farmers with equally lucrative legal alternatives. Moreover, preliminary results of a study currently conducted by UNODC on Afghanistan's opium economy[3], show that the overall profits of traffickers in Afghanistan are rising as a result of the higher price level (though profit margins are actually falling), creating an additional incentive for the country's opium economy to proliferate.

Trafficking in cocaine

[1] UNODC, Afghanistan Opium Survey 2002, October 2002.
[2] UNODC/ICMP, *Afghanistan Annual Opium Survey 2002.*
[3] UNODC, "The Opium Economy in Afghanistan – An International Problem" (forthcoming), New York 2003.

Global *cocaine seizures,* after having risen strongly in the 1980s, increased only moderately in the 1990s and remained basically stable in recent years (see Figure 10). The stabilization of seizures reflects the largely stable to slightly declining production of coca leaf at the global level in recent years, following massive increases in the 1980s.

As with the opiates, interdiction efforts increased over the last two decades. Rising interdiction efforts are again reflected in growing interception rates which are higher than for any other drug. Over the 1985-2001 period about 40% of the cocaine that was estimated to have been produced, was actually seized, a far higher proportion than in the 1980s (around 30%). The overall high levels of interdiction of cocaine are a consequence of multi-ton shipments of cocaine in boats and containers and reflect the strong priority given to the fight against cocaine trafficking by the US authorities.

These broad trends at the global level conceal, however, some important, divergent trends at the regional levels. Coca leaf production shifted in recent years from Peru and Bolivia to Colombia. Colombia thus is not only the largest manufacturer of cocaine but also the largest producer of coca leaf, the raw material for the production of coca base and ultimately cocaine. Cocaine trafficking has been largely stable to declining in North America, the world's largest consumer market for this drug, in recent years. In contrast, cocaine trafficking continued to increase in South America, Africa and Europe, reflecting growing cocaine demand in these regions.

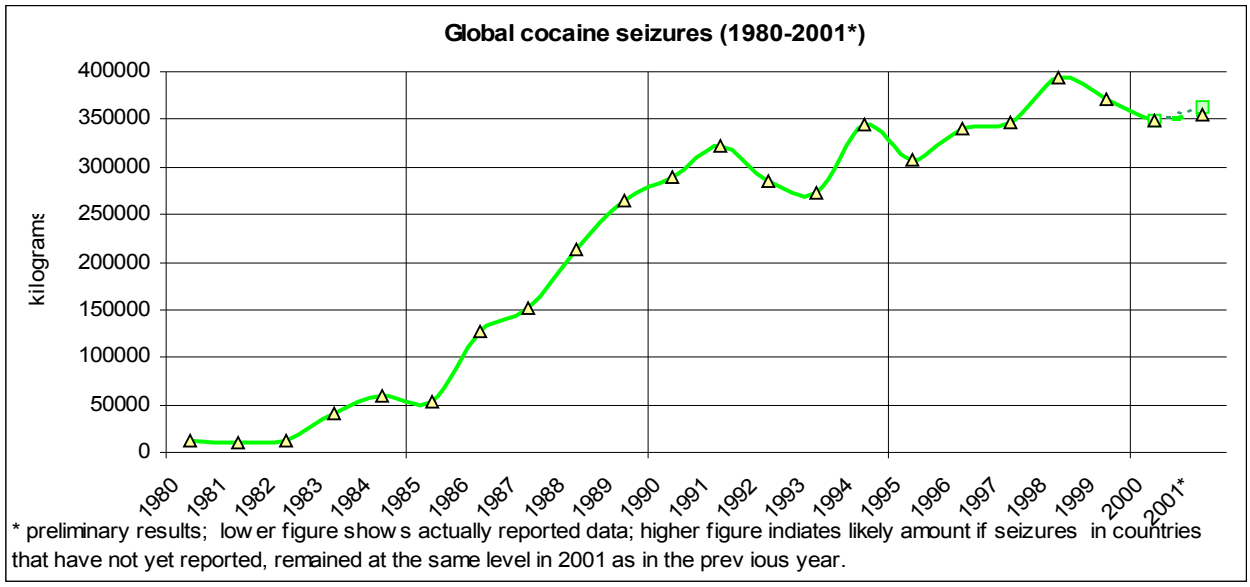


Figure 10

Source: UNODC, DELTA.

Trafficking in amphetamine-type stimulants (ATS)

The strongest increases of seizures and trafficking in recent years were reported for the *amphetamine-type stimulants (ATS).* The growth rates in ATS seizures clearly exceeded those reported for heroin or cocaine in the 1990s. In 2001, however, ATS seizures declined. This decline was mainly due to lower methamphetamine seizures reported from China,

where most methamphetamine production appears to take place. (Excluding China, ATS seizures would have continued to increase). Seizures of ecstasy also showed an upward trend in the 1990s but fell in 2001. Nonetheless, overall ATS seizures remained at far higher level in 2001 than in the early 1990s.

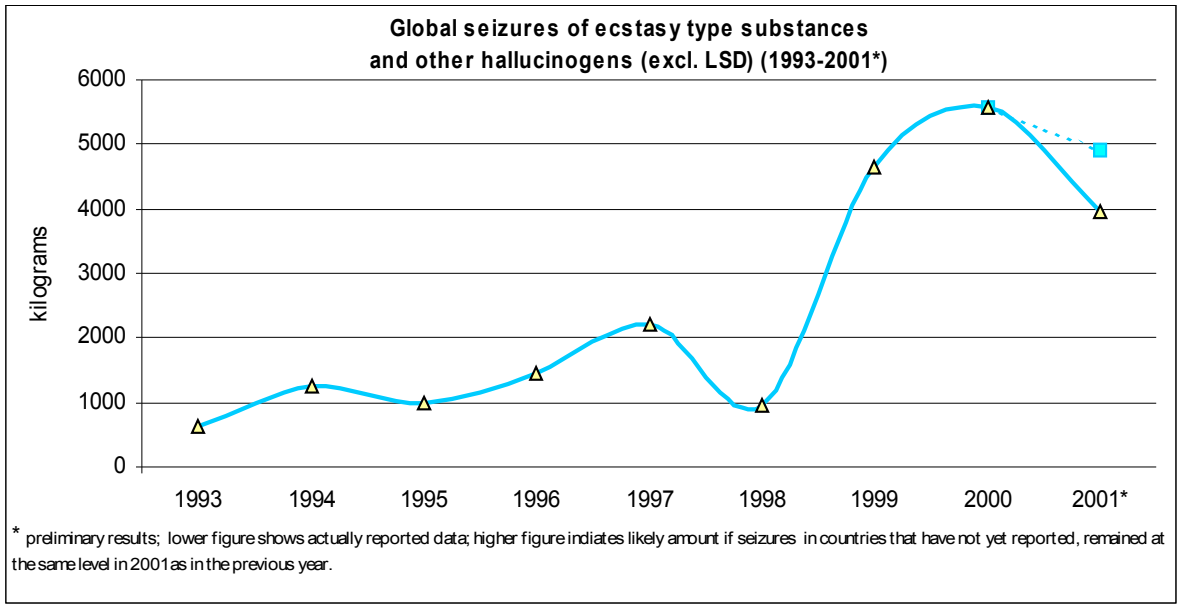


Figure 11

Source: UNODC, DELTA.

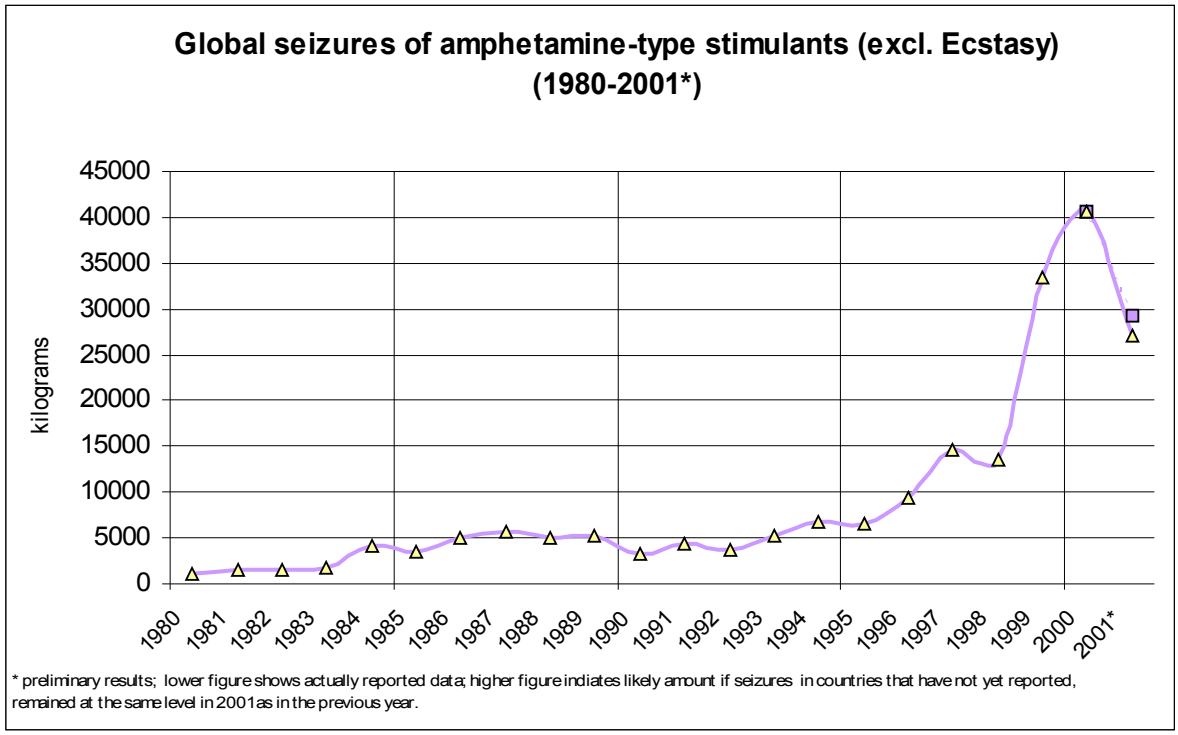


Figure 12

Source: UNODC, DELTA.

Trafficking in cannabis

Changes in cannabis trafficking, and thus in cannabis seizures, were far less significant than those reported for other drugs in recent years, signalling the existence of basically mature markets. Cannabis herb ('marijuana') seizures showed a downward trend in the 1980s but started rising again in the 1990s, notably over the last few years. In contrast, cannabis resin seizures showed an upward trend until the mid 1990s and remained basically stable thereafter. In 2001 cannabis resin seizures fell to the levels reported in the late 1990s.

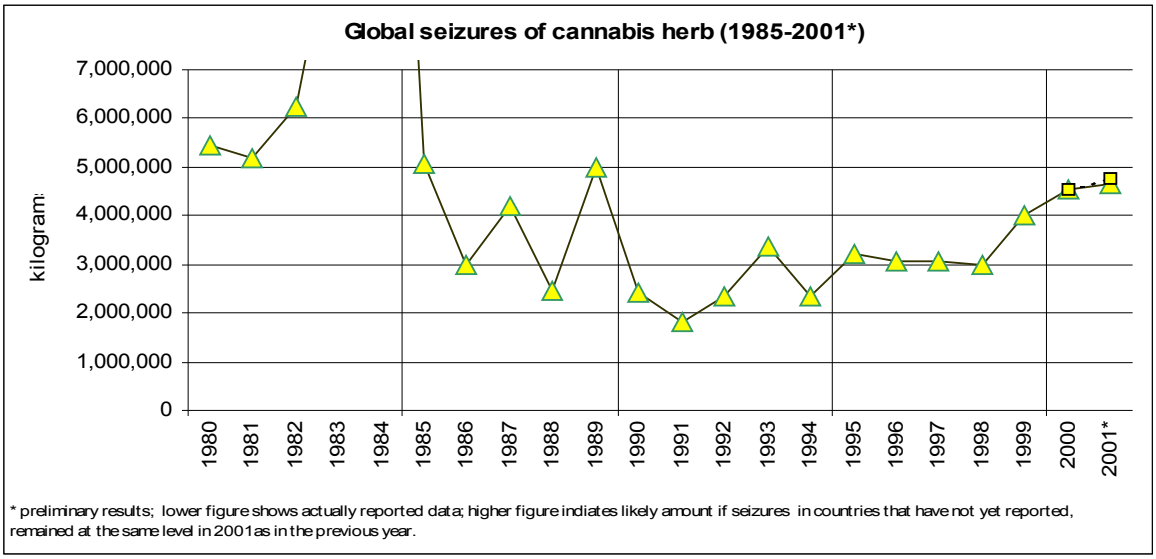


Figure 12 bis

Source: UNODC, DELTA.

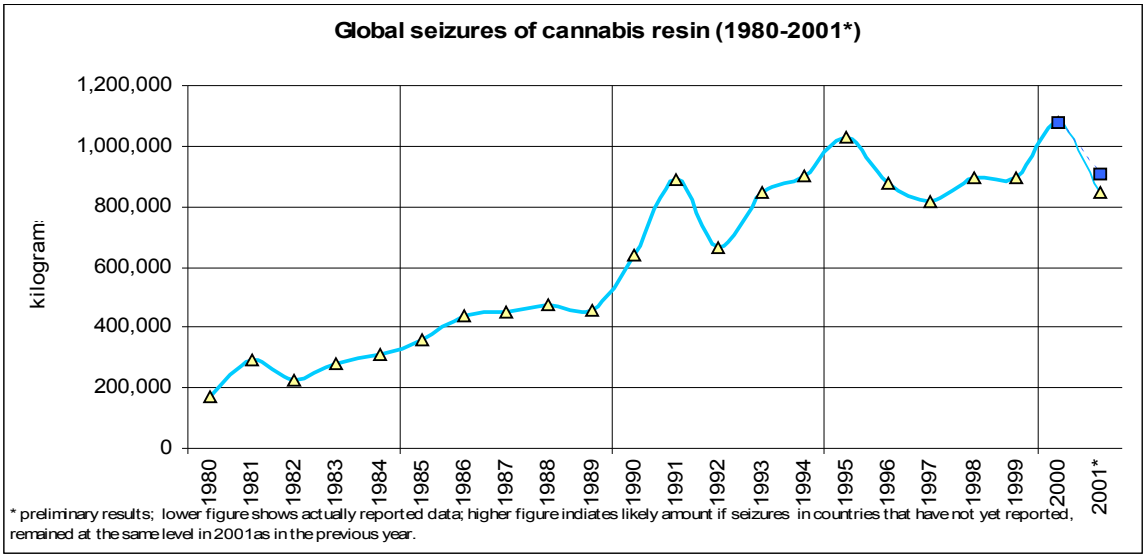


Figure 13

Source: UNODC, DELTA.

Summary and conclusions

Drug trafficking is still the most lucrative business activity of organized crime worldwide. The *drug market* in the USA was estimated at more than $60 bn in 2000 and the West European drug market can be estimated at close to $50 bn. While cannabis is worldwide the most widely consumed drug and – in quantity terms – the most widely trafficked drug, heroin and cocaine account for the bulk of the economic gains from drug trafficking. In economic terms, heroin and cocaine account for more than two thirds of the West European market and more than three quarters of the US market .

Both *heroin and cocaine* are trafficked *'inter-regionally'* while trafficking in *synthetic drugs* is mostly *'intra-regional'*. Trafficking and thus seizures of cocaine take mainly place in the Americas and, to a lesser extent, in Western Europe. Heroin trafficking is mainly concentrated around the two opium producing areas, Afghanistan and Myanmar, as well as in Europe and to a lesser extent in North America. Trafficking in amphetamine-type stimulants is mainly concentrated across South-East Asia and, to a lesser extent, in North America and Western Europe. Trafficking in cannabis herb takes place across the globe. Concentrations can be found in the Americas and in Africa. Trafficking in cannabis resin concerns mainly Morocco, Pakistan and Western Europe.

In terms of the *organizational structure* of the drug business, there seems to be a trend towards smaller organizations which keep a lower profile and are therefore more difficult for authorities to detect. Nonetheless, drug trafficking also continues to be an important source of income for many of the larger crime syndicates which are involved in several legal and illegal business activities.

The two thirds reduction of global *opium production* in 2001 was not repeated in 2002. Global opium production in 2002 increased again to the output level reported in 2000. As a consequence of the Taliban opium ban in 2001 there was a marked decline in opium and morphine seizures in that year. By contrast*, heroin* seizures remained almost unaffected, reflecting the existence of huge stocks built up over the 1999-2000 period. While there may have been some easing of heroin trafficking in 2002, it has to be expected that in 2003 a new wave of heroin supply will head towards the consumer markets of Western Europe and the Russian Federation. In parallel, huge income from drug trafficking in and around the countries of production – when compared to low levels of local GDP – must be expected which may well fuel a number of other criminal activities.

Cocaine trafficking increased strongly in the 1980s but has shown signs of stabilization in recent years. This reflects overall stable production of coca leaf and mainly stable to slightly falling trafficking towards the USA, the world's largest cocaine market. However, this does not exclude increases in some of the transit countries of South America, the Caribbean, Africa and in the consumer countries of Western Europe. In volume terms, cocaine seizures exceed heroin seizures at the global level, in the Americas as well as in Western Europe.

The strongest increases in seizures, reflecting rising levels of trafficking and increased levels of consumption, were reported for the *amphetamine-type stimulants* in recent years. The upward trend, however, did not continue in 2001. But seizures in 2001 were, nonetheless, significantly higher than in the early 1990s.

Cannabis continues to be the substance most widely trafficked worldwide, though it plays less of role as a source of income for criminal groups than heroin or cocaine. Changes in cannabis seizures were less significant than for other drugs in recent years. There has been an ongoing increase of cannabis herb seizures in recent years, though they are still below the levels of the early 1980s. Cannabis resin seizures have been basically stable in recent years after having increased continuously until the mid 1990s.

While most of the trafficking patterns have not changed much in terms of routes and geographical distribution in recent years, there has been a change in the organisational structure of many of the groups that are active in this business. Moreover, access to modern means of transport and to global communication are, in a way, revolutionizing the drug business as well, enabling smaller groups to run large-scale drug trafficking operations. In many parts of the world, cellular phones, notably pay card telephones, already constitute basic instruments for conducting the drug business. There have also been reports of the use of the Internet for conducting international drug 'business' operations, including for obtaining know how, laboratory equipment and the necessary chemical precursors. Drug trafficking groups are also increasingly using sophisticated encryption software in order to avoid detection by the authorities. In other words, a significant number of drug trafficking groups are already making full use of modern technology, taking advantage of globalisation. However, on the law enforcement side, bureaucratic hurdles and issues of national sovereignty often prevent law enforcement institutions from cooperating as actively and closely across borders as is already done by organized crime groups.

Nonetheless, it should be also stressed that rising interception rates over the last two decades (which can be shown for cocaine and heroin) are an indication that the law enforcement bodies have improved their overall effectiveness. However, rising interception rates were largely the result of improvements of interdiction capacities in a limited number of countries. As long as controls in a significant number of countries are not up to international standards, the strengthening of law enforcement efforts in a few countries may lead to a switch in trafficking routes, resulting in spill-overs from transit-trafficking to local consumption and thus in a further spread of drug abuse at the global level. While drug demand reduction programs are an important long-term investment, experience has also shown that most societies have little resistance to drug abuse if availability of drugs increases considerably. Against this background, it should be clear that improved cooperation of law enforcement institutions at all levels, as well as a stronger focus on dealing with organised crime, including in the field of drug trafficking, is necessary to successfully challenge the operations of these criminal groups and limit the spread of drug abuse at the global level.

The Relationship between Technological Change and Trafficking

CHRISTOPHER D. RAM
United Nations Office on Drugs and Crime

Part I: The development of information and communications technologies and the evolution of related forms of crime

Introduction

Smuggling and trafficking in prohibited or controlled commodities is an old problem with a new twist. Recent developments have produced changes at almost every level of commerce. They have altered the ways in which producers and customers are introduced, or in the negotiation of prices and the transportation of goods. More generally, they have altered some elements of the basic social and economic environments within which commerce takes place. More specifically, they have affected the basic nature of the commodities themselves, even creating new ones in some cases. All of these developments have affected both legitimate commerce and the illicit smuggling and trafficking of contraband. In some cases parallel changes have been produced, and in others the developments have produced different effects on legal and illegal or covert activities. But almost every aspect has been affected in some way, and almost all of the effects are significant. This paper will examine some of the changes and the factors which have contributed to them. Its central theme is that the primary (although by no means the only) factors underlying these developments are technological developments, which operate both directly and indirectly, through their support of globalisation.

The increasing globalisation of trade and other economic relationships can be seen, in part, as the product of technological development, particularly in areas such as information, communications and transport. Many of the basic economic pressures and relationships driving globalisation have always existed. From the time of Marco Polo, great fortunes have been made bridging the gaps between the supply of commodities and the demand for those commodities, using the latest transport technologies. Transportation technologies have changed from the camels of the Silk Road, to the tea-clippers of the 19th century, to the aircraft of today, but the basic principles at work remain the same.

The same is true for communications technologies. Having accurate information in a timely manner translates to economic advantage. This has always been the case: in 1815, for example, the English banker Nathan Rothschild famously used carrier pigeons to learn of the defeat of Napoleon at Waterloo 24 hours before his competitors and made a fortune, first selling to create the impression that Napoleon had won, and when prices fell, buying again before the news of the British victory reached the market. Modern investors use broadcasting, newspapers and the Internet to research their investments, and modern offenders use the same media to create misleading information and manipulate prices. Again, the underlying principles and activities remain much the same.

What has changed, primarily as a result of technological developments, is the amount of information which can be obtained and how quickly this can be done, and the speed with which tangible and intangible commodities can be transferred from one place to another. A five-minute Internet search, for example, disclosed 7,530 references to the 1815 activities of Mr. Rothschild, including a Rothschild family archive from which the

information was taken.[1] In fact, as the footnotes to this paper illustrate, many of the sources used to support the propositions it contains were located using the Internet and other information and communications technologies. A more subtle, but also significant change has been in the reliability of the information which can be found. The new technologies allow almost anyone to publish information on-line, but without the filtering effects of professional editing and publishing, there are fewer guarantees that what is published is accurate or free from controversy. In the on-line environment, to the traditional commercial principle of *caveat emptor* might be added the equally-important principle of *caveat lector*.

Technological development can be seen as a cause of globalisation or merely as an essential element of its infrastructure whatever the approach, its overall significance is not in question. One reason for the steady increase in the linkage of key structures (such as the interaction and inter-dependence of national and regional economies, the flow of goods, services, human beings and information from one sector of the global sphere to another), is that a range of new technologies make this possible in ways and at speeds which were not possible in earlier periods. Further these technologies allow access to such flows to ever-broader segments of the population.[2] A central theme of much of the writing about high-technology and computer-related crime – and of this paper – is that this expansion has had much the same effect on the activities of criminal offenders as it has had on non-criminal commercial and private activities.

The proliferation of high-technology and computer-related crime represents a significant threat to high-technology development and the realisation of the benefits of globalisation, and one which proponents of development and globalisation ignore or underestimate at their peril. Criminal behaviour is not, however, the only concern raised by new technologies. The increasingly open flows, particularly of information, have also contributed to more general friction and anti-globalisation sentiments as satellite broadcasting, the Internet and other communications technologies download information which is dominated by the cultures of technologically-developed societies into other societies where it conflicts with established traditional values.[3]

This paper will begin with a brief examination of the nature of modern information and communications technologies, and to a lesser degree of transportation technologies, and their effects on both legitimate and criminal activities. These cannot entirely be distinguished. While most computer-related crime consists of older, "traditional" offences committed or adapted to use the new technologies, some entirely-new forms of behaviour, such as "hacking" and the creation of hostile programs such as computer-viruses have emerged. In some cases, the impact of the technologies on behaviour not previously considered to be criminal has increased the seriousness of individual cases or the collective impact of many cases, to the point where pressure has developed to use the criminal law in order to regulate their activities more effectively. For example, the ease with which information can be taken, copied and transmitted using the new technologies has led to pressure to expand criminal offences and investigative powers to protect such things as intellectual property and trade secrets, the "theft" of which had previously been seen as a matter for civil, and not criminal actions and remedies in most countries.

Turning to the question of the trafficking or smuggling of commodities, the paper will discuss the effects of various technologies in terms of three distinct categories of

[1] http://www.rothschildarchive.org
[2] See Hobsbawm, 2000, particularly at pp.54-56.
[3] See Roach and Macbride 2000.

commodity which have emerged out of the activities of smugglers and traffickers and the responses of governments to those activities. The first category is that of intangible commodities, or what the OECD and World Customs Organisation refer to as "virtual goods", which consist entirely of information or data and can effectively be smuggled or trafficked using the technologies themselves as the primary instrument. The second category is the more traditional range of tangible commodities, such as drugs, firearms and other weapons, or tobacco and alcohol products. The technologies play a major supporting role in these activities, principally in bringing together buyers and sellers, arranging transactions and dispersing proceeds, all on a covert basis. The third category is that of human beings. Human beings have been dealt with as a commodity for many centuries but, recent developments have forced a new appraisal of the problem and fresh action by the international community. Here technologies play a similar role to trafficking in other tangible commodities, but with the added factor that unlike inanimate tangibles, victims of trafficking and smuggled migrants are themselves independent actors whose conduct is directly influenced by the information they receive.

Development and proliferation of information, communication and other relevant technologies

Most analyses of computer-related crime focus on the development of computer and network capabilities since the first network was made operational in the 1960s,[1] and this paper will adopt a similar focus. It should be borne in mind, however, that such recent events are part of a larger and longer-term development of transportation and communications technologies, and that this has produced effects in crime and crime-control which pre-date this period. Wireline technologies such as telegraphy, telephone systems capable of carrying analog voice signals, and wireless telecommunication all pre-date the 20th century, and were used by law-enforcement as early as the mid-1800s.[2]

The most critical developments have occurred since the 1950s, as a series of major technological developments have permitted a steady, and often very rapid expansion in the availability of the technologies, the numbers of people using them, the range of tasks these technologies are capable of performing, and the speeds and volumes at which those tasks can be performed. All of these changes have exerted influences and produced effects, both on crime and crime-control. The pattern has been one of steadily accelerating change as new developments are exploited and trigger even newer ones. Whether this trend will eventually level off remains to be seen. The accelerating rate of change in the late 1900s is illustrated by comparisons of conventional and mobile telephones: users of conventional telephones have increased from fewer than 100 million in 1950 to about 1 billion, or 1/6 of the world's population, in 2000, while the same increase occurred in mobile telephone use between 1990-2000, with mobile use expected to exceed conventional use in 2002 or 2003, and much of the rapid increase taking place in developing countries.[3]

[1] See, for example, Grabowski 2001, O'Neill 2000, and Steele 1997.

[2] Samuel Morse patented the first telegraph in 1838 and telegraph systems using his Morse Code became common during the mid-1800s. The telephone was patented by Alexander Graham Bell in 1876, and the first radio transmissions were sent and received by Marconi in 1899. The first long-distance wireless telecommunications, in which radio signals were reflected off atmospheric layers to reach receivers beyond the line-of-sight horizon were sent from Canada to the UK by Marconi in 1901. A viable trans-Atlantic cable for wireline signals first became operational in 1866. Early criminal cases involving telegraphy include that of John Talwell, apprehended as a result of a telegram from Slough to London in 1845, and Dr. Hawley Crippen, apprehended after fleeing England for Canada by boat in 1910. For the evolution of telecommunications through the period 1950-2000, see ITU 2002.

[3] ITU 2002, Executive Summary, pp. 9-10 and Figures 2 and 5.

Access to the Internet, which did not exist until 1969,[1] was relatively limited during the 1970s. Personal ownership of small computers was rare[2] and most links were between institutions and those working in an institutional context, using them for data-transfer. Only 23 "Internet hosts" existed in 1971, and only 213 in 1981. In the 1980s however a steep geometric increase began, as the technologies became accessible and available and the desirability of access became apparent both to governments and to individual users. By the end of 1985 the number of hosts passed 2,000, in 1989 it had reached 100,000, and in 1990 it passed the 300,000 mark. It reached one million in mid-1992, 10 million in late 1995 or early 1996, 100 million in late 2000, and as of July 2002 stood at over 162 million.[3] On-line commercial transactions, which had been prohibited until 1993, reached $1 billion per year in 1996. In the third quarter of 2001, conservative estimates showed total retail sales exceeded $7 billion in the United States alone.[4]

An "Internet host" is simply a computer connected to the network, identified by querying a sample of possible Internet addresses and tabulating the number of automatic responses, and the number of hosts is therefore not necessarily an accurate indicator of the number of individuals who actually have access to the network.[5] The ratio of users to hosts is probably relatively small – probably fewer than 5:1 in developed countries, where many computers are owned and used by individuals or family units, and many users have more than one access point (e.g., home and office access, portable computer owners etc.). The pattern of usage is different in developing countries, however, where few own their own computers and most people access the network through academic or institutional facilities or through public facilities such as Internet cafés. In these countries, the ratio is probably much greater than 5 Internet-users per host. One on-line source estimated that, in September 2002 at total of about 605 million people had access. Based on an estimated 175 million hosts, the global ratio of hosts to users would be about 3.5 users for each host.[6]

The geographical expansion of the Internet and other telecommunications facilities has also been extensive, although somewhat less consistent. Developing countries lag far behind developed countries, and indicators such as the number or percentage of people "on-line" are seen as important indicators of the development of information-based economies. In 2000, the United Nations reported that only about 4.5% of the global population had network access, but that 44% of North Americans and 10% of Europeans did, while rates for Africa, Asia, and South America ranged from 0.3 to 1.6%. In 2001, the OECD noted that its member states showed a "clear trend" towards knowledge-based economies and highlighted factors other than development, such as the structure and access costs for telecommunications services, which affected rates of access and use.

---

[1] The actual genesis of the Internet depends on which specific development is used as the basis. Development of a military network known as the ARPANET (the US Department of Defence's Advanced Research Project Agency Network) began as early as 1965, but the first public access, in the academic community, did not occur until 1969.

[2] Small computers suitable for personal ownership and use did not exist until 1969 and were not common for another 10-15 years, pending developments in hardware, software, economies of mass-production and public acceptance. See: Polsson, K., "Chronology of personal computers", http://www/islandnet.com/~kpolsson/comphist, visited 30 June 2003. Polsson notes that the first computer intended for the home market was produced in 1969 by Honeywell, at a selling price of $10,600.

[3] Sources: (USA) Public Broadcasting System, "Life on the Internet: Timeline", http://www.pbs.org/internet/timeline/timeline-txt.html and Internet Software Consortium, http://www.isc.org.

[4] Tehan 2002 and (USA) Public Broadcasting System, "Life on the Internet: Timeline", http://www.pbs.org/internet/timeline/timeline-txt.html. The complexity of e-commerce has made its ongoing development increasingly difficult to quantify, see Tehan 2002. Tehan's figures reflect consumer transactions, but do not include other transactions.

[5] Concerning the methodology of Internet Host Surveys, see http://www.isc.org/ds/new-survey.html. In recent years, single machines have been reconfigured to contain multiple addresses, or "virtual hosts", which are now counted as hosts. The Internet Software Consortium notes that, as its figures are based only on hosts which automatically respond when queried, the numbers should be considered minimums, with actual numbers of hosts probably greater.

[6] Source: http://www.nua.ie/surveys/how_many_online/index.html. The NUA figures are based on compilations of other sources and do not indicate the methods used to estimate numbers of users. The estimate of 175 million hosts in September 2002 is the author's, based on extrapolation of the previous internet host data.

Within the OECD, the data also suggest that countries with high rates of access also tended to have higher rates of increasing access. This trend, if it applies to least developed countries, would suggest that, absent mitigating factors, the "digital divide" between developed and developing countries may become wider over time.[1] The ITU takes the opposite view, contending that the digital divide is closing, but its assessment includes the expansion of wireless telephone networks in developing countries and acknowledges that the pattern for Internet access is less encouraging, particularly if the quality of Internet access is taken into consideration.[2] Advances in computer networking, telephone and similar technologies are seen as having significant potential to aid in sustainable development, but only provided that obstacles to satisfactory levels of accessibility can be overcome.[3]

The technologies themselves often contain elements which overcome obstacles to access, and a significant factor to their proliferation in developing countries is their adaptability, often at costs low enough to make such proliferation practicable for the first time. For example, the success of cellular telephone systems in developing countries is largely due to the feasibility of establishing transmitters and microwave links in regions where the high costs of installing wireline telephone systems were prohibitive. Collective or shared use of telephones has reduced individual costs, and the use of solar power and advances in energy-storage have reduced the obstacles due to lack of electrical power. Computer technologies are also particularly well-suited to adaptations which overcome individual obstacles, such as illiteracy and physical disabilities. Low literacy rates were originally seen as a constraint on access, but are becoming less significant as websites are adapted to make them accessible, and Internet access is now seen as both a motivating factor and teaching tool for increasing adult literacy rates and for teaching children to read. The English language remains the dominant language of Internet sites, but the ease and low cost of on-line publishing has also resulted in the dissemination of written materials in many languages where low volumes would previously have made this commercially impractical. The ability of the technologies to produce and disseminate visual images, sound and other non-linguistic content also decreases the impact of language barriers.

Expansion in the range and capabilities of information and communications technologies

The geometrical increases in the number of computers, linkages and users has been accompanied by an equally dramatic expansion in the capability of the various technologies. They are constantly being adapted to perform new functions, and to do so more quickly and reliably.

Basic telephone service, used to exchange verbal messages in analog format, had spread through most developed countries by the mid-point of the 20th century, with steadily increasing penetration in developing countries as the century concluded. The advent of computer technologies, particularly in switching equipment, gradually reduced costs,

[1] See OECD 2001. The OECD itself has no least developed countries as members, which highlights the effects of factors other than basic development levels. Within the OECD, the number of Internet hosts ranged from a high of 70.7 per 1000 inhabitants (USA) to a low of 0.2 (Turkey). The data also suggest that the rate of increase is generally higher for countries with higher basic access rates, although there are exceptions.

[2] ITU 2002, p.6. The ITU notes that the access of many users in developing countries is limited to basic functions such as e-mail by low-speed computers and low-bandwidth networks which cannot handle the larger volumes of data needed to download and view Internet content such as web-pages. Other quality factors encountered by users in developing countries include unreliable network lines and switching equipment which degrade or distort data, and, to the extent that it limits access, very high ratios of users to hosts.

[3] See UN:ECOSOC 2000, Parts IV and V.

increased the complexity of systems, and increased the numbers of persons who could have access to them. Transmission technologies, including the use of communications satellites, wireless microwave transmission, and more recently, fibre-optics, further reduced costs, particularly with respect to long-distance transmissions.

The most recent major development in conventional telephone technologies has been the use of digital formats, in which the analog signals produced by the human voice and understood by the human ear are translated into signals consisting of binary digits. This use of digital formats permits further expansion by enabling many signals to be sent through the same conduit (optical fibre, electrical wire or radio/microwave channel) at the same time, and by increasing the speeds at which signals can be transmitted. Digital formats also facilitate the use of telephones to transmit or receive data other than the human voice, such as visual images and computer data, and the incorporation of technologies such as encryption, which have numerous effects on use by both criminal and law enforcement elements.

The technological advances have brought about a steadily-increasing range of activities the technologies themselves are capable of performing, and a steady trend, known as "convergence" in which the capabilities begin to overlap to the extent where the underlying technologies themselves may become indistinguishable. For example, the Internet has been used to broadcast news or entertainment in live-video formats in much the same way as television broadcasting, and the use of Internet e-mail and verbal conversations as a low-cost alternative to long-distance telephone communications is becoming increasingly common. Specific features of the technologies which support this development include the following.

- **The expansion of wireless communications and increases in available bandwidth and signal-compression.** Wireless communications, including cellular, satellite and broadcast technologies allow access in regions where this was previously unavailable and impracticable, and access for applications which require mobility. The spectrum, or range of frequencies at which wireless communications can be broadcast has been a limited resource, but this has recently been overcome by other developments which allow the same limited bandwidths to carry many signals at the same time. Some of these also allow wireline and fibre-optic channels to carry many signals simultaneously.

- **Increases in miniaturisation and speed.** The first integrated circuit, with five elements, was produced in 1958-59. The Intel Pentium III microprocessor, marketed in 1999, had 28 million elements, each capable of operating at from 450 million to 1.5 billion times per second, and was capable of processing 32 separate bits of data at once. Microprocessors with faster speeds and higher capacities were under development. These developments have changed both the speeds at which data can be processed by equipment such as computers and switching equipment and the speeds at which it can be transmitted, especially using wireless and fibre-optic media. This in turn has dramatically increased the complexity of tasks which can be handled in reasonable lengths of time. Underlying most speed developments has been the increasing miniaturisation of micro-circuitry. This increases the complexity of the circuitry which can be etched into a single IC (integrated circuit) "chip", and reduces the length of time taken for electrical signals to travel from one part of the chip to another. Increasing complexity in turn allows for parallel processing, in which the chip splits a task into segments and performs more than one segment at the same time.

- **Increases in storage capacity.** Faced with demands on capacity, the technologies have become more accurate at processing and recording data, which in turn permits data to be transmitted faster and in parallel streams. They have also succeeded in storing data in ever-smaller spaces, expanding the storage capacity of devices such as floppy-disks and hard drive disks. In 1990, personal computers were capable of storing 1-2 megabytes, whereas in 2002, memory-chips (devised primarily for digital cameras) of 250MB were common and capacities in excess of 1GB were available.[1] Data-storage has also become less expensive: a single, disposable compact disk capable of storing in excess of 700MB costs less than $1.

- **Increases in software complexity**. Relying on faster computers and designs which allow parallel processing, individual software applications have been integrated into more complex suites, and the range of tasks they are capable of performing has increased. New applications, such as sophisticated encryption programs, and applications which process very large data-files, such as those playing digital motion-pictures and music/audio files have become feasible. One effect of this is that newer software outstrips the capabilities of older equipment, forcing regular upgrades or replacement to increase capacity. Data produced by newer technologies tend to include more information, but also take up greater storage space.

Range and types of criminal offences linked to technological development

A wide range of criminal behaviour can be influenced or affected in some way by information and communications technologies. These relationships are still expanding and evolving as the technologies themselves evolve and as new criminal opportunities are created and explored by offenders. A number of different classifications have been proposed, depending on characteristics such as the nature of offenders or victims, motivations of offenders and degree of novelty with respect to established crimes or offending patterns. Generally, types or groups of crime within these categories are known as computer crime, computer-related crime, or cybercrime. A related category, telecommunications-related crime, has become increasingly difficult to distinguish as the underlying technologies converge.

a. Classification based on the role or use of technologies

The most commonly encountered classification is based on whether the technologies are themselves a target of offenders, or whether they are merely used as an instrument to commit other crimes.[2] Crimes where the technologies are used as instruments are sometimes further divided depending on the extent to which the technologies are used. For example, offences such as "hacking", computer sabotage or vandalism, the creation or intentional propagation of viruses and other hostile programs target computer networks and their users, whereas offences such as electronic fraud or the dissemination of child-

[1] One recent problem encountered by investigators has been large capacity data-storage devices small enough to be easily concealed or disposed of to avoid seizure. Devices as small as 25x25x3mm – about the size of a postage-stamp – can now hold as much as one gigabyte, the equivalent of about 2,000 average photographs or 2,000 formatted copies of this article. These are being used by paedophiles to transport child-pornography and by organised crime groups to store business records. See: Seyfer, J., "Criminals' new trick: Child-Porn Collectors Using Pocket-Size Storage Drives", http://www.bayarea.com/mld/mercurynews/news/local/5966920.htm, visited 30-05-03.

[2] See, for example, Charney, 1996, p. 932-34, Goodman and Brenner 2002, part "A", Council of Europe 2000, pp.12-13 and UN-CICP, 2001, Part II C. O'Neill, 2000 (pp.243-50), for example, includes computers as subjects, objects and instrumentalities of crime.

pornography involve the use of technologies as an instrument for criminal purposes. A third sub-category includes cases where the technologies were not directly instrumental in the crime, but played some other role. This includes cases in which computers were not used, but were later found to contain evidence, either because they were used for supportive purposes such as communications or concealment, or because evidence was recorded automatically or by persons not involved in the offence itself.

Further sub-categories could also be developed based on the exact role played by the technologies in particular types of criminal activity. In the case of fraud, for example, the Internet has been used as the principal instrument of the offence (e.g., the advertising of non-existent merchandise for sale or auction), in more peripheral ways (e.g., the use of fake web-sites to bolster the credibility of frauds committed face-to-face or using other media), or as the means of securing payment or laundering funds in frauds not otherwise linked to the technology. Similarly, in smuggling or trafficking crimes, the technologies may themselves be the instrument whereby contraband such as digital child-pornography is created and/or trafficked, or they may play a less direct role, such as providing secure communications for offenders or a conduit for the concealment and transfer of proceeds.

Generally, any involvement of information and communications technologies, however remote, involves in some way the common basic functions of the technologies in transmitting, receiving and storing information. These tend to be a mixed blessing for crime-control interests. On one hand, electronic information and evidence are created and stored in ways which were not previously possible, creating opportunities for investigators and prosecutors. On the other, the technologies sometimes are used to conceal evidence, or to produce vast quantities of data within which incriminating evidence may be concealed, and to displace existing offending practices into environments or jurisdictions where investigation and prosecution are more difficult. For this reason, a series of technical and legal questions relating to the gathering and use of electronic evidence have emerged as major issues in both domestic and international fora, as law-enforcement and security agencies seek to maximise their advantages and minimise and compensate for disadvantages.[1] These also involve other critical issues, notably those of privacy and other human rights, which have been thrown into a state of flux by the rapid development of the technologies.[2]

b. Classification based on novelty

A second common distinction is made between crimes which are new and essentially created by the technologies and crimes which existed before but have been modified or influenced in some way by the technologies. In most cases of modification, the effect of the technologies can be seen either in changes in the actual *modus operandi* of offenders or in increased occurrence rates, as potential offender gains are increased, risks are reduced, or both, although in some cases offence rates have fallen as technology-related risks to offenders increased and this became public knowledge.[3]

[1] See generally Charney, 1996 and Goldstone and Shave, 1999.

[2] The debate between privacy and security interests is discussed further in the segment dealing with the smuggling of encryption applications, below. See also Goldstone 1999.

[3] The general trend appears to have been to increases in technology-related crimes, but there are examples of cases in which rates have fallen, particularly as technologies increase risks. The use of telephones to make obscene or harassing calls or bomb threats, fire-alarms and crime reports dropped sharply in many places when computerised telephone switches automated tracing and caller-identification, for example, although some of this offending was displaced into e-mail and similar media, which afford a similar measure of anonymity for the senders of such e-mail. See McGraw 1995.

In practical terms, this basis for classification tends to produce the same general groups of offences as the previous one: truly novel offences tend to be those which also target the technologies and victims through their use of technologies, while offences which target victims for other reasons ranging from harassment to economic motives generally existed in some form previously. Some of these show ongoing evolution in parallel to technological change. Criminal harassment or uttering threats, for example, has shifted from the use of written notes to telephone calls to e-mail, but the basic elements of the offence remain the same.

Novelty itself can be assessed by objective standards, but it also depends to some degree on the perspective of the person assessing it and what is new to one person may be less so to others.[1] Many technology-related crimes exploit opportunities created by gaps between opportunity factors and control factors. These tend to follow cycles which start when technological change creates new opportunities in the form of new offender techniques which offer higher potential (material or other) gains, lower risks, or both. Related offending increases as offenders exploit the opportunity, but provokes a series of reactions which increase control factors in response to the problem. Technical reactions, such as improvements to anti-virus products or the distribution of "patches" to close security gaps in software, can be quite rapid, particularly in recent years, as security support has become a major marketing factor for hardware, software and service providers. Legal and social reactions tend to take longer: laws may require amendment, law enforcement agencies must develop new techniques and expertise, while potential victims become aware of the risks over rather protracted periods of time. As controls increase risks and reduce potential benefits offending is prevented, deterred, or in many cases displaced into areas where newer opportunity gaps have opened up. The speed with which the technologies and resulting criminal opportunities are evolving is a critical characteristic in understanding crime in this area.

Elements of novelty can be found in both completely new and pre-existing crimes and the same cyclical patterns are likely to be present to some degree with both types, which suggests that novelty itself may be seen more as a matter of degree than an absolute basis for classification. The same patterns also tend to appear, with some variations, regardless of the motivations of offenders. Those who commit novel offences involving hacking, electronic intrusion, computer viruses and similar elements have tended to be motivated by non-monetary incentives such as thrill-seeking, whereas those who commit more traditional crimes tend to be motivated by economic or material goals.

Neither category of motivation is in itself novel,[2] but technological change creates new opportunities to pursue the motivation in both cases. Hackers, like mountain-climbers, derive satisfaction from gaining access to places inaccessible to less-skilled individuals, especially if they are the first to do so. Where climbers plant flags, many hackers post notices or leave evidence to draw attention to their accomplishments. Once a particular technology has been hacked, the most dangerous and sophisticated offenders tend to move on in search of ever more difficult challenges. In the case of economic crimes, on the other hand, it is the opportunity gaps created by new developments which are exploited. New users of technologies are vulnerable to offenders with more experience, while offenders who encounter technical or other control factors in one region may be displaced into other

[1] Newcomers to the Internet are often victimised by crimes such as password and identity-theft because they do not yet appreciate the sensitivity of personal information on-line. In such cases the offence may be "novel" to the victim but not to the offender.
[2] Grabowski, 2001, at pp.36-7.

regions where such impediment have not yet developed.[1] Many securities frauds, for example, rely on new communication technologies to disseminate false information in order to manipulate prices to the advantage of offenders. Victims are deceived, in part, because they are not yet aware of how easily false information can be posted on-line, often using websites which appear legitimate or even to impersonate known and trusted information sources.

Most experts agree that the vast majority of criminal behaviour being observed currently involves pre-existing offences rather than novel ones. There is also some suggestion that the trend is for novel offences to diminish in proportion to overall offending, if not in absolute numbers. There may be some reduction, or at least levelling-off of rates for offences such as hacking and computer virus attacks as the novelty wears off and as technologies and their users develop and adopt security and crime-prevention techniques. The constant evolution of the technologies themselves will limit any such trend, however, by ensuring that new opportunities and challenges to offenders are constantly being created. The pattern of more traditional offences which use the technologies as instruments, on the other hand, suggests that this category is likely to expand for the foreseeable future, as the offences themselves appeal to a broader range of potential offenders, many of whom are still taking up or gaining access to the technologies and criminal techniques, and many new criminal opportunities remain to be fully exploited.

The use of novelty as a basis for classification also represents a problem in that offences gradually become less novel and are replaced by others, and by offences which incorporate additional elements. This is illustrated by various forms of hacking or gaining unauthorised access to computer systems, which originated primarily as a means of thrill- or status-seeking, but which has now become an instrument for more prosaic (and lucrative) criminal purposes.[2] Recent developments have seen hacking skills used for offences such as commercial espionage, and the theft of credit card data or digital identities for use in fraud, extortion and other economic offences.

c. Classification based on offender motivation: economic and terrorist crimes

Classification by offender motivation can potentially generate as many categories as there are motivations. However, for the purposes of this paper, two major categories will be considered: offences motivated by economic gain, and offences associated with social, political or terrorist motives.

In many new crimes, such as hacking and the creation or propagation of hostile computer programs such as viruses, offenders have thus far tended to be motivated by non-material factors as mentioned earlier, while more traditional crimes such as frauds have tended to be more materialistic. For the same reasons set out in the previous segment, the motivations of offenders shift over time and new motivations become associated with established offences.

[1] The latter scenario may become particularly problematic in relation to the efforts of developing countries to close what has been described as the "digital divide". There is at least the potential for still-developing systems to be attacked by offenders from more developed countries where such attacks have become excessively risky or technically impossible. With economic crimes, on the other hand, the potential is for offenders in developing countries to target victims in more affluent ones. This pattern has already been seen with West-African "419" advance-fee frauds, which began with letters, progressed to fax machines and now exploit e-mail, and which primarily target victims in the United States and other developed, English-speaking countries.

[2] See, for example Sullivan, B. "The year the criminals took over", MSNBC News, 31 December 2002, http://www.msnbc.com/news/849801.asp (visited 2/1/03). Reviewing 2002 stories, Sullivan notes a decline in crimes such as virus attacks and general hacking and a shift towards on-line frauds and other economic crimes.

In some other offences, the non-material and material factors often co-exist. One example is the dissemination or trafficking in child-pornography, where some offenders are paedophiles motivated by sexual gratification and others are simply trafficking in a commodity for profit. This can be an important distinction for both researchers and investigators, since it is likely to determine behaviour and which other offences, if any, the offender may have been involved in committing. More detailed typologies are often useful for specific research and the development of legislation and training materials, but also have some limitations. Some offences may fall into more than one category or move from one to another as technologies, offender motivation or other definitional characteristics evolve.

One of the more problematic categories of offending associated with information and communications technologies is that of terrorism. Terrorism has proven difficult to define both for political and substantive reasons.[1] Given the difficulty in defining terrorism based on the objective nature of the actions involved, efforts have been made to define or describe it based on the subjective intentions of offenders, or on the subjective or objective perception of or reaction to offences by the populations in which they occur.

The difficulties encountered and the ongoing efforts to overcome these notwithstanding, it would be helpful to keep in mind that the use of technologies by terrorists (or organised criminal groups for that matter) parallels that of legitimate users and reflects much the same range of uses which the technologies were designed to support. The actual uses of technologies are often not criminal or illegal, and it may be both legally and technically difficult to distinguish between terrorist, criminal and legitimate uses in many cases. Encryption products, for example, are used by terrorists to conceal identities and message content, which is precisely the purpose of the technology and exactly how legitimate individual and corporate users employ it. This fact has significant implications both for attempts to regulate or restrict the technology and for attempts to distinguish between terrorist and other uses for purposes of detection and investigation, and for research.

Nevertheless, the potential for misuse of information and communications technologies for terrorist purposes is considerable, and this fact has made the consideration of cyber-terrorism a major issue in strategies for the prevention of terrorism in two major areas; the possibility of the technologies themselves being attacked, and the possibility of these technologies being used in support of terrorist activities. There have been a few incidents in which technologies themselves have been attacked, but available research results indicate that at present the concerns in this area remain largely theoretical. The use of technologies by terrorists to plan, organise and communicate, on the other hand, is well-documented, and probably fairly well understood, at least to the point where counter-terrorism agencies have identified and traced high-tech media such as cellular and satellite telephones and Internet-based communications. However, it should be noted that at present these are indications that some terrorist groups may be returning to the use of face-to-face meetings since the risks associated with various forms of physical surveillance are perceived to be less than those of electronic surveillance.[2]

[1] Within the United Nations, an Ad Hoc Committee established by the U.N. General Assembly in its resolution 51/210 in December 1996 has made substantial progress towards a comprehensive international treaty against terrorism, but has not resolved several definitional issues. See U.N. doc. A/AC.252/2002/CRP.1/Add.1. A summary can be found in UN Progress Release L/2993, available on-line at www.un.org. Discussions within other multilateral settings have encountered similar problems.

[2] Terrorist usage of wireless communications of all kinds, including terrestrial cellular telephones and satellite-based systems, is believed to have declined since the 2001 attacks due to the belief that these can be identified, located and targeted by military or security forces. Successful targeting using communications media precedes the 2001 attacks, however. In April 1996, Chechen rebel leader Dzokhar Dudayev was killed by a Russian air-strike believed to have been directed at his satellite telephone, and Israeli security services are believed to have used the interception of conventional cellular telephone signals to target Palestinian militants in a number of incidents.

Terrorist groups use global telephone, e-mail and Internet applications to communicate, in many cases without being observed or identified simply because of the enormous volume of data flowing in such systems.[1] Even where specific e-mail messages, such as those sent in connection with the January 2002 kidnapping and murder of *Wall Street Journal* reporter Daniel Pearl, can be identified, tracing them to a physical source can be difficult, particularly if they have been sent from a public facility such as an Internet café. Terrorists also use digital security applications in the same way as conventional offenders and legitimate users. Encryption has been used to protect digital information stored or transmitted by known or suspected terrorists, including Ramsi Yousef, convicted of involvement in the 1993 World Trade Centre attacks and Zacarias Moussaoui, accused of involvement in the September 11 attacks. Encrypted data has also been recovered from Al Qaeda sites since their ouster from Afghanistan. Direct-to-satellite telephones have also been used to communicate from remote locations,[2] and portable Global Positioning System units are believed to have been used by at least some of the aircraft hijackers to attack the targets in New York and Washington on 11 September 2001.[3]

Some direct terrorist attacks on Information and Communications Technologies (ICTs) have occurred,[4] and other incidents in which harm has resulted from unintentional actions or attacks by non-terrorist groups suggest that significant harm could be caused by a serious and well-prepared electronic assault in what is described as "asymmetrical warfare".[5] Recent military engagements have all been accompanied by increases in on-line hacking and sabotage activities, both on the part of the States involved, and an assortment of protestors, activists and ad-hoc ideologies on all sides,[6] and ongoing conflicts in the real

---

More recently, on 5 November 2002, a vehicle in rural Yemen containing suspected Al Qaeda members was attacked by a drone-launched missile believed to be operated by the US Central Intelligence Agency, based on targeting information from a satellite-telephone one of them had been using. See "Death of terror chief deals severe blow to Al Qaeda", Times on-line, 5 November 2002, http://www.timesonline.co.uk/article/0,,4281-470189,00.html. One media report indicates that Osama Bin Laden stopped using his satellite telephone following heightened surveillance after the August 1998 attacks on two US Embassies in Africa. See Fielding, N. and Gadhery, D., "Al-Qaeda's Satellite Phone Records Revealed", Sunday Times, 24 March 2002.

[1] See, for example Delio, M., "Al Qaeda Website Refuses to Die", http://www.wired.com/news/infostructure/0,1377,58356,00.html, visited 20-04-03. Delio describes the ongoing efforts of a site believed to represent Al Qaeda to maintain operations while government authorities and Internet service providers shut it down. The site is moved by pro-Al Qaeda hackers, who illegally imbed it into legitimate sites. It contains political information supporting Al Qaeda's cause, and may also contain coded messages to operatives, who are told of its present location using electronic bulletin-boards and mailing lists.

[2] The use of satellite telephones by the Angolan UNITA leader, Jonas Savimbi to trade in conflict diamonds and arms is discussed below. Al Qaeda has also made use of satellite telephones, particularly while in Afghanistan, Pakistan and other remote regions. See Corbin, 2002, p.65 and 278-79. Media reports and court documents suggest that Osama Bin Laden used at least two different satellite telephones, and that these were subsequently used to link him with various associates and with several attacks associated with Al Qaeda. See Caruso 2001, Financial Times, "Bin Laden's Martyrs for the Cause" 28 November 2001, on-line at:
http://specials.ft.com/attackonterrorism/FT3IOXWHLUC.html; Morris, M., "Jihad phone linked to former Missouri student", Kansas City Star, 19 September 2001, on-line at: http://www.kcstar.com/item/pages/home.pat,local/3accfd88.919,.html; and Burke, J., "Bin Laden still alive, reveals spy satellite", The Observer, 6 October 2002, on-line at:
http://www.observer.co.uk/afghanistan/story/0,1501,805676,00.html.

[3] See Corbin, 2002, at pp.224-25 and 230. The leader of the hijackers, Mohammed Atta, was in New York on the day before the attacks, and is believed to have visited the World Trade Centre, possibly for the purpose of allowing his GPS unit to record the destination coordinates for the attack flight.

[4] Examples include attacks linked to ongoing internal conflicts involving Spain (ETA), Sri Lanka (Tamil Tigers) and the 1999 Kosovo conflict. See Denning, 1999.

[5] For example, U.S. sites such as those representing the White House and Pentagon are the targets of large volumes of (for the most part) unsophisticated attacks. Pentagon computers are attacked, on average, several times per day. See "Hackers target Pentagon Computers", CNN, 5 March 1999, http://www.cnn.com/US/9903/05/pentagon.hackers/, and Poulsen, K. "Pentagon computers attacked 715 times last year", Security Focus On-Line, 5 April 2001, http://online.securityfocus.com/news/188. See also Marcus 2001 at pp.204-05. In April 2001, officials from the FBI National Infrastructure Protection Centre reported only 102 open cases for the entire US Government, but indicated that many of them were single investigations into large numbers of multiple attacks suspected or believed to have been committed by single offenders or groups. The NIPC evidence also illustrates the range of attacks and levels of sophistication, which range from crude attacks by thrill-seekers or individuals protesting US policies to more sophisticated attacks by "foreign powers", presumably seeking information or probing security defences. See Dick 2001.

[6] Denning, 1999, includes several examples of protestors using cyber-attacks as a substitute for physical participation in demonstrations, including one case in which anti-globalism protesters unable to attend a G8 meeting held on 18 June 1999 in Germany responded to calls to hold local demonstrations and launched over 10,000 individual cyber-attacks in a 5-hour period. In the context of possible armed conflict in Iraq, US authorities prepared for increases in attacks on military and government computer networks, not only from Iraq itself, but from others seeking to protest or impede any military action. See Lichtblau, E., "Iraqi computer attacks feared", New York Times, 16

world now usually have a parallel conflict on-line.[1] The vast majority of on-line activity consists of political debate, or at worst, propaganda and counter-propaganda, but terrorist communications are clearly also occurring. Pro-Israeli sources have accused Hamas of operating a website containing information about how to make explosive devices, although this could not be substantiated at the time of writing.[2]

A related area of concern which falls between direct attacks and indirect applications has been the potential for the use of ICTs to perpetrate attacks carried out by other means. Obvious military examples of this, such as re-programming or jamming computerised weapons systems to miss targets or strike targets other than those originally programmed are the subject of extensive technical precautions, but more subtle variations have occurred with respect to propaganda and dis-information. One recent example consisted of "spoofing attacks" in which fake e-mails containing prejudicial information are sent by spoofers with fake return addresses in order to discredit the alleged sender.[3] Other possibilities include the use of ICTs to provoke some physical reaction which might then be used as a diversion or part of a terrorist attack.[4]

Clearly, the dependence of critical infrastructure elements on ICTs and the increasing linkage of such elements with each other and with open or relatively insecure computer networks raises some cause for concern that they may be disrupted, but most of the concern at present seems to involve threats to economic and social structures, with threats of death or injury mostly of an incidental nature.[5] The potential economic harm resulting from electronic terrorist attacks or from physical attacks on information or communications systems is substantial, however,[6] and the extent and complexity of infrastructure systems as potential terrorist targets will require ongoing reassessment.

January 2002, and "NIPC Encourages Heightened Cyber-Security as Iraq-US Tensions Increase", US National Infrastructure Protection Centre, http://www.nipc.gov/warnings/advisories/2003/03-002.htm. Once the conflict started, the predicted upsurge actually occurred, both on the part of assorted anti-war activists and on the part of those favouring the United States; see Anti-war hacking rises sharply", BBC News 26 March 2003, http://news.bbc.co.uk. Most were probably carried out by individuals, but some bore the hallmark of either State-based organisations or extremely sophisticated and well-resourced individuals. One major attack on the site of the Arabic-language news service Al Jazeera blocked access to it for several days, provoking complaints about the freedom of expression and the strategic wisdom of such action, and prompting U.S. authorities to issue a public caution that so-called "patriotic hacking" was still a crime under United States law and might be counter-productive. See "Arab Web Sites Plagued by Attacks", Associated Press, 17 April 2003, http://abcnews.go.com/wire/Business/ap20030417_163.html; "Hack attack on Al-Jazeera raises questions", USA Today on-line, April 30 2003, http://www.usatoday.com/tech/world/iraq/2003-03-30-iraq-web_x.htm; and "US hackers told to leave Iraq alone", BBC News on-line, http://news.bbc.co.uk/2/hi/technology/2760899.stm.

[1] Searching the term "Hamas", for example generates a mix of pro-Palestinian and pro-Israeli web-pages, including several maintained by the Israeli Foreign Ministry and families of Israeli bombing victims. The address www.hamas.org has been registered, presumably to block its use by Hamas itself. A similar duel continues between the unionists and republican factions in Northern Ireland: see "DUP winning cyberspace battle by a landslide", http://www.dup.org.uk/press.html. The other major unionist parties are all active on-line, as is Sinn Fein and the major Irish Republican newspaper, *An Phoblacht* .

[2] See the discussion of dangerous content, below, for details.

[3] This has been a tactic used by pro-Israeli and pro-Palestinian activists, each sending e-mails purporting to be from the other, containing what appear to be scandalous, blasphemous or incriminating information. Essentially, the attacks are carried out by sending e-mails on which the original message header sender address is replaced with that of the victim. This is not considered hacking and may not be a criminal offence in some jurisdictions, although other offences such as impersonation or electronic forgery may apply. See: "Fake hate e-mails mar activists' reputations", CNN on-line, 22 April 2003, http://www.cnn.com/2003/TECH/internet/04/21/hate.email.ap/index.html.

[4] See Schwartz, J., "Cyber-attacks with Offline Damage", New York Times, 14 April 2003, and Byers, *et al*., 2003. The authors discuss tactics such as the physical equivalent of denial-of-service attacks. In one example, a US-based spammer who publicly admitted his occupation was subsequently deluged with thousands of catalogues and mail-order products ordered in his name by users of a technophile website after his name and address were published there. The essence of such attacks is that the actual attack is physical, but inspired or activated in some way by the use of ICTs. In the context of terrorism, such tactics could be used for simple harassment or to overwhelm surveillance or control systems to mask a more serious attack.

[5] Of the eight areas of critical infrastructure identified for protection by the U.S. Government in 1996, only three (electrical supply, water supply and emergency services) would appear to have significant potential for deaths or injuries if disrupted. Others, such as transportation systems have specific elements (such as aviation security) which raise such issues. See Executive Order 13010, US Federal Register Vol.61 No.138, pp.37347-50, 17 July 1996. For a pragmatic threat assessment, see Lemos, 2002, arguing that while some threat to safety exists, most truly critical systems are either beyond the reach of potential terrorists or would cause primarily economic harm if significantly disrupted.

[6] See Junnakar 2002 for an assessment of the damage caused to New York-based information and communication infrastructure by the attacks of 11 September 2001 and the subsequent efforts of companies who deliver or depend on services to decentralise their systems to reduce the risk in future. This is particularly difficult in New York, where the high density of business operations and infrastructure makes decentralisation and redundancy difficult.

While no major direct attack has yet been attributed to a major known terrorist organisation, such an attack may represent an attractive option for several reasons. From an ideological standpoint, information and communications technologies may be seen as representing western, developed cultural values opposed by fundamentalist groups, or as vehicles for information considered by them to be offensive or blasphemous. The increasing reliance by developed countries on these technologies may also make them attractive targets because of the seriousness of the harm that could result if critical functions were disabled or disrupted. Networked activities may also be attacked simply because they are easily accessible from anywhere in the world, particularly if improved security measures and better intelligence-gathering make it more difficult or risky for terrorists to travel or approach potential targets physically.

The capability of many terrorist organisations to launch cyber-attacks is also likely to increase, as technologies, infrastructure and expertise spread through developing countries, and as a younger generation with the necessary skills is recruited. As with conventional crime, electronic attacks may also be more attractive in some cases because they can be committed by an individual or small group without extensive resources. As with biological viruses, computer viruses and other hostile programs could be used in relative safety by those who have advance warning and can incorporate digital defences analogous to biological vaccination, although the widespread advance preparation for such an attack probably could not be carried out in secrecy and the resulting attack would be neither a surprise nor anonymous.

Apart from the direct threat posed by such attacks, additional concerns arise from the fact that, in a conflict conducted in cyber-space, it can be even more difficult to establish who the combatants actually are than is the case with physical terrorist attacks.[1] One can imagine scenarios in which an attack launched by a terrorist group or even a disgruntled individual might be perceived by one State as an attack by another, provoking an armed response, for example. This parallels the development of more conventional high-tech crime, in which access to the technologies has brought a whole series of offences, especially those of a transnational nature, within the reach of a new class of relatively unsophisticated offenders.[2]

d. Classification based on content

A further basis for classification is to divide computer or communications-related crimes into those which involve the actual substantive content of data and those which do not. The former category can then be further divided based on the nature of the content and the reasons for which it is the subject of criminal offences. For example, crimes relating to intellectual property, commercial espionage and child-pornography are linked to the content of data, and the offences often involve the creation, possession, copying, taking or trafficking in specific types of content. Offences such as attacking or gaining unauthorised access to a computer system are not content-linked. A series of content-related offences can now be found in the laws of many countries, subdivided into "offensive content" crimes,

[1] See Barkham, 2001 at p.58, discussing the use information warfare by non-state actors as a concern with respect to proliferation and the lack of application of international law to such scenarios.

[2] A brief perusal of many of the messages posted by hackers leads one to question their conventional, if not computer-literacy. Once the basic techniques and digital tools are in hand, the more basic cyber-attacks can also be carried out, or at least attempted, without the degree of planning and consideration which would precede the commission of a physical attack of the same nature. One U.S. government site, for example reports, among other incidents, cyber-attacks on a web-site dealing with Afghan dogs in a rash of pro-U.S. hacking incidents following the physical attacks of 11 September 2001. See US-NIPC 2001(1).

such as those involving child pornography and hate-propaganda, and offences in which the content itself is not offensive, but criminal law is used to limit access to it for other reasons. This may be done to protect intellectual property or other economic interests; to prevent or deter its misuse for other reasons, such as the fact that the information is itself dangerous or subversive (hate-propaganda, bomb-making information) or is likely to be used for criminal purposes (offences involving the taking, possession or use of computer passwords, digital "hacking tools", or credit-card information); or because the information is of a personal nature (and thus protected), such that access or taking it constitutes an invasion of privacy.[1]

Seriousness of high-technology and computer-related crime

There is widespread consensus on three basic points. Most experts agree that the problem is rapidly increasing in scope and seriousness, as well as in the magnitude of financial and other costs involved. However, there is also consensus that there are no forensically reliable, global statistics to conclusively establish this trend or accurately quantify the harm caused. Finally, there is widespread agreement that incidents are seriously under-reported, by as much as 90%.[2] The evidence that exists consists of anecdotal of occurrences, the opinions of officials who deal with criminal and other cases, and, as a relatively recent development, data gathered from law enforcement agencies and facilities such as on-line reporting sites where victims can report ICT-related crime. There are some sampling and other methodological problems, but these are not insurmountable, and the sites will eventually generate sufficient data to establish and quantify trends over time.

In 1986, in what was probably the first significant analysis of computer-related crime, Prof. Ulrich Sieber found both relatively low levels of crime and little credible information. In reviewing the available evidence and methodological concerns, he concluded that:[3]

> "…it can be stated that the number of perfectly verifiable computer crimes in all reliable empirical studies is not very large…"

A decade later, in 1996, authors spoke of annual losses in the USA alone of $5 billion in 1991, and in 1996, $10 billion in the USA and £5 billion in the U.K.[4] The escalating seriousness of individual offences in both reality and popular perception is also illustrated by the frequency of references to major cases such as the "Cuckoo's Egg", "Legion of Doom", the criminal cases of Kevin Mitnick and the teenage hacker known as "Mafiaboy", and the 2001 virus attacks "Melissa", and "I Love You" in both academic and mass-media. In 2002, one author described the "I Love You"(a.k.a., "Love Bug") virus as having spread globally within 2 hours of first detection infecting the computers of 45 million users in at

[1] Some of these, such as the possession or dissemination of hacking tools or information, illustrate the indistinct nature of the boundary of what might be considered as "content". Most experts would see data which was used by criminals, such as child-pornography, lists of credit-card numbers, or written information useful for crimes, such as recipes for making explosives or instructions on how to hack into computer systems as content. Actual hacking tools, which consist of programs which can be downloaded and used directly for hacking, on the other hand, would not, and the classification of data such as computer passwords or credit-card numbers might depend on how they were used.

[2] The available statistics and major methodological concerns and reasons for under-reporting are discussed in UN-CICP, 2001, Part D. See also Charney 1996 at pp. 935-39, Goodman and Brenner, 2002 Part "C" (pp.9-12), Goldstone and Shave, 1999, and Grabowski 2001, at pp.37-38 (increases in technologies) and 46 (efforts to assess scope of evolving problem).

[3] Sieber, 1986, chapt.III, p.29. In his discussion, Prof. Sieber notes that the lack of authoritative data makes it impossible to form any strict conclusion about crime levels not qualified as in the quoted statement.

[4] Charney, 1996 at pp.936-37 and sources there cited.

least 20 countries and causing an estimated $2-20 billion dollars in damage.[1] Media reports often exaggerate the seriousness of occurrences or demonise offenders, but many of the offences are clearly of a very serious nature in economic terms, including as a threat to the viability of the technologies.

Given what is known about the rapid development and proliferation of information and communications technologies, and the links between those technologies and the new or expanded criminal opportunities they create, it would be surprising if the overall picture were not one of rapid, if not exponential, increase. The Report of the Secretary General to the 10th session of the UN Commission on Crime Prevention and Criminal Justice described the situation as follows.[2]

> As computer and telecommunications networks have expanded in scope and sophistication, the number of people who use them and the degree of reliance placed on them, have both increased dramatically. In March of 2000, the Secretary General reported to the Millennium Assembly of the United Nations that from a start in the early 1990s, the Internet had 143 million users by 1998, and that 700 million were expected to be "on line" by 2001. Electronic commerce, a more recent phenomenon, reached a total of $2.6 billion by 1996, and was expected to top $300 billion by 2002. There are few comprehensive statistics concerning high-technology or computer-related crime, but anecdotal evidence and such statistics as are available suggest that such crime is increasing in its extent as the numbers of potential offenders and victims "on line" increase. The range of criminal activities also appears to be expanding as technologies create new criminal opportunities and offenders find new ways to exploit them.

Too little is known about the misuse of technologies in various forms of smuggling and trafficking to permit any authoritative conclusions about levels or trends in offending, but the same trends are likely to be present for these crimes as for other crimes in which the technologies are used as an instrument for material gain.[3] As new technologies are developed, offenders are likely to use them to facilitate ongoing activities such as drug-trafficking, and in some cases new activities may be undertaken in areas where they become possible or less risky as a result of new opportunities created.

ICT-related crime also presents methodological challenges to those gathering, compiling and analysing information. Statistical information which specifically identifies ICT-related crime is more likely to be forthcoming in areas such as the theft/trafficking of intellectual property, child-pornography and other intangible commodities than for the smuggling and trafficking of human beings and tangible commodities such as narcotics or firearms. In the former areas, electronic smuggling or trafficking represents a new type of offence or a major shift in offender behaviour directly associated with the technology, leading to the compilation of discrete statistical information. In the latter categories, statistics tend to track the total numbers of incidents, but are less likely to classify or quantify cases according to whether technologies were used or how. Fraud statistics, for example, might eventually be classified based on the involvement of technologies, but this is not being done at present.

[1] Goodman and Brenner, 2002, Introduction. See also UN-CICP 2001 at paras.31-32, discussing the various types of costs incurred by the virus and difficulties in quantification. Sources cited there reflect a range of estimates from $7-10 billion worldwide.

[2] UN-CICP, 2001, para.30. Statistics are based on the Report of the Secretary General to the Millennium Assembly of the United Nations, A/54/2000, paragraph 152 and on Grabowski 2001 at p.40.

[3] The same patterns and trends may not apply to offences such as harassment and some unauthorised access cases, which are often attributed to motivations of a non-economic nature, such as thrill-seeking or status-seeking.

The new technologies can also be used to report crime or gather data, which will provide raw information, but will also raise sampling, classification and other issues. US law enforcement agencies in particular have recently begun using on-line tip sites to allow informants or complainants to report crimes ranging from child-abuse to terrorism.[1] One relevant example is electronic fraud, which appears to be rapidly increasing as offenders adapt to the new technologies and larger numbers of potential victims go on-line. A new on-line reporting system operated jointly by the FBI and National White-Collar Crime Centre, which is dedicated specifically to fraud reporting, allows complainants to choose from a menu of 14 categories of fraud, but these are not mutually-exclusive and rely on victims as the basis of classification.

Any data generated in this way would also have to be adjusted to account for the fact that not all victims have Internet access or are equally likely to use it, inflating reporting rates from regions, occupations or other groups who do in comparison to the general population. The soliciting of on-line tips also makes reporting crime easier, which is likely to increase reporting rates independent of any actual increase in crime. Data generated by the site and other sources is reported annually and shows a tripling of both occurrences and economic losses between the 2001 and 2002 calendar years.[2] This probably reflects both an actual increase in crime and an increase in the percentage of crimes reported, but these cannot be separated, which will make the calculation of actual offending rates and trends difficult until the effects of the new means of reporting are more clearly understood.

Public and private sector roles in controlling high-technology and computer-related crime

(i) Importance of private-sector involvement

Unlike the physical environments in which crimes are committed, investigated and prosecuted, the electronic environment, sometimes described as "cyberspace"[3] is largely designed, constructed and controlled by non-governmental entities. This means that the implementation of many measures to prevent crime and to facilitate its detection, investigation and prosecution, which are commonly accepted in the physical environment, cannot be so easily deployed in cyberspace. Even the basic infrastructures which support wireline and wireless telephone services have increased in complexity to the point where even the most basic wiretapping can no longer be done directly by law-enforcement. The assistance of technicians employed by service-providers has become essential, raising issues of cost and confidentiality.

Hardware and software are developed for profit, incorporating characteristics which will make them attractive to users, and until relatively recently, security and crime-control elements have not been a high priority.[4] Many technical features, such as high-speeds, large volume capacities, remote access and privacy products have tended to either favour crime over crime-control or, at best, be relatively neutral. Features which facilitate the detection

[1] See: https://tips.fbi.gov/ (general FBI tip site) and http://www1.ifccfbi.gov/index.asp (FBI/NW3C fraud site).
[2] See IFCC Annual Report for 2002, at: http://www1.ifccfbi.gov/strategy/statistics.asp, and Rusch, J., "The rising tide of Internet Fraud" (discussing methodological issues), at: http://www.usdoj.gov/criminal/cybercrime/usamay2001_1.htm.
[3] The term was originally used by science-fiction author William Gibson in the first "cyberpunk" novel, *Neuromancer* in 1984.
[4] This may be changing. A series of incidents involving viruses and other digital mayhem during 2001 provoked Microsoft, whose technologies and customers have been victimised, to begin 2002 with a public pledge to assign security features a higher priority and make them a part of marketing strategies. See, for example BBC News, "Microsoft to tackle security failings", 17 January 2002, http://news.bbc.co.uk/2/hi/science/nature/1766061.stm and Microsoft report: "The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress", http://www.microsoft.com/presspass/features /2003/Jan03/01-15twcanniversary.asp. Generally, offenders tend to seek out and target the vulnerabilities of the largest producers, and especially Microsoft, because these products are most widely used, increasing the impact of criminal conduct.

and investigation of crime often involve the retention and accessing of data, which raises privacy concerns and fears that technologies into which they are incorporated will be uncompetitive or less profitable. The highly-competitive and multinational nature of high-technology development has also placed it largely beyond the grasp of regulatory controls in any one country, because controls imposed country-by-country make those subject to requirements less able to compete than those who are not, particularly if added costs or loss of customer privacy protection are involved.

The transnational nature of computer networks also curbs the effective use of investigative measures and generally complicates other crime-control efforts. On-line searches, for example, raise issues with respect to national sovereignty, legal requirements for official mutual legal assistance requests, and practical concerns about the need to coordinate law enforcement efforts.[1] More generally, existing practices for international harmonisation and cooperation in criminal matters require expansion and adaptation to deal with new forms of crime and investigative measures which, with one notable exception, have not been forthcoming thus far.[2]

These factors have made it apparent that the private sector will have to have a larger role to play in dealing with ICT-related crime than it has had with crime in physical environments. In areas where crime-control is profitable, private-sector involvement has proliferated. Faced with the erosion of some State-based protections, ICT users have turned to technical measures such as firewall, encryption, anti-virus and other security applications. Manufacturers and service-providers have provided these whenever it proved either necessary to protect existing sales and profits or a profitable business in its own right, but crime-control measures that do not meet these criteria have not been deployed.

One example is the need for service-providers to retain traffic data associated with messages in case these must be traced later in an investigation. The retention of such data supports crime-control, but it costs money and affects subscriber privacy, which can hurt sales if other providers are offering more favourable terms. Against the direct and immediate costs, service-providers must also weigh indirect costs such as the deterrence of customers afraid of on-line crime and the potentially higher costs of cooperative measures imposed by legislatures or the courts. Both governments and the industry have sought to cooperate in implementing voluntary data-retention requirements in the hope of balancing all of these interests, and periods of voluntary data-retention were considered in meetings between G8 members and the private sector in 2000 (Paris) and 2001 (Tokyo).[3]

One way of addressing this problem would be to establish agreed measures and a globally-coordinated strategy to develop effective measures. Views differ about whether standards should be imposed by legislation or established by voluntary means, and it seems likely that any successful strategy would ultimately have to involve elements of both. Voluntary standards of compliance raise the prospect of a single company opting out, either for competitive advantage or because it is owned, operated or influenced by organized crime. At the same time, the nature and scope of the effort required of the private sector

[1] For a practical examination of issues relating to cross-border search and seizure and other investigative techniques, see UNAFEI 2001. See also Charney 1996 and Sussmann 2000.

[2] European Convention against Cybercrime, ETS No. 185, adopted Budapest, 23 November 2001. In addition to the countries of Europe, Canada, Japan, South Africa and the United States participated in drafting the treaty and are expected to become States Parties. The Council of Europe has invited other non-European countries to join as well, provided basic legal and human rights standards are met.

[3] Discussions in the G-8 "Lyon Group" and between G-8 members and companies have included consideration of a voluntary minimum 28 day period for the retention of traffic data, although some countries maintain longer periods. The USA, for example, requires retention for 180 days. See Sussmann 2000 at pp.468-69.

and the fact that effective crime-control, taken strategically, is also generally good business argue for a substantial degree of voluntary cooperation.[1]

Regardless of the mix of imposed and voluntary standards, the basic establishment of common standards for crime control measures would increase the ability of commercial companies to implement otherwise-unprofitable measures, while still preserving a competitive position. Such a strategy would also have to take into account the differing views and needs of developed and developing countries, as the collaboration of all countries will be needed to avoid jurisdictional gaps or "data havens" which can be exploited by offenders.

Reaching a global consensus on the control of ICT-related crime is likely to require a tripartite bargain in which the basic needs of developed countries, developing countries and the private sector are all addressed and balanced. The private sector would be called upon to implement crime-control measures in designing and marketing hardware, software and services, and to assist State agencies with investigative measures. In return it would gain a healthier environment in which to conduct business, fair competition, and security against unduly harsh regulatory standards and standards which vary from one jurisdiction to another. Developing countries would be called upon to implement effective laws and to train and deploy technical experts within law enforcement agencies for purposes of domestic crime control and to provide international cooperation. In return they would obtain direct assistance in these areas, access to the necessary expertise, and protection of high-technology elements of their development strategies from crime. Developed countries would be called upon to provide direct support to developing countries. They would also be asked to assure developing countries of access to information and expertise from the private sector, while assuring the private sector that commercial interests in shared information will be protected.[2] In return, developed countries would obtain cooperation from both the private sector and developing countries. In addition to these interests, experience with the Council of Europe Convention[3] suggests that a balance between privacy and other human rights interests and effective investigative powers will have to be struck, an exercise likely to involve some tempering of expectations on the part of interest groups on all sides.

(ii) Potential civil or criminal liability of service providers

In the present environment, manufacturers and service-providers often find themselves caught between conflicting pressures generated by law enforcement and judicial powers pursuing offenders on the one hand, and by their customers on the other. One area where this is apparent is the question of whether Internet Service Providers (ISPs) can or should be civilly or criminally liable for hostile programs or offensive content generated by their subscribers. Law and policies based on analogies to older forms of communication

[1] The position of the G8 and governments of countries with extensive high-technology industries in general has been that cooperation should be voluntary (Sussmann 2000 at pp.468-69). Within governments, economic and commercial interests favour voluntary strategies which are seen as supporting fair competition and industrial development. Law enforcement and security interests tend to favour more coercive measures to establish and preserve effective investigative options. For an illustration, see the discussion of encryption products, below.

[2] Security of products has been a major private-sector concern, but this may be changing. A major concern of many governments and large corporate users of software has always been the possibility that "back doors" installed into operating systems could be used for espionage. In 2003, Microsoft publicly agreed to provide foreign governments with access to the source codes for Windows and other products, to allow them to vet them for security problems. This was partly provoked by the success of other products, such as the Linux operating system, with open-code policies. Simply giving away source codes raises the possibility of copying, but also in some cases can make a product more competitive.

[3] When the draft text of the European Convention was released, it was immediately attacked by interest groups. Major concerns were based on the balance between privacy interests and intrusive investigative powers and the fact that the treaty was not open to public scrutiny during the negotiation process. See, for example, American Civil Liberties Union, "8 Reasons why the U.S. should reject the international cybercrime treaty" http://archive.aclu.org/issues/privacy/ Cybercrime_Feature.html, visited 30-05-03.

such as broadcast or print media generally favour holding the providers themselves liable. Newspapers and book publishers can be sued for libel or publishing obscene material, for example, based on the principle that they were aware of content generated by an author and magnified any harm caused by giving it public dissemination. In response, those who host Internet sites and provide other services argue that established rules should not apply because the technologies themselves are not analogous.

Unlike conventional print and broadcast media, providers argue that they are not able to effectively monitor content and screen out offensive or illegal material, and that they are also not qualified to make the legal or moral judgments required. [1] Once a website has been established for a client, the client can post information directly, and in the case of web-sites which host such things as chat-rooms or electronic bulletin-boards, other users can also post information. None of this flows through the ISP, which therefore has no effective control over what is posted. Also, whereas the volumes of information which flow through print and broadcast media are relatively limited, the sheer volumes of digital information involved, especially in the case of the large carriers, effectively preclude any screening for the nature of content or illegal activity such as downloading in a jurisdiction where importing the content was prohibited.

Traditional media are characterised by asymmetrical information flows, in which a small number of sources such as professional journalists generate information for dissemination to large numbers of subscribers or viewers. The new media on the other hand, feature more symmetrical and unmanageable patterns, in which the numbers of potential sources and destinations for information are both equal and very large. This increases the volume of raw information which would have to be reviewed, and makes it much more difficult to assess validity, credibility or the criteria on which exceptions such as fair use or legitimate political or artistic expression can be based.

From a legal standpoint, ISPs may be shielded from liability for offences such as possession, exportation or dissemination of offensive content in some countries on the basis that, being unaware of the nature of the content, they lack the intent required to establish the offences. This fails, however, in cases where law enforcement or other sources specifically draw the presence of the content to their attention. Some law-enforcement agencies and interest groups have used this method, using searches or tips to identify potentially offensive content, reviewing the content and alerting service providers to its existence. Once the provider is aware of the content, if it is not removed, criminal charges or civil action seeking to punish the provider or force removal of the content may be pursued. Questions of *mens rea* aside, service providers may well be held liable under the criminal laws of some countries, particularly for offences such as publication or dissemination, and at least one has been convicted of such an offence.[2]

(iii) Compelling manufacturers and service providers to assist law enforcement agencies

As noted above, the scope and complexity of both storage and communications media has increased to the point where many basic investigative procedures can no longer be carried out without the assistance of engineers or technicians employed by the service providers. In some media the designs of hardware and software may make such measures

[1] See Akdeniz 2001 at pp. 260, 262-66 for discussion of this issue in the context of child-pornography.

[2] See Akdeniz 2001 at p.260, note 43, and 262 note 51. In this case, involving a German service provider, the conviction was subsequently overturned.

impossible or impracticable even if such assistance is provided. This raises a series of issues, of great concern to both law enforcement and service providers about the extent to which the providers may be compelled to cooperate with investigators, and the extent to which both manufacturers and providers can or should be compelled to design and operate systems so as to make investigative measures possible and practicable.

One example of these issues was already raised above: in order to make possible the tracing of criminal communications, the makers of hardware and software must ensure that traffic data can be collected and stored, and service providers must ensure that this is actually done. This ensures that traffic data can be obtained by law enforcement (usually pursuant to a search warrant or similar judicial order), but also generates costs associated with collecting and storing large volumes of data, and problems associated with protecting the data and the privacy of users from unauthorised access as well as with locating and disclosing specific data files when judicially ordered to do so. Wiretapping and electronic search and seizure operations also consume system time and the time of technicians working for service providers, raising the question of costs and whether they should be allocated against the service-provider and its customers or the State and its taxpayers.

Under existing laws and practices in most countries a provider could be searched for such data using the appropriate judicial authority. However, the data cannot be found if they were never stored or have been erased and will be very difficult to find given the complexity of systems and large volumes of data. Some countries have adopted legislation which allows the courts to order the immediate preservation of data to prevent erasure and to compel the provider and its employees to positively assist searchers in locating and disclosing specific data.[1] At the time of writing, one such power was being judicially tested in the United States.[2]

Part II: The effects of new technologies on smuggling and trafficking

I. The smuggling of intangibles or "virtual goods"

The nature of "virtual goods"

As a general examination of the phenomenon of high-tech smuggling and trafficking, this paper takes a broad view of the meaning of these terms and of the range of tangible and intangible commodities which can be the subject of such behaviour. However, governments and enforcement agencies have found it necessary to be more cautious and pragmatic, as they are confronting the immense difficulties encountered as traditional activities are altered by the use of the information and communications technologies, both by legitimate users and criminal offenders. The volume of both commercial and non-commercial on-line activity has increased exponentially, the economic interests are enormous, both for developed and developing countries, the inter-operability of national regulatory frameworks is essential, and many of the specific issues are very much *terra incognita* for policy-makers.

[1] See, for example *Criminal Code of Canada*, S.487(2.1) and (2.2) (power to cause computer system to be used to assist in search). Articles 16 and 17 of the Council of Europe *Convention on Cybercrime* require States Parties to adopt measures necessary to ensure the expedited preservation of content data (Art.16) and traffic data (Art.17), and such measures are in the process of being adopted in countries seeking to ratify the instrument.

[2] *Recording Industry Association Of America, v. Verizon Internet Services*, U.S. Dist. Ct. (D.C.) Civil Action 03-MS-0040 (JDB), 24 April 2003 (denial of motion to quash subpoena compelling Verizon to disclose identity of subscriber sought by RIAA in civil action relating to digital piracy).

Electronic commerce and free trade, for example, have combined to lead to a vast increase in the numbers of legitimate commercial transactions conducted across national borders. For example, where previously a manufacturer of raincoats in Pakistan might typically ship lots of 10,000 to wholesalers or retailers in Europe in a single transaction, officials may now be confronted with 10,000 shipments of one raincoat each to customers who have ordered their own raincoats directly on-line. This has major implications, not only for the taxation of the transactions,[1] but also for the costs and effectiveness of screening the legitimate movement of goods to guard against the inclusion of drugs and other contraband.

In setting out new tax policies, governments have reacted cautiously. Electronic commerce makes transactions more difficult to tax, but the prospect of a significant shift of trade from physical to on-line transactions may represent a major loss of tax revenue and a problem in cases where import taxes are still levied to protect domestic economic interests. The approach of the United States was to declare a complete moratorium pending the resolution of the basic policy question of whether to tax Internet transactions at all and questions of fairness in taxing on-line and physical transactions, developing policies which ensure competitiveness with taxation regimes and businesses based in other countries, and the feasibility of taxing goods which can be delivered electronically or digitally, among other issues.[2] The approach of the OECD, adopted by the WCO, has been to treat what the WCO describes as "virtual goods" as services and not commodities. This means that they are not generally subject to the import, export and taxation regimes applied to more traditional commodities. In the opinion of the European Union this makes them subject to value-added taxes, a position which the U.S. views with concern for various reasons including for the purposes of ensuring competitiveness.

The effect of this on patterns of smuggling and trafficking may well be profound. If Internet transactions are subjected to import taxes, then transfers which take place in evasion of such taxes would generally be considered as smuggling. Given the problems of identifying physical transfers of goods ordered and paid for electronically and the even greater problems of taxing transactions where the goods themselves are transferred electronically, the extent of non-compliance and smuggling could well be very substantial. If, at the other extreme, no electronic transactions are taxed, the definition of smuggling and its potential scope would be limited considerably. Effectively, the only smuggling of either tangible or intangible goods would be in cases where import or export is restricted for other reasons such as dangerousness (firearms, weapons and related commodities or technologies), crime control (child-pornography, narcotic drugs), public health (prescription drugs), or non-governmental economic interests (intellectual property protection).

The volumes of intangible goods being transferred using information and communications technologies has increased dramatically since such activities began in the 1960s. The most obvious reason for this is that the ability to transfer data at high speeds over broadcast, telephone and computer networks has made such transfers much easier. During the 1960s, telegrams were common and intercontinental telephone conversations

[1] The tax implications alone are striking. Major issues include the policy question of whether e-commerce transactions should be taxed, if so by which regimes (e.g., import, sales or other taxes), the problem of identifying and establishing location or residency of vendors and purchasers, the elimination of intermediates such as importers or wholesalers, and the use of cryptography and other security applications to avoid taxation entirely. See Ivascanu, 2000, at pp.243-51 and U.S. Treasury Department 1996.

[2] See *Internet Tax Freedom Act*, 47 USC 51, s.1101(a), recently extended until November 2003 by the *Internet Tax Non-Discrimination Act* , H.R. 1552, 3 January 2001. Numerous public documents discuss the Internet taxation issues under review. See, for example, "Administration Policy Statement Advisory Commission on Electronic Commerce", Meeting Dallas Texas, 20 March 2002, U.S. Treasury Dept. Doc.# LS-492

relatively rare. The advent of satellite, microwave and fibre-optic transmission media and digital technologies to generate and compress signals and direct traffic has expanded capacity, reduced costs, and made access much more widespread.

An even more significant factor in increased traffic is the fact that the new technologies have resulted in the creation of tremendous volumes of new intangible commodities which can be transferred electronically. Virtually anything which consists of information can be reduced to digital data, and this is being done at an unprecedented rate. First computer programming codes and then simple printed texts were digitised, then audio signals such as music, and most recently still and motion-picture visual images have been digitised, as have mass-broadcasting and wireless and wireline telephone signals. Further adding to the traffic volume is the ease with which data can be copied, both legally and illegally: a popular song exists not as one digital file, but as hundreds of thousands of copies, any one of which can be copied further or transmitted electronically from one place to another. With the added factor of digital networks, the conventional distinction between copying and transmission has also all but vanished: from the standpoint of the operator, there is no longer a difference between copying or moving a file from one part of a computer to another and moving it between computers which may be thousands of kilometres apart.

Types of intangibles goods trafficked

As indicated in the previous section, the category of intangible or virtual commodities which can be smuggled or trafficked includes virtually anything which can be reduced to pure information or data, and which has either economic value worth protecting, or dangerous or offensive characteristics that warrant restrictions on import, export, possession or transfer. The full range of virtual commodities is still evolving and expanding, but some of the more common ones can be broken down into the following groups. These are not necessarily mutually exclusive: some types of content have characteristics which could place them in more than one category. Child-pornography, for example, could be considered offensive, dangerous to the children used to make it, and of (illicit) commercial value.

(i) Socially or morally offensive content.

Data in this category are generally subject to restrictions because the information is seen as socially or morally offensive. They may also be seen as dangerous (see below) and may have illicit economic value, but are subjected to controls and sanctions primarily because their offensive nature. In such cases, smuggling or trafficking is primarily for the purpose of eluding such restrictions, although economic gain may also result, particularly if the restrictions and risks themselves drive up the market value. The major types of information in this category include obscene, pornographic or erotic material in general; child pornography; racist or other hate-propaganda; material which is considered blasphemous; and material which is considered politically or socially subversive.

Whether particular information is subjected to restrictions and sanctions in a particular country obviously depends to a significant degree on its political, cultural, social and religious standards, and to the extent that these do not coincide, internal and/or

international friction can develop.[1] Material considered obscene, racist or subversive, for example, tends to create problems if the information is posted on web sites located in a jurisdiction where it is legally protected as artistic or political expression, making it freely accessible to people in a jurisdiction where dissemination, import or even possession is considered a crime. Distinguishing between offensive and dangerous content may also depend to some degree on moral or value-based judgments, and some material (e.g., child-pornography) may be both dangerous and offensive. Subversive information is often considered to be dangerous by the State it is directed against, but merely offensive or even a form of expression protected by human rights standards in other States. Apart from making transmission possible at all, the major role played by the technologies in such cases is that they bring together societies previously separated by geography, language and other factors, giving those involved little or no time to adjust.

(ii) *Dangerous content.*

In some cases, the possession or transfer of data may be subject to restrictions or sanctions because of direct harm which has little or no economic aspect. Examples of this include technical information on how to commit crimes such as murder, how to manufacture explosives or explosive devices,[2] how to produce chemical, biological, nuclear or other weapons, and general national security information. Often this information is available through non-electronic sources, but there is greater concern with electronic availability because it makes the material available to a much wider audience. Materials discussing the chemistry of explosives have become much more accessible to experimenting children, for example,[3] and there are some claims that terrorist groups are using the Internet to disseminate similar information.[4] Another type of information which may fall into this category in some cases is information relating to national security or law enforcement, which might jeopardise or compromise operations or endanger the safety of operatives or others if disclosed.[5] Such information may be disclosed or taken for other reasons but trafficking for profit also occurs.[6]

---

[1] See Roach and Macbride 2000, and for a somewhat blacker perspective, Barber, 2000 in the same source.

[2] In a 2001 U.N. survey, a number of countries asked to provide information about explosive-smuggling raised the availability of bomb-making information on the Internet as a parallel concern. Given the possibility of making explosives with commonly-available substances, some felt that it would be easier and less risky for offenders to transfer only the information, rather than attempting to smuggle explosives. See U.N.- CICP 2002b, subparagraph 32(g). Similar results were also found in an earlier study. See doc. A/54/155, 29 June 1979, Part III C, paragraph 30 (production of improvised explosive devices).

[3] In the United States, officials have reported increases in the numbers of explosive-related incidents in which Internet instructions were involved between 1985-96. They also note that about one third of overall incidents involved "juveniles" under 18 years of age. See Oral Statement of Special Agent Mark James (of the US Bureau of Alcohol. Tobacco and Firearms) before the U.S. Senate Commission on Science, Commerce and Transportation, 20 May 1999, http://www.atf.treas.gov/press/speech/fy99/markjames.htm. In many cases the concern about Internet access to such information is greater for juveniles, as this is the single largest group which would not have ready access to the information from other sources such as university libraries or trade publications.

[4] Richard Reid, charged with the December 22, 2001 attempt to blow up an airliner in flight with a bomb concealed in his shoe, has claimed that the device was made by him using instructions downloaded from the Internet, although forensic evidence partially contradicts this. Several recent Internet items also claim that the middle-eastern Hamas organisation, has used the Internet to disseminate information about how to make and use suicide-bombs to attack Israel. See Candiotti, S. "'Shoe bomb' suspect claims he used Internet recipe", www.cnn.com, 8 January 2002, and "How to bomb thy neighbour: Hamas offers online 'Academy'", http://216.26.163.62/2002/me_palestinians_07_16.html, visited 12/11/02.

[5] In *R. v Shayler* (unreported, 2002), the accused was convicted of disclosing secret information obtained while employed with Britain's MI 5. Much of the initial information was photocopied and sold to a newspaper, but while living out of reach of extradition in France, Mr. Shayler indicated that he was in possession of further damaging information and threatened to release it using the Internet. See "Former Spy Guilty of Disclosing Secrets", BBC News, 4 November 2002, at http://news.bbc.co.uk/1/hi/uk/2400389.stm and Timeline: Shayler Spy Row, BBC News, 4 November 2002, http://news.bbc.co.uk/1/hi/uk/2400701.stm.

[6] In the "Cuckoo's Egg" case, Markus Hess, based in Germany, was using unauthorised access to several open U.S. sites as a remote base of operation in order to gain unauthorised access to more sensitive information kept in better-protected sites, for the purpose of selling it to the KGB. See Charney 1996, pp. 932-38 and Stoll, 1990. Aldrich Ames, who spied for the Soviet Union against the U.S., apparently did so for economic reasons and used computer diskettes and encryption to avoid detection, although the data was delivered by more conventional drop-sites in order to conceal his identity not only from U.S. surveillance, but also from his Russian handlers as well. See Wise, David, *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million*, Harper-Collins, 1995.

Concerns about dangerous information are usually focused on preventing hazards associated with the information, and would typically include measures directed both at the dissemination or transfer of the information and at physical activities which might result from its use. To prevent the making of bombs, for example, authorities would examine the dissemination of information about how to mix explosive compounds and how to make bombs and detonators; the dissemination of information about where and how to obtain tangible commodities such as military or commercial explosives and/or the precursor chemicals needed to manufacture them; and criminal communications in support of the smuggling or illicit transfer of bombs or components by offenders who already have access to them. Deterrence may also be used: the website of one major explosives manufacturer creates a permanent record of every computer which accesses it and contains a public warning to this effect. Having dealt with the information aspects of the problem, most governments would also try to address the problem by restricting physical access to explosives and other components through mechanisms such as licensing basic access and use.

(iii) Commercially valuable data.

In this category, the possession or transfer of data is subject to sanctions because unauthorized dissemination causes loss of value or economic harm to the owner of the data. The two most significant types of information are commercial secrets and intellectual property. In both cases, value tends to accrue as the information is assembled and can be lost if it is disclosed. Revenues generated by the granting of permission to use data such as music recordings or access to reference information stored in a data-base is either lost if the information is made freely available, or accrues to persons not entitled to it if unauthorised copies or access are sold. In the case of commercial or trade secrets, losses are less direct, but can be substantial. For example, competing interests may gain access to information needed to duplicate products without the underlying costs of research and development, or information which can be used to compete unfairly.

While offensive content tends to be prohibited for everyone, sanctions against dealings in commercially valuable data must distinguish between persons entitled to have or use the data and those who are not. This, and the fact that the interests at stake are usually of a private and economic nature, have resulted in national laws which dealt with the problem as a civil or administrative matter. New developments in information and communications technologies have resulted in increases in occurrences and economic losses, which has in turn put pressure on governments to bring criminal justice measures to bear on the problem. In the case of trade secrets and commercial espionage, another effect has been an apparent trend to use State national security or intelligence agencies in both espionage and counter-espionage roles.[1]

(iv) *Data of value if used for other crimes.*

This category includes information which has no legitimate value, but can be used to commit crimes, thereby generating illicit proceeds. Some of the types of information in this category are also of a personal nature and unauthorised access or dissemination may also be

[1] The use of intelligence agencies to assist domestic industries in resisting commercial espionage has become common in developed countries and is relatively public, but offensive use of State experts to conduct commercial espionage has also been reported. See Moscarino, 1998 at p. 606 and Tucker, 1997, pp. 1110-1113. One indirect effect of this is almost certainly the erosion of cooperation between governments in more conventional tasks such as combatting terrorism and more traditional forms of espionage. Tucker notes (p.1111), for example that U.S. companies have been spied on by the agencies of foreign allies using training and techniques developed by the U.S. and shared for more legitimate national security reasons.

criminalized on that basis. Actual information includes personal information which can be used to obtain cash, goods or services or equivalent value, such as: credit-card information; calling-card information; data needed to reproduce or "clone" cellular telephones; electronic banking information such as ATM access codes; and similar information. It also includes information which can be used to gain access to such information or to gain access to electronic services or information of other kinds, such as: computer system access codes or passwords; encryption keys and digital signature information. A third type of information in this category is information which can assist offenders in committing crimes which would not otherwise be possible, such as software designed to support or assist in gaining unauthorised access (the digital equivalent of burglary tools) and other, more general information about hacking or other criminal activities. To the extent that these crimes may generate proceeds, the information needed to commit them may be stolen or accessed and copied, and trafficked between offenders. A common example is the hacking of a commercial website to obtain the credit-card information of its customers, which can then be sold to other offenders for use in credit-card frauds, or used as the basis for extortion of the web site operator, whose business interests would be damaged if it were disclosed.

Specific intangible commodities

(i) Cryptography software and information

The legal and ideological battle over the dissemination of cryptography applications has tested many of the fundamental issues relating to the transfer of information, particularly in the United States. While the principles of encryption and its use to protect sensitive information date back centuries, concern was largely limited to national security agencies, mathematicians and aficionados until the development of modern technologies made strong cryptographies possible, necessary, and available to the average user. During the 1970s, mathematical pioneers such as Whitfield Diffie and Martin Hellman realised that the increasing use of computers and telecommunications networks to create, store and transfer data, often of a sensitive nature, would require protection. They also realised that the development of the computer itself made feasible the routine use of complex algorithms by unsophisticated users to encrypt and decrypt their data.[1] The demand led to the development of new forms of encryption, in particular asymmetrical cryptography, which could be more readily used in computer environments. The basic principles developed by Diffie and Hellmann led first to the development of RSA, a commercial product intended for sophisticated, institutional users in 1977. Shortly thereafter, Phil Zimmermann, a computer scientist and political activist used elements of RSA to develop a much more user-friendly product, which he named "Pretty Good Privacy", or PGP, increasing the potential for widespread use.

These developments were regarded with concern in the law enforcement and intelligence communities because the new cryptographic products could be used to shield not only legitimate communications and stored data, but those of criminal offenders and the targets of national security investigations or surveillance as well. The threat was twofold. First, as the complexity of cryptography and the number of digits or "bits" in an encryption key increase, the number of possible combinations which must be tried to break the code in

[1] For a general history of the development of cryptography during the period from 1970-2000 by Diffie and Hellman (development of asymmetrical cryptography, Rivest, Shamir and Adelman (creators of the RSA cipher), and Zimmerman (who adapted the RSA product to produce "Pretty Good Privacy", or PGP, see Singh 1999, chapt.6 and 7). Singh also notes that the developments which took place in the public sector were paralleled by work undertaken by cryptographers at the UK Government and Communications Headquarters (GCHQ) which went largely uncredited due to official secrecy until the public developments made this moot. See chapt.6 at pp. 270-92.

what is known as a "brute force" attack increases exponentially. This means that as products moved toward what is known as "strong" cryptography, they quickly outstripped the capabilities of even the most well-resourced and sophisticated attackers.[1] The most sophisticated and well-resourced offenders, such as international drug-trafficking rings and terrorist groups, might be presented with communications which were secure against, if not interception, then the reading of intercepted messages.

The other problem is one of volume. The occasional use of encryption by serious offenders could conceivably be successfully attacked, but if even relatively basic cryptographic applications became routine, the task of decryption could prove a major problem for law enforcement, as well as a range of regulatory officials whose duties include inspecting or auditing data. When dealing with a single case, relatively large volumes of intercepted or stored data may have to be decrypted in order to simply identify the specific data relevant to an investigation. More generally, routine or automatic use of cryptography in products such as wire-line and wireless telephones and e-mail and Internet communications software would vastly increase the number of cases in which work on decryption would be needed.

The potential loss of national security and law-enforcement capability led to the development of legislation in the United States restricting the export of "strong" encryption devices. Other countries, balancing the risks and benefits of accessible cryptography[2] adopted positions which ranged from unrestricted development and sale (Ireland) to complete prohibition (France).[3] The threat of pending legislative restrictions on access or export from the United States led Mr. Zimmermann, the developer of PGP to allow an anonymous friend to post his PGP software on a public UseNet in June 1991. This effectively allowed anyone, anywhere, to freely download the software needed to use PGP, and word of the new product and discussion of its implications began to spread quickly. This, in turn, led to two legal actions against Mr. Zimmermann: the company which owned RSA brought an action claiming damages for infringement on their copyright, and the U.S. Government began a three-year grand jury investigation to determine whether PGP had been illegally exported from the United States.[4] Ultimately, in 1996, the government discontinued its efforts, in part because PGP was already available world-wide.[5]

---

[1] For several illustrations, see Smith, 1997, chapt.1.6, 2.2.2, and 9.2.1. The DES standard, with a 56-bit key requires the checking of 10^{16} combinations, taking a large computer about 3.5 hours, while the use of an 80-bit key would take the same computer 6,655 years and a 112-bit key would take the same machine 30,000,000,000,000 years (table 2-3, p.49). The time represents the period needed to check all of the possible combinations, reflecting the most pessimistic assumption that the last combination tried was the right one, but even in practical searches, the task is formidable. A *Scientific American* challenge to break the RSA cipher required an assembled group of 1,600 individual computers eight months to identify the correct key (chapt.9.2.1, at pp.205-06).

[2] The major arguments in favour of access to encryption products were that they were needed to protect privacy and freedom of expression, that the added degree of security would prevent on-line crime and foster consumer trust, particularly in electronic commerce, and that imposing restrictions would put domestic companies marketing cryptographic products and other computer applications which included cryptographic elements at a disadvantage to countries where these were not restricted. Much has been written about the policy issues surrounding cryptography restrictions, including Goldstone, 1999, Saundersby 1999, White, 1999, and OECD 1997(1) and (2) and OECD 2002.

[3] Madsen, *et al*, 1998. Ultimately, commercial and privacy interests prevailed, leaving law enforcement and intelligence agencies to deal with the loss of surveillance capability through other means, if at all. This drew some criticism in the wake of the major terrorist attacks against the United States of 11 September 2001, but generally the traffic in strong cryptography applications is completely or relatively unrestricted, with the exception of countries in which more general controls on expression and access to government information also apply, including Belarus, China, Pakistan, the Russian Federation, and Singapore (Madsen also includes France and the USA, where restrictions have been reduced or lifted since 1998). In discussion following the September 2001 attacks, Mr. Zimmermann expressed concern about the possible use of strong cryptography by Al Qaeda and other terrorists, but maintained his view that the balance of interests favoured access to such cryptography. See Cha, A. "To Attacks' Toll Add a Programmer's Grief", Washington Post, 21 September 2001, p. E01, and Zimmermann, P., "No regrets about developing PGP", 24 September 2001, posted on-line at: http://slashdot.org/article.pl?sid=01/09/24/162236&mode=thread.

[4] For an account of developments, see Singh, 1999, chapt.7.

[5] Singh, 1999, chapt.7, pp.314-15.

Unrelated to the question of exporting, importing or trafficking in PGP were the constitutional questions of whether cryptography should be protected under the First Amendment to the U.S. Constitution, either as a form of speech or expression on the part of Mr. Zimmermann or as an instrument of expression for those who might need PGP to express themselves freely and anonymously,[1] and these issues dominated the subsequent litigation.[2] Arguments raised and considered did, however, highlight the legislative difficulties in controlling the export of intangible information. The property interests of RSA aside, the novel issues raised by the Zimmermann case included the following.

- Whether or not the downloading or other transfer of PGP over the Internet constituted an "export" at all. In focusing on whether the International Traffic in Arms Regulations amounted to an unconstitutional limit on exports, the courts appear to have accepted that an export had occurred. The legislation itself sought to address this question by including as forms of export "…downloading or causing the downloading of, such software to locations outside of the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo-optical, photo-electric or other comparable communications facilities…"[3]

- If an illegal export had in fact occurred, whether the offence was committed by Mr. Zimmermann and/or his anonymous friend in simply posting the software on a site within the U.S., or by numerous unidentified persons outside of U.S. jurisdiction who had accessed the UseNet from abroad.

- From a policy and constitutional standpoint whether a regulation directed at the transfer of pure information in the form of software code was viable, when the same data could have been exported lawfully in other forms, including printed books or documents. Information reduced to a digital format was much more readily useful for encryption – which is why legislative steps were taken to restrict distribution – but the difference between digital and other representations has to do with the medium only, and not the actual message. Both Bernstein and Junger, were left, for example, in some doubt as to whether the dissemination of academic papers discussing or describing cryptography were caught by the ban.

- More generally, whether the attempt to restrict foreign distribution of the software was enforceable and practicable at all, given the ease with which data could be exported by e-mail or downloading. Even in the atmosphere of publicity surrounding the cryptography policy debate, many computer users would have been in a position to send or receive PGP and similar applications across international borders, and would not have been aware of the export restrictions. For example, foreign nationals who downloaded PGP would not have been subject to, or even aware of, the U.S. export offences. The practical problems become even more pronounced when encryption is incorporated into other computer applications such as e-mail programs, and as many academic, business and other professionals travel while in possession of computers equipped with such software.

[1] See concluding comments of the Court in *Bernstein* (1999) and Nguyen, 1997 at 679-82.
[2] See *Bernstein v. U.S. Dept. of State* 922 F. Supp. 1426 (1996), 945 F.Supp. 1279 (1996), 974 F. Supp. 1288 (1997), and *Bernstein v. U.S. Dept. of Justice* 176 F.3d 1132 (1999). See also *Daley v. Junger* , 8 F. Supp. 2d 708 (1998) and Nguyen, 1997.
[3] US Regulation 15 C.F.R. para.734.2(b)(9)(B)(ii), quoted in *Bernstein* (1999) at footnote 6. the original regulation was Pub. Law No. 94-329, Title II, s.212(a)(1), codified at (1994) 22 USC 2778.

The feasibility of export controls on software has also been called into question by the rapid development of other information and communications technologies during and since the *Bernstein* and *Junger* decisions. Cryptographic applications remain a major concern, but there are other ways to conceal data from criminal investigators, and none of these were subject to the export controls applied to encryption. Many of these also have legitimate applications and commercial value, and all can be transferred electronically posing the same technical problems as arose with encryption.[1]

The encryption debate and litigation in the United States provides a useful *entrée* into the smuggling and trafficking of electronic commodities or virtual goods because of the strength of the debate and the intellectual and financial resources dedicated to developing the issues and raising them before the U.S. courts.

Information and communications technologies play a major role in these issues. The commodity itself – in this case encryption software – was directly produced by the technologies, which made the development of strong cryptographies for unsophisticated users possible. Encryption and decryption is too demanding and time-consuming to be practicable, unless the process is automated using pre-written software and a computer which uses the software to scramble and de-scramble data. The second direct role is that the technologies also produced the means whereby Mr. Zimmerman, his anonymous friend and/or the recipients actually exported the software in a manner which was not amenable to either interception by technical means or to legal export restrictions and prosecution for smuggling.

The other major effect of the technologies is less direct, but arguably more profound in its impact. The demand for encryption was largely driven by the proliferation of ICTs. During the 1970s, academics, law-makers, human rights activists and commercial interests began to understand that the storage of ever-increasing volumes of personal information in data-bases, and the ability to link, search for and access such information quickly and comprehensively represented a major and growing privacy issue. The concerns grew as computers were linked together in networks which could not be protected by physical security measures and data in transit between computers became vulnerable to interception. Commercial interests developing hardware, software and providing network access and other services also saw the privacy fears of customers as both a business opportunity and a risk. Only those products with privacy protections incorporated would be competitive, and those from companies or countries which could not protect privacy would lose out. The ultimate result was a series of decisions by countries, which had sought to restrict the strength of encryption products, to abandon this approach to preserve the competitiveness of their domestic encryption industries, their ICT industries, and of electronic commerce in general.[2]

(ii) Child pornography

[1] Many such applications conceal data by interspersing it with other data, with the formula needed to re-separate the files as both algorithm and key. See, for example, Saundersby, 1999 discussing "chaffing" and "winnowing". Another application is "steganography", in which small files are imbedded in larger ones, such as digital photographic images. Steganography applications are usually relatively easy to "break"; their security lies in concealment, as searchers do not suspect that data has been hidden at all. Substantial files, including child-pornography images, can be completely concealed in this way.

[2] Widespread electronic commerce depends heavily on encryption applications, particularly the encryption of credit-card and other personal data, and the use of digital signatures to identify transaction parties to one another. Any lack of security would likely result in both actual electronic crime, and in loss of consumer confidence as a result of the fear of crime.

Among the types of offensive content, child-pornography is of particular interest because it enjoys the greatest international consensus in favour of prohibition. Definitional details may vary, but generally countries agree on what child-pornography is, and that production, possession or transfer, even by purely electronic means, should be considered a crime. This makes it a useful basis for comparison and a precedent for legislative and policy development. In several countries, it has also been the basis of court cases considering the right to freedom of expression and other constitutional or legal constraints on measures to restrict production or dissemination by electronic or other means.[1]

The major reasons given for suppressing child pornography are a combination of values relating to the human rights of children and sexual and other forms of exploitation, and the practical goal of protecting children from abuse. Concerns about abuse include direct victimisation (e.g., rape or sexual assault) in the course of making child pornography, and indirect victimisation from the distribution of images without consent, the use of pornography to "groom" or encourage other children to engage in sexual activity, and from the potential for further offences committed by paedophiles who may be encouraged or stimulated by the use of child pornography.

The available evidence suggests that new information and communications technologies have had a significant impact on virtually every aspect of the production and trafficking of child pornography. The effects and the mechanisms which have produced them range from subtle to profound, but the evidence of many of them can be clearly seen, and some raise issues which are likely to become important in dealing with trafficking in other intangible commodities in the future.

Child-pornography differs from some other forms of trafficking in that not all of it is profit-motivated. The evidence suggests that some activity consists of trafficking by conventional organised crime groups who sell materials, or access to materials, to paedophiles for profit. In other cases, however, it consists of reciprocal sharing of content by paedophiles for non-profit purposes. Both commercial and non-commercial trafficking is ultimately based on the desire of paedophiles for such material in the face of legal restrictions and the risks and costs of obtaining it illegally.

Key policy issues surrounding the suppression of child pornography include the extent to which it can be restricted in the face of constitutional or other laws protecting expression; whether only child pornography which involves the direct victimisation of children or all child pornography (including, for example, drawings, "pseudo-photographs", images of adults who resemble children, and written material) should be suppressed;[2] the extent to which service providers and others can be held criminally liable for dissemination, a group of issues arising from jurisdictional discrepancies about how to define child-

[1] The major cases thus far are *R. v. Sharpe* (Canada) and *Ashcroft v. Free Speech Coalition, et al.* (USA), below. Similar issues are being raised in other countries. See, for example, Ellis, E. "Can child porn 'research' be legal?" (South Africa), *The Star* on line, April 22 2003 (visited April 24 2003), http://www.thestar.co.za/index.php?fSectionId=225&fArticleId=134699. For commentary on the available evidence, see Graham 2000, particularly at footnotes 105-111, Martin 2001, and Cisneros 2002.

[2] See *R. v. Sharpe* [2001] 1 S.C.R. 45 (Supreme Court of Canada), as well as *Reno v. A.C.L.U.*, (1997) 521 U.S. 844, 117 S.Ct. 2329 and *Ashcroft et. al. v. Free Speech Coalition, et. al* (Supreme Court of the United States, 16 April 2002, case No. 00-795), all holding, in part, that constitutional protections of expression or speech limited the extent of restrictions on child-pornography, particularly that for which production did not involve real children. See also Akdeniz 2001, pp.252-53 and 256-59. Since most would consider the use of real children to make pornographic material a form of victimisation, the justification for suppressing material which uses real children is fairly clear-cut. Suppressing drawings, pseudophotographs and written material is more problematic because it depends either on a general policy of suppressing paedophilia, or establishing less-direct forms of harm to children, such as the use of pornographic material by paedophiles to "groom" future victims, for which the evidence is less clear. See Akdeniz 2001, pp.252-53. Arguments against allowing pornography which uses models who resemble children but are over 18 years of age also include the fact that making such an exception often necessitates proving the age of the subject, which is impossible in most major cases because the victim cannot be located.

pornography and the extent to which it should be suppressed;[1] and technical and legal issues surrounding the use of the technologies themselves to identify and screen out such material.[2]

Quantifying the global extent of activity relating to child-pornography in terms of numbers of producers, consumers, victims or monetary value poses a major challenge for researchers because so much of the problem is hidden and it appears to be changing very rapidly.[3] What is not in serious contention, however, is that there has been a significant increase, and that this is due to a large extent to a series of developments in information and communications technologies. These have increased both the supply and demand for child-pornography, and have reduced the risks of detection and prosecution associated with dissemination. One key question in the field is the extent to which the technologies have actually increased the number of consumers (e.g., by attracting paedophiles who would not or could not obtain the material face-to-face), as opposed to the extent that they have simply made a previously-existing phenomenon more easily seen and monitored. A related question is the extent to which previously-existing paedophile activity has simply been transferred from a physical to an electronic environment.[4]

The reasons for any actual expansion in the making, smuggling and trafficking of child-pornography can be seen to a large degree in the specific uses to which various technologies are put.[5]

a. The making of child-pornography

While national definitions vary, generally child pornography consists of information in the form of written text, audio recordings, or still or moving visual images. The most common forms, visual images, may depict real children, adults who resemble children, or non-existent children (drawings, altered photographs etc.). Recent developments have made the equipment needed to record and view pornographic images, such as video and digital cameras, available to much larger number of basic users than previously, both by making them less expensive and automated to the point where professional skills are no longer needed. At the same time, the technologies have transferred the control of the entire production process in the hands of the consumer, displacing the control and surveillance effects of the photographic laboratories which were previously needed to develop and print film-based images. A further development, which arises out of the ability to manipulate digital images, has been the creation or modification of child-pornography using techniques

[1] Such issues include the cut-off age at which subject-matter should be considered as child pornography (most countries have established 18); and whether mere possession should be criminalized. See generally, Ivezaj, 1999. See also UNESCO, 1999.

[2] As concern about on-line pornography in general has increased, software companies have developed products intended to identify and deny access to offensive material. From a technical standpoint, lacking human judgment these often screen out legitimate or innocuous materials, such as academic or journalistic discussions of pornography, and material which might be considered as having scientific, medical, literary or artistic merit. These are most commonly used privately by parents to screen content to which their children have access, but legal issues arise when they are used by public institutions such as libraries. During the writing of this paper, the Supreme Court of the United States held that both voluntary decisions by public libraries to block access to pornography of any kind and federal legislation requiring them to do so did not offend that country's constitutional Bill of Rights. See *United States et al v. American Library Association, et al* US Supreme Court, 23 June 2003, file #02-361, not yet reported.

[3] UNESCO, 1999 and ECPAT, 2001, p.17. The latter refers to a "…new and hugely expanding market…" for child-pornography. Major quantification problems include the fact that a single image is immediately copied and may be found in numerous locations world-wide within only a few hours (O'Connell 2001, p.72) and the fact that, while numbers of files posted can be measured, many of those who download or view them leave little trace of their activity, particularly on sites which do not charge fees (O'Connell 2001, p.68). Monitoring newsgroups in January 1998, O'Connell found over 6,000 images posted in a two week period, and she notes that this did not include other digital distribution media.

[4] At least one source (ECPAT 2001, p.20) notes that there has been a reduction in the use of printed erotic magazines as users moved on-line, a fact which has led the publishers to open their own on-line erotic sites to maintain market-share. The extent to which this is also true of "hard-core" and child pornography cannot be established.

[5] See generally, ECPAT 2001, pp.19-22, Ivezaj 1999, pp.823-28, Akdeniz 2001, pp. 247-50, UNICEF 2001 and UNESCO 1999. There is substantial agreement among all of these sources about the various ways in which technologies are used, as well as the overall effect of increasing the global traffic in child pornography.

such as digital "morphing". This can be used by offenders to alter innocuous images to make them pornographic, to make images of adults look more like children, to merge several images, or to alter recognisable characteristics to conceal the identity of children or locations where images were recorded.

The effects of these developments have been increased opportunities to create child-pornography, a perceived (and to some extent actual) reduction in the risk of detection and prosecution, and hence a general increase in the supply. The use of manipulated images makes identification and tracing more difficult, and raises serious legal obstacles to prosecution in jurisdictions where it must be established that real children were used to make the images.

b. The storage and dissemination of child-pornography

As with other virtual commodities, once reduced to digital data, child-pornography can be electronically copied, transferred and generally disseminated in the same ways as any other data, which vastly increases opportunities for dissemination. Indeed, dissemination has become so easy that, as with legitimate intellectual property, one problem faced by offenders is how to protect their interests in the material they produce in order to derive economic benefit from it. Unlike legitimate intellectual property, however, paedophiles often share pornographic material *gratis*, or accept "payment" in the form of other pornographic material shared in turn. A common form of on-line paedophile activity now involves the establishment of child-porn "libraries" which allow a user access to an entire collection of materials once the user has contributed a specified quantity of materials of his own.[1] A related problem, rooted in the ease of copying and sharing, has been the difficulty of quantifying the number of images or files, since investigators often encounter the same materials repeatedly. Apart from the basic ease of copying and transfer, the technologies also allow import/export transfers with no effective customs surveillance, and the ability to transfer the same data to large number of users simultaneously. Both of these effects simplify dissemination, while reducing costs and surveillance.

c. The reduction of risk to offenders

As noted above, the advent of digital cameras, video-cameras, and the ability to privately access Internet sites from home computers reduce the degree of outside surveillance which existed with earlier forms of child-pornography. The high volume of information now on-line and the speed with which it moves from place to place also create an ever-larger pool of legitimate material within which offenders can conceal their own activities, making detection less likely. The risk of surveillance, detection and prosecution is further decreased by the advent of security and privacy-enhancing technologies such as cryptography and steganography, which allow incriminating data to be concealed from general monitoring or surveillance such as law-enforcement investigators "surfing" the Internet in search of illicit material, and in the case of "strong" cryptographies, even from fairly determined efforts at seizure and the reading of content believed to be offensive.

Both cryptography and steganography are frequently used by paedophiles to conceal child pornography while in transit, and cryptography applications are also used to encrypt stored data. Risks are also reduced by the use of technologies such as anonymous re-mailers and cloned or disposable cellular telephones to avoid leaving traffic data which

[1] See, for example, "Teenager ran biggest Internet child-porn library in Britain", *The Independent*, 14 November 2002, p.2.

could be used to trace the activities of offenders, should one of their on-line contacts be compromised.[1] Risks are also reduced in other ways. The ability to communicate with other paedophiles allows newcomers access to information and assistance in avoiding detection both by using security technologies and by more basic habits such as not posting personal information about themselves and choosing filenames and on-line aliases which use oblique or coded terms for paedophile activities.[2]

The very nature of computer networks also tends to make it easier for paedophiles to locate and use child pornography from the privacy of their own homes, which further reduces inhibitions (below) and may well affect patterns of trafficking and use. As noted above, access to the Internet through individually-owned computers predominates in developed countries, whereas access in developing countries tends to be through common or shared sites. This means that paedophiles in developing countries who do not have individual access must download files and face the additional risk of surveillance inherent in printing them in a relatively public environment.

d. Reduction of offender inhibitions

Paedophile activities, including the use of child-pornography, are often rationalised or normalised by offenders using moral or ideological justifications. These include minimising the perception of harm caused to children,[3] characterising laws which impose age-limits on the legal capacity to consent to sexual activity as an infringement on children's rights, and drawing parallels between paedophilia and homosexuality as forms of natural sexual orientation.[4] This activity pre-dates the Internet, but the nature of Internet communications supports it by allowing paedophiles, and especially newcomers, to associate with large numbers of other paedophiles, and to express themselves in relative security. Where previously offenders may have been isolated individuals, they are now able to share their experiences and views with other offenders, including both justifications and very practical advice on how to locate pornographic material, how to identify and entice vulnerable children on-line and in the physical world, and how to elude detection while committing paedophile offences. As one expert puts it, the message is: "You're OK and what you're doing is OK; don't listen to the rest of the world, just listen to us."[5]

Given the uncertainty about the nature of sexual orientation and whether paedophilia is such an orientation, it is doubtful whether access to such justifications could be said to actually create paedophiles, but it would be surprising if it did not entice those who might not otherwise have acted upon their inclinations to do so and encourage and expand their range of paedophile activities. In this context, the nature of the network not only increases trafficking in child pornography by making it easier and less risky to access, but also by convincing offenders that it is morally or ethically permissible to do so and creating an atmosphere in which the use of child-pornography is not only an act of sexual gratification, but of self-expression. This tendency may be further reflected in the preference of most paedophiles for images and material which portray children as consenting or willing

[1] This is a technique used by on-line offenders in general. See Edelstein 1996.
[2] O'Connell 2001 at pp.65-69 and 70-72.
[3] A number of journalistic accounts of child-pornography prosecutions include comments by the accused to the effect that they did not recognise that actual children were harmed in production, that acquiring only pre-existing images would not further victimise children, or that the indirect victimisation of children *via* pornography was justifiable on the basis that using such materials was preferable to engaging in direct sexual activities with children.
[4] The most prominent organisation is NAMBLA, the North American Man Boy Love Association, which is based in the USA, but maintains a German Internet site, http://www.nambla1.de/.
[5] Mahoney 2001.

participants.[1] It may also be fuelled by the condemnation of paedophile activities by outsiders, both on-line ("flaming") and in other mass-media. This fuels a sense of persecution and solidarity among paedophiles once they are brought into contact with a group.[2]

e. Paying for child-pornography

As noted, trafficking in child-pornography differs from many other commodities in that at least some of the distribution involves simple sharing or bartering by and among paedophiles without the exchange of money.[3] Where money is exchanged, however, the technologies simplify this and provide ways in which payment can be made while avoiding attempts to trace the funds for purposes of seizure and forfeiture or to use the payment structure to trace and identify distributors and customers.[4] Many of these technologies have been developed as essential infrastructure for electronic commerce, which makes placing any significant limits on their use impracticable. The same characteristics make them useful for money-laundering.[5] The immediate effects include making payment easier and less-risky for all offenders involved in the transaction. As with other forms of economic crime, the technologies also make it easier to accumulate, transfer and launder the proceeds of child-pornography. More generally, the effect is to inject monetary value into production and distribution, which attracts organised crime and other non-paedophile offenders into the field, and almost certainly increases the rate at which children are victimised, especially in developing countries, where poverty exerts pressure and law-enforcement control tends to be less effective.

f. Use of Internet child pornography by offenders

Generally, the uses to which child pornography is put by offenders include basic sexual gratification; use as a commodity to exchange for money or other child-pornography; use to expose real children to paedophile practices in order to "groom" them as eventual victims; and blackmailing previous victims to prevent them from exposing offenders.[6] There is also great concern about the fact that the Internet is attractive to children making it, in turn, equally attractive to paedophiles, who use it to make contact with real children and in some cases to abuse or even abduct children.[7] Paedophile rings have also exchanged information about techniques for grooming victims and even the identity of victims. To the extent that technologies contribute to the desirability or usefulness of child-pornography for these purposes, they also contribute to demand and overall levels of trafficking.

g. The increase of risks to offenders: use of technologies by law enforcement

Not every aspect of the technologies reduces the risk of surveillance and detection, and the failure to realise this fact has led to the detection and successful prosecution of large

[1] O'Connell, 2001, pp.66 and 70-73.
[2] O'Connell 2001, at pp.72-73.
[3] Non-monetary trafficking is also common in intellectual property cases, and represents an additional challenge to legislators and investigators because financial gain cannot be used as a basis for liability and funds cannot be traced and targeted. See O 'Connell 2001, pp.76-79. Non-monetary offenders may also attract more popular sympathy, although this is primarily a problem encountered in intellectual-property cases, given the popular condemnation of paedophiles. See Goldstone 2001, part I.A. "Large scale [copyright] infringement without profit motive" and the following segment.
[4] Some methods of payment are riskier for offenders than others, however, as the discussion of the "Operation Ore" and "Candyman" cases in the following segment illustrate. In those cases, credit card information provided by offenders was used to trace them after law enforcement officials broke the encryption relied upon by a large distribution site for child pornography.
[5] See Edelstein, 1996 and Rueda 2001.
[6] UNESCO, 1999.
[7] ECPAT 2001, p.20. Numerous individual cases of Internet-related child abuse or child-abduction are now reported, prompting both law enforcement agencies and Internet Providers to establish programmes to educate parents and children about the potential dangers.

numbers of offenders in recent years, particularly in child-pornography cases. Generally, on-line contacts leave traffic data which can be used to trace those who visit websites, and information is also often recorded about whether data was downloaded, particularly by sites which charge fees. In many cases, law enforcement agencies which encounter trafficking in child-pornography are able to trace files from one offender back to the source, and then to trace all of the communications with that source to locate large numbers of other offenders. This commonly involves more than one country, and investigators meet on-line to coordinate investigations and the seizure of physical evidence from the offenders.

Prosecutions in such cases are generally based on recovered traffic data (proof of offences such as importing or dissemination), and stored files recovered from the offenders' own computers (possession offences and proof of the nature of the content imported or disseminated). Several major recent cases have involved the United States and the United Kingdom, which dedicate substantial law-enforcement resources to such investigations. At the time of writing, the largest case thus far, a U.S.-based case known as "Operation Ore", had generated data on about 310,000 suspects based on recovered traffic data and credit-card information. 7,200 of these were under investigation in the U.K. amid considerable media attention due to the high profile of some of the suspects,[1] raising the question of whether similar investigations were ongoing in other countries. One major challenge facing investigators and child-welfare authorities in such cases is determining the true place of origin of pornographic materials and trying to locate the children used to make it, both for support/rehabilitation and as potential witnesses.

Within Europe, international cooperation will be substantially assisted by the *European Convention on Cybercrime* (Art.9) which requires the criminalization of the production, making available, distribution, transmission, procuring or possession of child-pornography using computer systems or data storage media, and establishes a framework for international cooperation to investigate and prosecute cases.

h. Conclusion

As with other intangible commodities, the development of new information and communications technologies can be seen to be having both direct and indirect effects on virtually every stage of the production of and trafficking in child pornography. Some of the effects have assisted law-enforcement in controlling the problem, but the dominant effects have been significant increases in supply, demand, the ability of offenders to generate revenues, and the flow of revenues from users back to producers in widely-separated locations. In doing so, they have almost certainly increased the frequency with which real children are sexually abused in order to produce child-pornography. This, in turn has been associated with the treatment of children themselves as a commodity for trafficking, as

[1] See "Operation Cathedral and the Wonderland Club", ECPAT 2001, pp.25-27. "Operation Ore" began with the investigation of a Texas-based web site which charged subscribers and opened links to other sites in early 2001. U.S. law enforcement authorities seized credit-card and subscriber data from the provider, generated a list of about 310,000 customers and began sharing these as investigative leads with law enforcement agencies in other countries. This included 7,200 U.K. suspects, of whom about 1300 had been arrested in the first 10 months alone. One effect of this in the U.K. was to lead regional police agencies to complain that they lacked the resources to pursue all of the cases quickly enough, and police were forced to screen the leads to identify those in positions of responsibility or with access to children as priority cases. This in turn led to the identification of high numbers of suspects in the police service and educational professions, as well as others in positions of power or political influence. See "Mass Arrests over Child-Porn", BBC News, 20 May 2002, and "Operation Ore: Can the UK cope?", BBC News, 13 January 2003, http://news.bbc.co.uk. See also "Britain's Hunt for Child Pornography Users Nets Hundreds Besides Pete Townshend" New York Times, 14 January 2003, "1200 arrested in British paedophile raids", Times On-Line, 18 December 2002, http:www.timesonline.co.uk/article/0,,2-517566,00.html, "Dozens arrested in child porn probe", CNN.com/US, 19 March 2002, http://www.cnn.com/2002/US/03/18/fbi.child.porn/?related , and "Child Porn Ring Smashed", CBS NEWS.com, 19 March 2002, http://www.cbsnews.com/stories/2002/03/18/national/main503982.shtml.

traffickers are able to generate profits not only from exploiting children for sexual services and general labour, but also for the production of pornography.[1]

Intellectual property

The other major intangible commodity which will be discussed in detail is intellectual property. As with the previous categories, new technologies have tended to increase activities which might be considered as forms of trafficking. The nature and extent of the effects of the technologies depends to some degree on both the technologies and the nature of intellectual property and why dissemination is restricted. Unlike cryptographic products and child pornography, restrictions are placed on intellectual property for economic reasons. The right to copy or use intellectual property is usually the primary means of generating revenue for the author or creator, effectively compensating them for having created the subject-matter in the first place, and much of this revenue is lost if the information is illicitly copied and disseminated. Another major distinguishing feature of intellectual property is the fact that not all copying and dissemination is illicit. To generate revenues, it is necessary not only to prevent unauthorised copying and use, but also to allow authorised activities with as few restrictions as possible, and to find legal and technical ways of distinguishing between the two.

Musical artists testifying in the recent (2001-02) *Napster*[2] hearings compared the downloading and copying of their materials *via* the Napster site to simply walking into record stores and taking physical recordings without paying for them. This illustrates the problem: to pay artists for creating the musical recordings, it is necessary to give them wide commercial distribution in a manner that is attractive for consumers, while preventing further copies from being made and sold for the benefit of copiers who did nothing to create the material in the first place. The legitimate production and dissemination of intellectual property, particularly in forms which can easily be copied, is more prevalent in the developed countries, which possess the technical facilities needed for production and the primary markets for much of the material. Illegitimate copying is divided between organised criminal elements copying for profit in developing countries where law enforcement and other controls are weak, and large numbers of individual users copying and in some cases distributing materials for other reasons in developed countries. Much of the pressure for international protection in *fora* such as the WTO, and for the application of criminal, as opposed to civil, measures, has come from countries such as the United States, which have extensive investments in key industries in the entertainment and technology sectors and therefore the most to lose through widespread illegal copying and distribution.

Since the value of most intellectual property involves either actual use, such as reading books, listening to recorded music or watching motion-pictures, or the copying of such materials in order to sell them or store them for later use, it is in this area that technologies have had the greatest impact. As noted in the introduction to this segment, however, the role of technologies in creating and storing intellectual property in forms amenable to copying, storage and transmission has also had a substantial effect by increasing the volume of raw material which can be copied and trafficked electronically. The most commonly-trafficked forms of intellectual property include music stored in analog

[1] ECPAT 2001, p.18.

[2] *A&M Records, et. al. v. Napster Inc.*, U.S. 9th Cricuit Court of Appeal, 2 December 2001, Case #00-16401, holding that the Napster site, on which users could post copyrighted music files for other users to download, contributed to the infringement of copyrights on the files by persons who downloaded them and awarding an injunction against Napster, Inc.

(traditional magnetic tape) or digital (conventional CD, DVD, MP3 and other) formats; motion-pictures (video-analog and DVD formats); computer software; and to a lesser extent valuable still images.

A related form of trafficking involves, not the distribution of genuine intellectual property, but the use of fraudulent labels or other information to mislead consumers into believing that fake items such as designer clothes or other items to be worth more than is actually the case. To follow the previous *Napster* analogy, instead of taking recordings actually made by an artist, offenders falsely label other recordings as the work of that artist, defrauding purchasers and causing the artist loss of revenue and reputation.

As with other intangible commodities, information and communications technologies can generally be used to produce or copy intellectual property, to transfer or disseminate it, and to collect and conceal or launder proceeds. The commercial nature of both legitimate and illegitimate dealings in intellectual property produce other, less direct effects, however. New technologies such as international broadcasting and the Internet are also used to advertise and create demand for products, and this demand drives both legitimate and illicit dissemination. As with child-pornography, some of the global activity appears to be profit-driven, but there is also a significant amount of non-economic sharing of information. The *Napster* case is in many ways similar to virtual "libraries" containing child-pornography, in the sense that users were able to post copies of musical recordings, which other users could then download free of charge.[1]

The primary effects of technology on this form of trafficking lie in the migration of various forms of intellectual property into media which are more amenable to copying, and the development and proliferation of the devices and expertise needed to copy them. This is the central dilemma faced by content producers: they require the new technologies to facilitate legitimate production and distribution, but use of the same technologies brings with it increased vulnerability to parallel, illicit production and distribution. The major forms of intellectual property have all "gone digital" within the last decade, because this generally reduces costs, enhances creative flexibility, improves quality and facilitates legitimate distribution. Motion-pictures shot using digital cameras, for example, can be edited more easily, facilitate the insertion of special effects material and can be copied electronically, which is cheaper and of better quality than the duplication of emulsion-based film stock. They can be distributed to cinemas using compact storage formats such as digital video-discs (DVDs), or even sent electronically through wire, fibre-optic or wireless channels. Similar developments have taken place in the music industry, and some other forms of intellectual property such as computer software and content data kept in reference databases have always existed in digital formats.

Technological changes have affected the process in several significant ways. Many devices enabling basic copying and use have been created over the past two to three decades, and there has been a general trend to make these devices more widely available, as prices fall and products are designed to be operated by relatively unsophisticated or unskilled individuals. In many cases, this process is driven not only by pressures to develop and market the technologies, but by pressures to increase access to the intellectual property they deliver. For example, the marketing of devices, such as compact-disk players, has been largely driven by the marketing of music, computer software and other products. The major effect of this trend has been to place large numbers of devices in the hands of

[1] See Goldstone 2001, part I.A. "Large scale [copyright] infringement without profit motive".

consumers, which creates correspondingly large numbers of opportunities for illicit use for copying and distribution. Another effect, in jurisdictions where illicit copying, transfer or use is treated as a crime, has been problems with prosecutions in cases where offenders such as juveniles and novices are either not convicted or not punished because they are not seen as serious criminals by the courts.[1]

Increase in demand for illicit copies has also been generated by the fact that, with digital information, completely identical copies can be made, without any loss of quality. Previously, the copying of analog media such as motion-picture film and magnetic recording tape had always involved some loss of quality, enabling the owners, who had original "master" copies, to produce better quality reproductions than infringers. A further concern is that digital files can also be altered more easily, allowing artistic works to be changed and used for purposes not intended by the owner or creator of the original work.

Technological developments have also expedited the copying process in other ways. The rapidly increasing capacity and speed of storage, transmission and processing equipment has reduced the amount of time taken to make and electronically transfer copies, and the costs of doing so. The enormous sizes of digital files required to store an entire motion-picture, complete with multiple sound-tracks for example, were effectively impossible to transfer, but have recently been made possible by such developments, and it is likely that the transmission of digital files, either electronically or using physical storage media, will become the primary means of film-distribution because it is less expensive. Data files do not require the making and transfer of photographic film stock, which is bulky and expensive, and do not require periodic replacement as a result of wear-and-tear. The major developments which have made this possible, and which make illicit transfer, copying and use possible, include: broadband transmission, which allows many channels of data to be transferred simultaneously, digital compression, which increases efficiency and decreases file size, and the faster speeds with which computers can process data once it is downloaded.

A related development, following on the advent of laser-disc technology to store large volumes of data and the digital formats (CD, DVD, MP3 etc.) for storing it, has been the increasing availability of CD-writers, which allow individual users to make and store their own copies of large files. This fact, combined with the basic nature of the Internet, has in turn generated one of the central problems of controlling access to intellectual property. This is similar to one of the major problems encountered in attempting to restrict the distribution of cryptography, child-pornography and other intangible commodities. As copying and storage technologies proliferate, copying patterns change from scenarios in which a relatively small number of individuals control the copying and distribution process, which facilitates both the licensing of legitimate dissemination and the prosecution of illicit trafficking, to scenarios in which large numbers of individuals download and make their own copies, which is much more difficult to regulate. The injunction which was awarded against the operators of the "Napster" web-site was not for infringement of copyright, but for facilitating infringement on the part of the subscribers who visited the site and illegally downloaded recordings.

Several technological developments have also made detection and/or prosecution more difficult. As noted above, the storage of files in electronic, but public locations, such as the Napster web-site, where others can download and copy them, leads to questions about

[1] Goldstone 2001.

whether the actual posting can itself be prosecuted or whether the illicit conduct lies in the downloading and copying. This is likely to be a greater problem for investigators, prosecutors and legislators if the criminal law is used because of the higher standards of clarity, certainty and proof which are required. As with cryptography applications, the download process also leads to difficulties in prosecuting cases of illicit import or export when the material is downloaded in another country. As with other forms of on-line crime, the electronic and ephemeral nature of much of the evidence also complicates the process of conducting investigations, establishing linkages between illicit copies and those who make and disseminate them, and the production of information which meets basic evidentiary standards in court.

Some technologies, notably encryption, have also been used by the owners of intellectual property in order to attempt to prevent illicit copying and use, and to facilitate investigation. For example, encrypted data can imbed unique identifiers into legitimate copies to facilitate the tracing of illicit copies. Basic encryption of data can also be used to prevent the making of intelligible copies, but this requires decryption capabilities for legitimate users, which in turn facilitates the "hacking" of encrypted versions which can then be decrypted and copied for illicit distribution. The result has been a technological battle between producers and pirates which has yet to be resolved or provide a decisive outcome in favour of either side.

II. The trafficking and smuggling of tangible commodities

Role of technologies in smuggling and trafficking

Intangible commodities can be created and transferred using information and communications technologies. This is not the case with tangible goods or commodities, which must physically be moved from one place to another. New technologies nevertheless play a significant role. As with intangible commodities, this role is often parallel for legitimate transfers and illicit smuggling or trafficking: traffickers generally employ the technologies in much the same way as do legitimate traders. A company which has ordered a critical machine part, for example, may check the website of the shipper to determine that it has been shipped, where it is and when it will arrive. An organised criminal group smuggling drugs or other contraband concealed in legitimate goods may conduct the same check to identify any unusual routings or delays which might indicate that the shipment is under suspicion.[1] More generally, orders are placed, prices are negotiated and transfer arrangements are made for narcotic drugs, firearms and other illicit tangible commodities just as they are for legitimate items.

The methods used by legitimate shippers and illicit traffickers to move tangible goods also tend to be relatively similar for all goods, with some variations due to factors such as size, weight, value and the relative need for fast transfers. The actual means of shipping commodities such as firearms, gems or other valuable minerals or narcotic drugs, tend to depend on factors such as the routes chosen and the other sorts of commerce available for concealment on those routes, although the nature of the commodity also plays a role. Trafficked human beings and rare animal or plant species must be kept alive, for example, and the small size and high value of gemstones make forms of smuggling practicable which would not be for bulkier forms of contraband.

[1] INCB 2001, para.12.

In examining the various roles played by information and communications technologies, international drug trafficking is of particular interest. Major traffickers in narcotic drugs are among the most sophisticated and best resourced of organised criminal groups, and are well-positioned to invest time and resources in mastering new technologies and finding ways to adapt and use them for criminal purposes. This means that practices and patterns now becoming apparent in this area are probably indicative of what will occur in other types of trafficking and organised crime in the future, as drug traffickers diversify, criminal expertise is transferred, and technological equipment and expertise generally moves "down-market" to offenders with fewer resources.

The organised criminal groups involved in the drug trade have also been targeted by law enforcement agencies using sophisticated technologies such as electronic surveillance of their communications, radar detection of aircraft and vessels, and satellite surveillance of areas where narcotics are grown and refined, and in many cases, they have developed countermeasures,[1] the use of which is likely to spread in action against other forms of organised crime.

(i) General communications applications

Just as traders in legitimate commodities are able to identify potential sources of supply and customers on the Internet, so can organised crime. The long distances and anonymity afforded by the Internet provide an added measure of security for offenders, who can establish *bona fides* before making actual contact or engaging in criminal transactions, or alternatively, break off contact if an undercover law enforcement operation is suspected. A further measure of security is afforded by the high volume of Internet communications, which help to conceal actual communications, and create electronic venues such as nondescript, closed "chat-rooms" where discussions can proceed undetected. General uses of concern to drug-control agencies include the basic promotion of drug-abuse and lifestyles which favour such abuse, and a propaganda/counter-propaganda struggle has been conducted on-line for some time.[2] As with other forms of organized crime, drug-traffickers also use computer networks to communicate with one another, generally drawing smaller organised criminal groups together, enabling them to cooperate effectively as extended criminal networks.[3]

A wide range of technologies is also used for specific criminal communications such as the ordering, arrangement, and delivery of contraband shipments and payment for such shipments. These generally incorporate features which make them secure or involve the use of specific security products for protection. One common practice is the use of prepaid, disposable, cloned or multiple cellular telephones, which are difficult to intercept and allow offenders to communicate anonymously, since service providers have neither a true name nor a physical location on record. Satellite telephones are also used to avoid interception and communicate from remote locations.[4]

[1] Not all of these involve sophisticated technologies. Placing simple radar detectors on their aircraft, for example, has allowed traffickers to plot the extent of radar coverage by keeping records of the locations at which radar signals were first encountered.
[2] INCB 2001, para.20.
[3] See P. Williams 2001 and United Nations Office on Drugs and Crime, Global Programme Against Organized Crime, "Towards a typology of organized criminal groups", in "Results of a Pilot Survey of 40 selected organised criminal groups in 16 countries", available on-line at: http://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.
[4] This is not limited to drug-trafficking. The smuggling of weapons and diamonds by UNITA during the 1990s was conducted by brokers travelling between Angola and other countries, but the activities were coordinated by Jonas Savimbi in person using a satellite telephone. See Angola 2000, paragraph 9, footnote 4. Use of satellite telephones by terrorist groups is also discussed under that topic, above.

(ii) Defensive security applications

Electronic mail can be protected from automated screening or sniffing for specific content by relatively basic cryptography or even simpler, by the use of coded language to conceal the true content. It can also be protected from even well-resourced attacks on its content by strong cryptography, particularly if large volumes of information must be decrypted to identify and read the specific content relevant to an investigation.[1] Anonymity applications such as anonymous remailers can also be used to strip traffic data from electronic messages, preventing investigators from tracing their origins if they are intercepted, and making it difficult to use intercepts in court unless they can somehow be linked to the offenders by other means.[2]

(iii) Offensive or counter-offensive use of technologies

Technologies can also be used in offensive or counter-offensive applications, particularly in cases where organised criminal groups are themselves targeted by law enforcement using technological methods. Given sufficient expertise and resources, offenders may be able to use many of the same methods as law enforcement.[3] Cases have been reported in which hacking, physical thefts or the corruption of officials have been used by offenders to gain access to sensitive law enforcement information.[4] One Colombian drug trafficking organisation was reported to have cross-referenced electronic surveillance on telephone calls to law enforcement with a downloaded electronic telephone directory of the entire population of Cali to identify possible informers and undercover officers.[5] Apart from penetration of law enforcement computer systems, both radio and wireline telecommunications systems may be vulnerable to the interception of in-transit communications, particularly if they are not protected by encryption and other security applications. Many of the same methods can also be used by criminal organisations to spy on or attack competing criminal organisations or to infiltrate legitimate business operations.

While the major concern of law enforcement agencies will generally be to protect sensitive information in their possession from unauthorised access, offensive disinformation and sabotage are also potential problems. Incriminating intelligence or evidentiary data can be erased or altered so as to make it unreliable and inadmissible, and false information can be planted to mis-direct investigators, consuming resources or leading them away from actual shipments of contraband. Counter-offensive, or "back-hacking" methods can also be used to counter attempts by law enforcement to penetrate the stored data of criminal organisations.[6] In such efforts, attempted penetration results in the attacked system tracing back the incoming communication and uploading software that will either damage the attacker's computer system or enable the offender to gain unauthorised access to it.

Such threats from sophisticated criminal groups have always existed, but the potential for harm has become much greater because of the large amounts of data stored, the ease of access afforded by computer systems, and media which can more easily be

[1] INCB 2001, paragraphs 10, 17.
[2] In many cases, offenders such as virus-writers, traffickers and extortionists who have used remailers have eventually been convicted when investigators find identical data in their computers, such as copies or fragments of a virus for example, but this requires the use of other means to locate and identify a suspect and obtain sufficient grounds to search the computer under locally applicable laws. Regarding anonymity applications, see DuPont, 2000 and Edelstein 1996.
[3] In some cases, it has been alleged that former law enforcement or intelligence experts have been recruited by organised criminal groups. See Ramos 1996.
[4] INCB 2001, paragraphs 9 and 18.
[5] INCB 2001, paragraph 18 and Ramos, 1996.
[6] INCB 2001, paragraph 10.

concealed. Subtle electronic intrusions by organised crime may also go unnoticed for some time, compounding the damage as investigators continue to rely on information or sources that have been compromised. Generally, the risks associated with offensive activities increase with the sensitivity of the communications or data targeted and the sophistication of criminal efforts to obtain or compromise it. The risks decrease with the sophistication of measures taken to protect stored data and communications channels. All of these represent a much more serious problem in developing countries, where government agencies are often at a greater proportional disadvantage in terms of both financial resources and technical expertise.

These threats can often be effectively addressed by sound security precautions, but it is important that law enforcement officials at all levels bear in mind that the use of high-technology applications by both law enforcement and organised crime has to a large degree levelled the playing field between the two sides. Basic security precautions are now a requirement for any law enforcement agency employing modern information and communications technologies. The security of portable media such as laptop computers and diskettes, as well as unencrypted data in transit is a particular concern. Another significant risk, particularly with drug-trafficking and other major organised crime investigations, is the potential for access through corrupt officials who may leak passwords or other technical information which can allow ongoing penetrations. Physical security of places where data are stored or sites from which they can be accessed is also essential, and can pose major challenges when access can be gained from many networked machines, as all of the linked machines or sites must be protected. Other important precautions are the compartmentalisation of information, limiting the damage if any one part of a system is penetrated, frequent changes in passwords, physical and firewall separation of secure communications and storage media from those used to access open networks, and the installation and maintenance of security products which detect and block unauthorised access attempts and create secure archives of all system activities. Essentially, these are the same as for any large commercial or other operation which has sensitive information to protect, although the probability of attacks and the sophistication of attackers may be greater, and should in no case be under-estimated.

Types of tangible commodity trafficked

The range of tangible commodities trafficked reflects both similarities and differences when compared to electronic commerce in legitimate tangible commodities. Generally, commodities which are well-known and have established values, such as books, recordings, air-travel and computer-related products have enjoyed at least moderate success as e-commerce products, whereas personal items such as shoes or clothing, have not, and the same is true for illicit commodities. Apart from concerns about fraudulent misrepresentation, narcotic and other drugs, firearms, tobacco and alcohol products are all established products whose basic characteristics and qualities are known to purchasers without personal inspection. In addition, however, illicit markets also select products based on the need to avoid detection of smuggling by concealing transfers or the nature of the goods involved, and to shield the identities of the parties in order to avoid criminal liability. Experience with legitimate mail-order and e-commerce also suggests that they are able to serve small, select markets such as customers in remote or rural locations or those seeking products sufficiently unusual or rare that only a global or very large market-base can be cost-effective. A partial parallel can be found with the marketing of rare animals and stolen art, antiquities or other collectable items, which can be offered anonymously to a very wide

market in the hopes of identifying a small number of potential customers or offered directly to those customers if they have been previously identified.[1]

(i) Narcotic and other drugs

As noted above, traffickers in narcotic drugs are probably among the most sophisticated and extensive users of information and communications technologies, in terms of the range of technologies applied, the uses to which they are put and the frequency with which they are used. Apart from the direct uses set out in the previous segment, technologies are also used for promoting the use of illicit drugs and for related criminal activities such as money-laundering.[2]

A related commodity is non-narcotic prescription drugs, which are now purchased and sold on-line with increasing frequency. The commercial market prices of prescription drugs generally far exceed the actual costs of manufacture, as companies use their most successful products to recoup research and development costs for less successful efforts. The wide price gap thus created can be exploited by illicit sellers, if they are able to obtain drugs at their actual production cost. This commonly occurs, both legally and illegally in circumstances where prices differ in jurisdictions which are adjacent or between which good channels are available for shipping the drugs once they have been ordered and paid for electronically. For example, drug prices are lower in Canada than in the United States, and one source has estimated the trade from Canadian pharmacies to U.S. customers at about $650 million each year.[3]

Depending upon applicable laws, some of this commerce may be legal, but sales directly across international borders generally violate import taxation requirements, and may also raise public-health concerns. The effectiveness of safeguards such as prescription requirements, which normally consider individual concerns such as side-effects and reactions with other drugs a patient is taking, and more general restrictions on unproven remedies is greatly reduced.[4] For example, a thriving black-market exists for Viagra and similar drugs, which are controlled by prescription in some jurisdictions due to side-effects and possible harmful interactions with other drugs and are made expensive by the proprietary licensing fees charged to manufacturers.

Quality control is also an issue. The drugs sold under established brand names may be cheaper generic versions from places where their manufacture is permitted, or even substances which are not drugs at all.[5] Even where trafficking is not a crime, established consumer-protection and licensing legislation may not adequately regulate the activities, a problem common to electronic commerce in general. Amendments may be needed for

[1] Numerous examples of this can be found on-line. Objets d'art and antiquities from individual thefts and looting during and after World War II and other conflicts have been trafficked on-line, and recent concerns have been expressed about the potential sale of items stolen from Iraqi museums, both during the Hussein regime and the conflict which ended it in March and April of 2003. Museum associations, law enforcement agencies and at least two government agencies (the Egyptian Ministry of Antiquities and the U.S. Department of State) maintain websites at which looted and stolen objects are catalogued. These are triggered by on-line search engines, making it less likely that a potential purchaser seeking an item would purchase one without being aware of its illicit provenance. Another recent example of the sale of illicit collectors' items was the attempted sale of debris from the break-up of the space shuttle Columbia on re-entry in February 2003. Officials, concerned about the loss of evidence needed to establish the reason for the loss, acted quickly to claim the debris as government property, and some criminal charges were brought after items were purchased through on-line auction sites by undercover officers.

[2] INCB 2001, paragraphs 19-26.

[3] IMS Health Ltd. of the United States, cited in Harris, G. "Canada Fills U.S. Prescriptions Under the Counter", New York Times, 4 June 2003. Canadian law provides for more limited patent and other protections, which reduces revenues to producers for research and development, but results in lower consumer prices.

[4] Cantrell, 2001 and B.Williams, 2001.

[5] See B.Williams 2001, at pp.153-56. Other drugs seen as problematic due to demand or risk factors included diet drugs, prescription amphetamines, and anabolic steroids.

example, to clarify whether protective measures are a matter for the legislative jurisdiction of the vendor or purchaser. At the same time, proponents of on-line transactions argue that customers in need of health-care products should have the right to shop for the lowest prices and that the use of the Internet facilitates this,[1] a controversy which is likely to be exacerbated by the demands of interest groups and some governments that generic, non-profit treatments be made available for illnesses such as HIV-AIDS.[2]

(ii) Firearms, small-arms and other weaponry

On-line trafficking in small arms, firearms and other weaponry is also seen as a problem, both for national and regional security in conflict regions,[3] and in terms of domestic crime control or gun-control regimes.[4] In both cases, the major concern is that the lack of personal contact between vendor and purchaser reduces surveillance and provides opportunities for the acquisition of firearms by recipients who would otherwise be caught by applicable legal restrictions intended to screen out known offenders and other high-risk cases. A related problem is that the use of Internet transactions for ordering and payment and postal or other delivery of the actual firearm makes it more difficult to trace the gun or establish the identity of the recipient if the weapon is later used to commit a crime.[5] The same factors which contribute to on-line trafficking in firearms may also contribute to trafficking in more sinister commodities such as illicit nuclear materials and chemical or biological weapons or their precursors. Numerous web-sites and anonymous postings appear to offer substances such as enriched uranium or plutonium for sale, but few if any of these appear to be credible. Some actual trafficking of these substances has occurred, however, and the potential for secure on-line communications as a means of matching buyers and sellers is obvious.[6] Some trafficking in conventional explosives or explosive precursor chemicals may also occur, although as discussed above, the greater concern in this area appears to lie with trafficking in intangible technical information needed to produce explosives from chemicals which are so common that there would be no point in trafficking them on-line.

(iii) Other tangible commodities

Tobacco is legally available in most countries, and the incentive to purchase and sell it illicitly is primarily rooted in the high taxes levied by some governments. Enormous illicit profits can be made by smuggling tobacco products from low-tax to high-tax

[1] Harris, G. "Canada Fills U.S. Prescriptions Under the Counter", New York Times, 4 June 2003.

[2] Pressure to make anti-viral and other drugs for the treatment of HIV-AIDS available at low cost to developing countries peaked in 2002 with litigation in South Africa challenging producers' patent rights and with a series of trade disputes between the companies and host governments – particularly the U.S. – which sought to protect patent rights. The litigation was ultimately abandoned by producers and the preferred solution to the trade issues seems to be that patents would be protected on the basis that low cost drugs would either be provided or licensed by the major producers. See BBC News, "AIDS drug trade dispute ends", September 18, 1999, http://news.bbc.co.uk/2/hi/africa/450942.stm and CNN, "Generic AIDS drugs imported into South Africa, despite ban", 29 January 2002, http://www.cnn.com/2002/HEALTH/conditions/01/29/safrica.aids.patents/.

[3] See Angola 2000, paragraph 9, footnote 4. See also Wintour, P. "Internet arms dealers face curbs" , The Guardian, 6 December 2000, on-line at http://www.guardian.co.uk/ internetnews/story/0,7369,407424,00.html, downloaded 22-10-02.

[4] Both the United States and Japan have engaged in the preparation of legislation to control gun sales arranged on-line. See "Lawmaker proposal would regulate Internet gun sales" CNN.com, April 26 1999, discussing companion bills placed before the US Senate (Sen. C. Schumer, S.637 The Internet Gun Trafficking Act of 1999) and House of Representatives (Rep.B. Rush, HR 1245, The Internet Gun Trafficking Act of 1999) on 16 March 1999. Both bills remain before legislative committees and have not become law. The Government of Japan announced plans to develop legislation to crack down on the use of the Internet for firearm trading in 2003: see "Government to step up crackdown on Internet trading of firearms", Kyodo News Service, 24 April 2003, on-line at: http://www.japantoday.com/e/?content=news&cat=2&page=2.

[5] See: Knapp, D., "Point, click…buy a gun?, CNN on-line, 29 April 1999, http://www.cnn.com/US/9904/29/on-line.gun.sales/, "Lawmaker proposal would regulate Internet gun sales, CNN on-line, 26 April 1999, http://www.cnn.com/TECH/computing/9904/26/gun.internet/, and Hillebrand, M., "Congress Looks to Slow Internet Gun Sales", E-Commerce Times, 8 June 1999, http://www.ecommercetimes.com/perl/story/600.html.

[6] Robitaille, A. "Smuggling special nuclear materials", CSIS Commentary #57, Canadian Security Intelligence Service, May 1995, available on-line at: http://www.csis-scrs.gc.ca/eng/comment/com57_e.html.

jurisdictions, and at least one major tobacco manufacturer has been implicated in collusion with smugglers.[1] Essentially the allegations in these cases is that major tobacco companies have conspired or collaborated with smugglers by selling large quantities of cigarettes into low-tax jurisdictions at above-market prices, with the tobacco then being smuggled into higher-tax jurisdictions and sold at a profit. The role of information and communications technologies in this trade is probably much the same as for other tangibles such as narcotic drugs, although in one particular trade it has assumed a larger role. Federal law in the United States makes it illegal to import or trade in products of Cuban origin as part of that country's economic embargo on Cuba, and a thriving on-line trade in which U.S. residents order Cuban cigars on-line from foreign vendors has arisen as a result.[2] Another illicit tangible commodity trafficked on-line is endangered species and other exotic animals and their products. In this case, the Internet is used to identify and link purchasers with animals, and in some cases to create false records to the effect that the animals have been bred in captivity.[3]

III. The smuggling and trafficking of human beings

Slavery and other conduct in which human beings are treated as a commodity are a very old problem which has become much more serious as a result of globalisation and technological advances. Trafficking in human beings, in which individuals are recruited, transported elsewhere and exploited in illegal activities such as prostitution and child pornography or child-labour, and the smuggling of migrants, in which illegal entry or illegal residence is procured for a fee, have become major sources of revenue for transnational organised crime. In 2000, the international community responded by adopting a series of treaties which require States Parties to criminalize smuggling, trafficking and related activities, and to cooperate with one another in prevention, investigation, prosecution and other matters.[4]

In many ways, information and communications technologies can be used to smuggle or traffic human beings in the same way as for any other tangible commodities. Computer equipment can be used in the forgery of passports, visas, work permits and similar documents, and e-mail or other telecommunications media can be used to arrange the arrival and concealment of trafficking victims.

The use of the Internet to facilitate sex tourism contributes to trafficking regardless of whether the victims are moved to the travel destinations or not. In an effort to combat the problem, some countries have criminalized travelling abroad for the purpose of having sex with children[5] and concerns have been expressed that, as the risk to offenders who travel

[1] "Cigarette smuggling costs £4bn", BBC News on-line 27 November 2000, http://news.bbc.co.uk/1/hi/business/1042842.stm. The involvement of companies in collusion with smugglers has been clearly established in the case of smuggling across the United-States/Canada border in the 1990's when senior employees of one company pleaded guilty smuggling-related charges. Canadian efforts to pursue the lost revenues, estimated in the hundreds of millions of dollars, were unsuccessful when U.S. courts declined to enforce Canadian fiscal legislation. Subsequently, similar activity was uncovered in Europe, prompting action by the European Union. See ËU to sue US tobacco companies on cigarette smuggling allegations", Financial Times (London) 21 July 2000, and "Europeans suing big tobacco in US", New York Times, 7 November 2000.

[2] Karp, J., "Smuggling Stogies Online" TechTV On-line, 9 July 2002, http://www.techtv.com/cybercrime/viceonline/story/0,23008, 33376772,00.html, downloaded 22-10-02.

[3] Hall, K., "Beastly crimes: Smuggling exotic animals is a billion-dollar industry" , Seattle Times, 6 August 2001, posted on-line at: http://seattletimes.nwsource.com/html/nationworld/134330071_exotic16.html, downloaded 22-10-02.

[4] See UN Convention against Transnational Organised Crime and the Protocols thereto, GA/RES/55/25, annexes. The instruments were adopted by the General Assembly on 15 November 2000. The Convention entered into force on 29 September 2003.

[5] The United States, for example, has made it a domestic crime to travel abroad for the purposes of having sex with children. See 18 U.S.C. § 2423(b). Canada, on the other hand, has extended the application of domestic crimes relating to a range of offences involving sexual activities with children to cases where the act is committed abroad by any person who is a Canadian citizen or permanent resident. See S.C.1997 c.16, enacting *Criminal Code* s.7, subs. (4.1). More recently, Canada has also empowered any court which convicts an

increases, incentives may be created to traffic the children back into offender jurisdictions in what is described as "reverse sex-tourism".[1]

As human beings, the trafficking victims are exposed to broadcast media, the Internet and other means of communication, and by influencing their conduct, these media can also influence trafficking. The exact effects, however, and whether they contribute to trafficking or the prevention or suppression of trafficking, depend on what information is imparted and how.

A major common factor cited by most experts on trafficking in persons is the desire of potential migrants or trafficking victims to migrate. Usually this involves some combination of what are sometimes described as "push" and "pull" factors. Unpleasant conditions, such as poverty, conflict or oppression in the source country, the expectation that circumstances will be better in the proposed destination country, and the availability of some means of transport from one to the other generally combine to produce both the smuggling of migrants and trafficking in persons. In the former, smugglers simply respond to the desire to migrate by smuggling migrants from one country to another for a substantial fee and often at considerable risk to the migrants. In the latter, traffickers use the desire to improve economic conditions to gain control of victims using first deception, and then later more coercive methods once the victims have been transported away from families and other support structures with which they are familiar.

In both scenarios, both "push" and "pull" factors are almost certainly influenced by information imparted by the mass-media, and the penetration of broadcast media and the Internet into developing countries is probably a significant factor influencing both rates of occurrence and the patterns of source, transit and destination. Where local conditions are unpleasant or dangerous, the depiction of a better life abroad sends a powerful message. This may not necessarily even be accurate: fictional media in particular tend to portray life in Europe, the United States and other destinations of choice in a better light than the reality of the day-to-day conditions that will actually face new immigrants when they arrive.

This same mechanism can also be used to prevent or suppress trafficking in persons and the smuggling of migrants, however. Most trafficking includes some element of deception, and this process can be disrupted by targeting population groups seen as vulnerable to trafficking with information about the reality of life abroad and the criminal nature of traffickers, as well as the risks of becoming victims of trafficking. Persons seeking to migrate illegally can also be targetted with information about the risks faced in the course of smuggling and with accurate information about destination countries.[2]

The trafficking in human beings for purposes of prostitution and various forms of forced or coerced labour are believed to be most common forms of activities, but the definition of trafficking includes other variations which may also be influenced by information and communications technologies. The definition also includes the giving or

offender of any offences involving child sex to use the Internet to communicate with children (S.C. 2002, c.13, amending *Criminal Code* s.161, subpara.(1)(c).

[1] Benneto, J. "Paedophiles Predicted to Turn to Child Trafficking", Independent, 29 July, 2002. The author cites a report of the Metropolitan Police vice squad, which has not been published. This pattern of reverse sex tourism might arise in the future, but is not likely to become common at present because as a general rule, the risk of detection, prosecution and punishment remains far higher in the developed countries where paedophiles reside than in the developing countries where the victims reside.

[2] See UN Convention against Transnational Organized Crime, Art.31, paras. (5) and (7) and Protocol to prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Art.9, paras.(2), (4) and (5). These call for both public-information campaigns and the alleviation of harsh living conditions as a means of preventing trafficking.

receiving or payments to achieve the consent of a person having custody over the victim, which would include the purchase and sale of children or the custody of children in adoption cases as well as some cases of arranged marriage, where one of the parties to the marriage did not consent or lacked the capacity to consent due to age or disability.

The proliferation of Internet adoption agencies makes it possible for parties to make covert financial arrangements and actually exchange money through channels which authorities responsible for child-welfare, immigration and other safeguards will find it difficult to monitor. The potential problems are illustrated by one 2001 case in which a parent in the U.S. offered two young girls for adoption, accepted large fees from at least two sets of adoptive parents in the U.K., and finally transferred the children to the highest bidder, triggering civil lawsuits and custody claims from both families in the U.K., as well as the children's father in the U.S.A. The mother was also subsequently prosecuted for fraud when it emerged that she had continued to claim welfare benefits in respect of the children after they had been transferred to the U.K.[1]

Conclusion

The influence of information and communications technologies on the illicit smuggling and trafficking of commodities are as pervasive and complex as they are for parallel legitimate activities. This poses a number of challenges, both for the public sector, which is charged with regulating legal commerce and with suppressing illegal commerce, and for the private sector which develops, markets and uses the technologies. As the experience with cryptography illustrates, technology-based controls are often impracticable because any measure which suppresses illicit activities has more or less the same effect on legitimate ones. Moreover, the benefits of the legitimate activities are in most cases so great as to generate costs far in excess of any benefits in such cases.

At the same time, both the direct costs of crime and the indirect costs associated with the fear of crime have emerged as significant factors which must be taken into account, not only in regulating the technologies, but in developing and marketing them as well. The search is now on for ways to incorporate effective crime-control into new products in ways which will increase their market value, or at a minimum, not decrease such value. Increasingly, standard-setting which transcends national technological boundaries will be needed to ensure that this can be done while maintaining viable competition between products and the industries which produce, market and use them. A central factor in this debate is the need to strike an appropriate balance between the need to protect the privacy of personal and commercial communications and stored data, and the need to ensure that illicit activities can be detected, investigated and prosecuted, and where possible, prevented or suppressed by the technologies themselves.

A further significant challenge is the pace of change. The nature and scope of all of the forms of illicit smuggling and trafficking in which the technologies play a significant role is determined in part by the evolution, availability and capacity of the technologies and the balance between opportunities and risks presented to potential offenders. New technologies are quickly taken up by offenders and put to use in ways which are sometimes unpredictable. This occurs at a rate which has become difficult for legislators and law

[1] See BBC News, "Internet adoption laws tightened", 30 April 2001, Adoption and the Internet, 17 January 2001, and "Complex legal battle ahead", http://news.bbc.co.uk/2/hi/uk_news/1304125.stm. Eventually, the biological father prevailed in a U.S. custody battle between him and the two families which had paid to adopt the children.

enforcement agencies to match even in the most affluent and technically-sophisticated countries. Developing countries face an even more daunting challenge.

Perhaps the ultimate challenge, however, is that of universality. With offences committed using the new technologies, offenders need no longer be physically present in a country to commit a crime there or victimise its residents. This means that the problems of any country have now become the problems of every country. What is true in theory for the effects of globalisation on crime becomes a matter of very hard practical reality where technology-related crimes are concerned. Legislative and enforcement measures applied in only one country will simply displace offenders to another. This can be done electronically, and without actual movement of the offender or any change in the locations of the victims targeted. Intangible or virtual goods in particular can be "stored" in or trafficked from any jurisdiction which lacks the technical capability to prevent this. In this environment, only a truly global approach and widespread, if not universal, consensus will generate policies which are economically and socially just, maximise the benefits of the technologies, and are truly effective in preventing and suppressing smuggling, trafficking and other illicit activities.

4. The Logistics of Trafficking

IMO Activities to Enhance Maritime Security

J C ADDISON MBE
On behalf of Captain H.G. Hesse[*]
Deputy Director, Head, Navigational Safety and Maritime Security Section Maritime Safety Division

History

In the aftermath of the Achille Lauro incident in October 1985, the fourteenth session of the International Maritime Organization (IMO) Assembly, in November of that year, adopted resolution A.584(14) on Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews. That resolution noted "with great concern the danger to passengers and crews resulting from the increasing number of incidents involving piracy, armed robbery and other unlawful acts against or on board ships, including small craft, both at anchor and under way".

Through that resolution, the Assembly requested the Maritime Safety Committee (MSC) to develop detailed and practical technical measures to ensure the security of passengers and crews on board ships. In doing so, the MSC was instructed to take into account the work of the International Civil Aviation Organization (ICAO) *vis-à-vis* standards and recommended practices for airport and aircraft security.

Following that meeting of the IMO Assembly, the United Nations General Assembly, in December 1985, called upon IMO "to study the problem of terrorism aboard or against ships with a view to making recommendations on appropriate measures".

Measures to prevent unlawful acts against passengers and crew on board ships (MSC/Circ.443)

Pursuant to the aforementioned request of the Assembly, the MSC, at its fifty-third session in September 1986, approved MSC/Circ.443 on "Measures to prevent unlawful acts against passengers and crew on board ships", for application on passenger ships engaged in international voyages of 24 hours or more and the port facilities which service them. The circular recommends that Governments, port authorities, administrations, shipowners, shipmasters and crews should take appropriate measures to prevent unlawful acts which may threaten passengers and crews; stresses the need for port facilities and individual ships to have a security plan and appoint a security officer; describes in detail the way in which security surveys should be conducted and the security measures and procedures which should be adopted; and addresses security training. It is interesting to note the list of issues addressed in this sixteen-year-old recommendation that applies only to passenger ships, and the list of issues being considered for incorporation in the new mandatory provisions that will apply to all types of ships.

SUA Convention and Protocol

[*] Views expressed in this paper are those of the author and should not be construed as necessarily reflecting in any way the policies or views of IMO or its Secretariat.

In November 1986, the Governments of Austria, Egypt and Italy proposed that the IMO should prepare a convention on the subject of unlawful acts against the safety of maritime navigation. The three Governments submitted the draft text of such a convention providing comprehensive requirements for the suppression of unlawful acts committed against the safety of maritime navigation which endanger innocent human lives; jeopardize the safety of persons and property; seriously affect the operation of maritime services and, thus, are of grave concern to the international community as a whole

Following elaboration of the draft convention by the Organization's Legal Committee, IMO convened, in March 1988, a conference in Rome, which adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA). Together with the SUA Convention, the Rome Conference adopted a protocol which extends the provisions of the Convention to unlawful acts against fixed platforms located on the Continental Shelf (Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, 1988). The two instruments entered into force on 1 March 1992.

The main purpose of the SUA treaties is to ensure that appropriate action is taken against persons committing unlawful acts against ships (and fixed platforms on the Continental Shelf). In this context, unlawful acts include the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. The treaties include provisions for the absolute and unconditional application of the principle either to punish or to extradite persons who commit or have allegedly committed offences specified in the Convention.

Passenger ferry security (MSC/Circ.754)

At the initiative of the Government of the United Kingdom, the MSC, at its sixty-sixth session in May/June 1996, approved MSC/Circ.754 on Passenger ferry security, providing a set of recommendations on security measures for passenger ferries on international voyages shorter than 24 hours; and ports.

Other security-related instruments

The Assembly, at its twentieth session (17 to 27 November 1997), adopted resolution A.871(20) on Guidelines on the allocation of responsibilities to seek the successful resolution of stowaway cases; and resolution A.872(20) on Guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic. These instruments had been developed by the Facilitation Committee at its twenty-fifth session, and both address, to some extent, security measures on board ships and in ports.

Recent Activities at the IMO since 11 September 2001

In the wake of the tragic events of 11 September 2001 in the United States of America, IMO Secretary-General William A. O'Neil consulted Member Governments on the need to review the measures already adopted by IMO to combat acts of violence and crime at sea. Thereafter, he proposed the adoption of a resolution on the "Review of measures and procedures to prevent acts of terrorism which threaten the security of

passengers and crews and the safety of ships". This resolution was subsequently adopted as resolution A.924 at the 22nd IMO Assembly – A.924(22) - in November 2001.

Resolution A.924(22) calls for a review of the existing international legal and technical measures to prevent and suppress terrorist acts against ships at sea and in port, and to improve security aboard and ashore. The aim is to reduce risks to passengers, crews and port personnel on board ships and in port areas and to the vessels and their cargoes, and to enhance ship and port security and avert shipping from becoming a target of international terrorism. The Assembly also agreed to a significant boost to the organization's technical co-operation programme of £1.5 million, to help developing countries address maritime security issues.

Pursuant to the adoption of resolution A.924(22), the IMO Secretariat has been restructured in order to ensure a systematic and consistent approach to maritime security issues. The Navigation Section of the Maritime Safety Division (MSD) has been re-designated as the Navigational Safety and Maritime Security Section. In addition to its traditional duties concerning the work of the Sub-Committees on Safety of Navigation (NAV) and on Radiocommunications and Search and Rescue (COMSAR), the new section will be responsible for regulatory matters relating to the prevention and suppression of acts of terrorism against shipping. It will continue to bear responsibility for matters relating to piracy and armed robbery against ships and will assist the Technical Co-operation Division to deliver technical co-operation projects relevant to maritime security.

At an extraordinary meeting of the MSC that was held concurrently with the twenty-second session of the Assembly, it was agreed to establish an Intersessional Working Group on Maritime Security (ISWG). This Group first met in February 2002 and again in September 2002. The Working Group also met during MSC 75 in May 2002.

Progress to Date

Noting that final agreement on any new measures would not be reached until the conclusion of the Diplomatic Conference on Maritime Security in December 2002, the following provides a brief summary of progress on a number of the important issues under consideration and which are considered to be particularly relevant to the Courmayeur Conference.

General

1. International Convention for the Safety of Life at Sea(SOLAS) chapter XI will be amended to include special measures for maritime security. Specifically, SOLAS Chapter XI will be divided into two parts: Chapter XI-1: Special Measures to Enhance Maritime Safety; and Chapter XI-2: Special Measures to Enhance Maritime Security. In principle chapter XI-2 will incorporate new regulations regarding definitions and the requirements for ships and port facilities. These regulations will be supported by a draft International Code for the Security of Ships and Port Facilities (ISPS Code) which will have a mandatory section (Part A) and a recommendatory section (Part B). The framework of the draft mandatory requirements for inclusion in SOLAS chapter XI-2 and Part A of the draft ISPS Code are set out in annex 1. The guidance given in Part B of the ISPS Code will be taken into account when implementing the SOLAS XI-2 regulations and the

provisions of Part A. However, it is recognised that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the Port Facilities visited by the ship. Similarly, in relation to the guidance on Port Facilities, the extent to which this guidance applies will depend on the types off cargoes and/or passengers and the trading patterns of visiting vessels. In principle, the new requirements will be applicable to Mobile Offshore Drilling Units (MODUs) in transit and in port and will not apply to fixed and floating platforms and MODUs on site.

2. Under SOLAS chapter XI-2 and Part A of the Code *Contracting Governments* can establish *Designated Authorities* within Government to undertake their security responsibilities under the Code. Governments or Designated Authorities may also delegate the undertaking of certain responsibilities to *Recognised Security Organizations* outside Government.

3. The setting of the *security level* applying at any particular time will be the responsibility of Contracting Governments and will apply to their ships and Port Facilities. The Code defines three security levels for international use:

    - *Security Level 1*, normal;
    - *Security Level 2*, lasting for the period of time when there is a heightened risk of a *security incident*; and
    - *Security Level 3,* lasting for the period of time when there is the probable or imminent risk of a security incident.

4. SOLAS chapter XI-2 and the ISPS Code will require certain *information* to be provided to the IMO and information to be made available to allow effective communication between Company/Ship Security Officers and the Port Facility Security Officers responsible for the Port Facility their ships serve.

The Company and the Ship

5. Any shipping company operating ships to which the Code applies will have to appoint a *Company Security Officer (CSO)* for the company and a *Ship Security Officer (SSO)* for each of its ships. The responsibilities of these officers are defined, as are the requirements for their training and drills. The training needs and requirements of the SSO will be developed in the context of the STCW Convention and as a matter of urgency by the Sub-Committee on the Standards of Training and Watchkeeping (STW) which will next meet in February 2003. The CSO's responsibilities include ensuring that a *Ship Security Assessment* is undertaken and that a *Ship Security Plan* is prepared for each ship to which the Code applies.

6. The *Ship Security Plan* will indicate the operational and physical security measures the ship shall take to ensure it always operates at security level 1. The Plan will also indicate the additional, or intensified, security measures the ship itself can take to move to security level 2. Furthermore, the Plan will indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by the Authorities responding at security level 3 to a security incident or threat. The need for these plans to be ultimately incorporated in the ISM Code has been acknowledged. The Ship Security Plan has to be approved

by, or on behalf of, the ship's Administration. The Company and Ship Security Officer will be required to monitor the continuing relevance and effectiveness of the Plan, including the undertaking of independent internal audits. Any amendments to specified elements of an approved Plan will have to be resubmitted for approval.

7. The ISPS Code includes provisions relating to the verification and certification of the ship's adherence to the requirements of the Code on an initial, renewal and intermediate basis. The ship will have to carry an *International Ship Security Certificate (ISSC)* indicating that it complies with the Code. The ISSC will be subject to *Port State Control* (PSC) inspections but such inspections will not extend to examination of the Ship Security Plan itself. The ship may be subject to additional control measures if there is reason to believe that the security of the ship has, or the port facilities it has served have, been compromised. The ship may be required to provide information regarding the ship, its cargo, passengers and crew prior to port entry and it is the responsibility of the company that up to date information relating to the ownership and control of the vessel is available on board. There may be circumstances in which entry into port could be denied. The issue of Control is one of the most important issues where there are significant elements that remain to be resolved December 2002.

8. The implementation of the mandatory fitting of *Automatic Identification Systems* (AIS) for all ships of 500 gross tonnage and above, on international voyages. Four alternative texts for different entry into force dates for amendments to Regulation 19 of SOLAS Chapter V have been developed together with a definition of first safety equipment survey, linked to the alternatives in which the term is used. The final decision on which alternative is selected will be for the Conference to make in December 2002.

9. The MSC has instructed the Sub-Committees on Radiocommunications and Search and Rescue (COMSAR), Ship Design and Equipment (DE) and Safety of Navigation (NAV) to consider the details of an *alert system* for seafarers to use to notify authorities and other ships of a terrorist hijacking. The requirements for ships to be provided with such systems are detailed in a new regulation in SOLAS chapter XI-2. The COMSAR and DE Sub-Committees have already started work on these details.

10. The DE Sub-Committee has considered the issue of *maritime security equipment and measures* to prevent unauthorised boarding in ports and at sea and report to MSC 75. It is recognised that the type of equipment to be used on board would depend largely on risk assessment (e.g. ship types, trading areas). The section of the ISPS Code that addresses the Ship Security Plan will include consideration of such equipment and measures.

11. It is recognised that urgent action on an up-to-date *seafarer identification document* is needed. The Secretary-General of the IMO wrote to the Director-General of the International Labour Organization (ILO), emphasising the importance that Member States of IMO give to updating the ILO seafarer identification document as a significant contribution to enhanced maritime security, and requesting early action on this matter. The Secretary-General offered the assistance of IMO in this process. The ILO Director-General brought this matter to the attention of his governing body in March 2002, which agreed that a new protocol to amend the ILO Seafarers'

Identity Documents Convention of 1958 (No. 108) be developed expeditiously for adoption by the ILO General Conference in June 2003.

The Port Facility

12. Each Contracting Government will have to undertake a *Port Facility Security Assessment* of its Port Facilities. This Assessment will be undertaken by the Contracting Government, a Designated Authority, or a Recognised Security Organization. Port Facility Security Assessments will need to be reviewed over time. The results of the Port Facility Security Assessment have to be approved by the Government or Designated Authority and will be used to help determine which Port Facilities are required to appoint a *Port Facility Security Officer.*

13. The responsibilities of the *Port Facility Security Officers* are defined in the ISPS Code, as are the requirements for the training they require and the drills they will be responsible for undertaking. The Port Facility Security Officer is responsible for the preparation of the *Port Facility Security Plan*.

14. Like the Ship Security Plan, the *Port Facility Security Plan* shall indicate the operational and physical security measures the Port Facility shall take to ensure that it always operates at security level 1. The Plan should also indicate the additional, or intensified, security measures the Port Facility can take to move to security level 2. Furthermore the Plan should indicate the possible preparatory actions the Port Facility could take to allow prompt response to the instructions that may be issued by the Authorities responding at security level 3 to a security incident or threat. The MSC has decided that more detailed work needs to be undertaken in close co-operation with ILO on comprehensive Port Facility Security Plan requirements. There has been concern that it may not be appropriate to require such plans for small ports. This matter is still under discussion.

15. The Port Facility Security Plan has to be approved by, or on behalf of, the port facility's Contracting Government. The Port Facility Security Officer shall implement its provisions and monitor the continuing effectiveness and relevance of the approved Plan, including commissioning independent internal audits of the application of the Plan. The effectiveness of the Plan can be tested by the relevant Authorities. The Port Facility Security Assessment covering the Port Facility may also be reviewed. All these activities may lead to amendments to the approved Plan. Major amendments to an approved Plan will have to be submitted to the approving Authority for re-approval.

The Rationale behind the News Requirements

In essence, the new SOLAS chapter XI-2 and the ISPS Code take the approach that ensuring the security of ships and port facilities is basically a risk management activity and that to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. The purpose of the ISPS Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat levels with changes in vulnerability for ships and port facilities.

This risk management concept will be embodied in the ISPS Code through a number of minimum functional security requirements for ships and port facilities. For ships, such requirements will include:

.1 ship security plans;
.2 ship security officers;
.3 company security officers; and
.4 certain onboard equipment.

For port facilities, the requirements will include:

.1 port facility security plans; and
.2 .port facility security officers

In addition the requirements for ships and for port facilities will include:

.1 monitoring and controlling access;
.2 monitoring the activities of people and cargo; and
.3 ensuring that security communications are readily available.

To ensure implementation of all these new requirements, training and drills will obviously play an important role.

Conference Resolutions

A number of other longer-term maritime security-related issues have also been raised during recent discussions in the IMO. As a result, nine draft Conference resolutions have been drafted, which, *inter alia*, address:

.1 establishment of appropriate measures to enhance the security of ships, port facilities and fixed and floating platforms not covered by the new SOLAS chapter XI-2;
.2 co-operation and further work with the International Labour Organization (ILO); and
.3 co-operation with the World Customs Organization (WCO).

Future Developments

The Diplomatic Conference on Maritime Security for the adoption of draft SOLAS chapter XI-2 and the draft ISPS Code is scheduled to meet concurrently with the second week of MSC 76 (2 to 13 December 2002) from 9 to 13 December 2002. Aside from the provisions in the SOLAS chapter XI-2 and the ISPS Code, work is underway on revisions to the SOLAS Convention that would address requirements for long-range tracking and identification systems and ship security alert systems to be carried aboard ships.

ANNEX 1

Draft SOLAS Chapter XI-2

SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

DRAFT INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND PORT FACILITIES

Part A

Mandatory requirements regarding the provisions of Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended

1. Introduction

   - Objectives

   - Functional Requirements

2. Definitions

3. Application

4. Responsibilities of Contracting Governments

5. Declaration of Security

6. Obligations of the Company

7. Ship Security

8. Ship Security Assessment

9. Ship Security Plan

10. Records

11. Company Security Officer

12. Ship Security Officer

13. Training and Drills

14. Port Facility Security

15. Port Facility Security Assessment

16. Port Facility Security Plan

17. Port Facility Security Officer

18. Training and Drills

19. Survey and certification

- Surveys
- Issue and endorsement of Certificate
- Duration and validity of Certificate
- Appendix to Part A (certificate formats)

Boats, Planes, Trains and Automobiles: Logistics of the Trafficking Market

NEIL BAILEY
International Division, National Criminal Intelligence Service, United Kingdom

Although the subject of this panel is logistics of trafficking, covering trafficking in every commodity would require much more thorough presentation, so this paper is concentrated on drugs. However, much of its content apply to all commodities.

American dictionaries describe logistics as "the procurement, distribution, maintenance and replacement of material." That definition applies just as much to the legal trade as to trafficking in illegal commodities.

One characteristic commodity by which I would like to begin is cocaine. The logistics element of the cocaine trade is absolutely vital. In order to get that product to market from where the coca leaf is grown, people have to move it thousands of miles. One related, but very important element, which will be illustrated further below, is that the trade in any illegal trafficking is always profit driven.

If we compare the illicit supplies of cocaine with many legitimate commodities which are moved around the world again for profit but quite legitimately, cocaine dominates in terms of tonnage. As far as the United Kingdom is concerned, we think that the cocaine market is worth approximately 40 tons. We are capturing perhaps just over two tons. The situation is similar for opiates.

To demonstrate the volume of commodities having moved around the world and the difficulties faced by law enforcement authorities, I have chosen one example from the United Kingdom, which is the Port of Dover. It is the tenth largest port in the United Kingdom. For the year 2000, over 16 million passengers, over 2,7 million cars and 1,6 million freight vehicles passed through that port. That is equal to 52,000 lorries every month.

With these sorts of quantities moving through just one of the ports in the UK, the reality is that the enforcement agencies, whether customs, border guards, or police, cannot hope to stop every single vehicle, person or car coming across borders such as that. So it is quite obvious that trying to control the trade in the trafficking of illicit substances - drugs or people (a huge problem now all across Europe) is a formidable challenge.

Why do people traffic in cocaine, heroin or people all across the world? Based on United Nations statistics, the farm gate growing price for cocaine is about £700 per kilo. The street value of cocaine in £65 a gram. In other words, £1 at the farm gate is £93 when the commodity finally gets to the market for which it is intended. A profit like that is a very powerful incentive for trafficking.

The profit is even greater in heroin. An investment of £1 in Afghanistan becomes £350 on the streets of the European Union. Profit drives the movement of perfectly legitimate commodities around the world as well. However, no manufacturer, distributor, wholesaler or retailer can expect a profit margin of 350 times.

Is law enforcement effective against trafficking not just in drugs but in anything? One of the biggest traffickers in the last twenty or thirty years was Howard Marks. There are three books about Marks: one called "The life and high time of Howard Marks" written over twenty years ago; another entitled "The Hunting of Marco Polo", written by an American law enforcement agent; and the book that most people have heard of and that was at the top of the best sellers' list in some countries for some time, which is called "Mr. Nice". The author of "Mr. Nice" is Mr. Marks himself.

The point Howard Marks makes in that book is very important. Enforcement agencies lack the expertise and professionalism to conduct international operations. There are too many egos and jurisdictions to foster the proper climate of co-operation. While we would like to believe that this is not true, a look at the career of Howard Marks shows that the point may have merits. Howard Marks moved vast quantities of cannabis all around the world for almost a quarter of a century, made a lot of money, and had an incredible life-style. Eventually he went to prison in America for a few years but now he is back with an equally pleasant life-style. Probably if enforcement agencies had been better, had shown greater expertise and professionalism, and shared information amongst them, they would have been better able to deal with Howard Marks many years before.

The following is a comment from a review of "Mr. Nice", when it was produced: "As Howard became more proficient at organising this smuggling of hashish, he started to be able to trade in knowledge of the transport industry. The knowledge of who can be paid off at the correct time and place." The issue is as current now as it was then. The illicit market, be it in drugs or in any other illicit commodity, depends on the legitimate free trade routes around the world. You would not bring, for example, heroin from Afghanistan to Western Europe without a legitimate trade of heavy lorry vehicles travelling from south-west Asia right across what is now called the "Balkan Route" to Europe carrying legitimate consignments of goods that all expect to see in the Western consumer markets.

The first thing to make clear is that the logistics of drug trafficking are comparatively straight-forward. The product is offered at low cost at origin and has a high retail value when it gets to its markets. Therefore, those involved in the logistics of moving that commodity from one place to the other are not in quite the same situation as people moving legitimate consignment goods, where a few pence on an invoice for transport make a difference to whether there is profit at the end of the day.

Let me offer an example: there is a large supermarket chain in the United Kingdom that has started recently to open supermarkets in Central and Eastern Europe. A lot of the products on sale in Central and Eastern Europe are shipped often from the UK by a variety of companies that compete for contracts. The competition is so fierce that a difference of £20 on a shipping contract for one month makes the difference getting the contract.

The profit margins in drugs that were cited earlier means that those involved in the logistics of trafficking are not worried about whether the price they are paying for one part of the journey is £20 or more. The profit is so large that they can afford to be quite generous in the payments they make to people along the trafficking route.

Another example which concerns us greatly at the moment in Western Europe is trafficking in people. Most of the big drug traffickers, including Howard Marks, have actually been dealt with eventually because law enforcement agencies know about them and about what they are doing, and cooperate in trying to catch them. The reason for that is

because the commodity that comes to Western Europe has to go somewhere, so law enforcement agencies are able very often to trace back the commodities to its origin and work for the future on similar consignments. That applies to drugs that are seen on the streets in any big city. Law enforcement agencies always try to work back and find out where the drugs are coming from and who transported them. With people trafficking it's significantly different. The people are treated as a commodity, are pushed into the back of lorries under consignments of consumer goods, and in some cases get through more than twenty border crossings before they reach the final country of destination. And when they are pushed out of the lorry they disappear in the community in that country, making it virtually impossible to trace back. Most of the illegal immigrants, even if one would find them and ask them, they would not be able to provide much information. They would merely say that it was dark, and they were put into the back of the lorry in some country at the other side of Europe. It was dark when they were taken out of the lorry somewhere in the United Kingdom or in Western Europe.

Some of the things law enforcement agencies can do to have an impact on that trade are the same for people as for drugs or any other illegal commodity. One very important point, on which I will be reverting, is looking at the legitimacy of the transport route. That is being done particularly by customs services for many years. Custom services try to determine whether the transport of the legitimate goods across the borders is viable. The difficulty, certainly with both the heroin trade and the people trade, is that illegitimate consignments of people or drugs are concealed amongst legitimate consignments which would not in themselves raise suspicion.

The recent terrible event at Dover with the Chinese people found in the back of a container vehicle serves as a good example of the difficulties faced by law enforcement agencies. If at any stage during the journeys of that vehicle it had been stopped at a border crossing and law enforcement agencies had looked carefully at the type of work, the viability of the journey, or whether the route was sensible, their conclusion would have been that everything was in order. There would not have been anything in the paperwork or other factors to cause that vehicle to be scrutinized. Therefore it is no longer the case that law enforcement agencies can simply rely on "profiling", as the customs services call it, to identify vehicles or other means of transport that might be used to conceal illegal consignments.

Consequently, law enforcement agencies have looked recently at improving the intelligence flows and sharing far more information than ever before with other countries. One of the reasons for this is that we realise now that we can disrupt some of the trafficking networks not necessarily when the commodity - whether drugs or people - gets to its ultimate destination, but somewhere before that. And again I would like to give an example with Western Europe.

If we have consignments of heroin which are destined for the UK market, it may sometimes be possible to allow heroin to come to the United Kingdom so as to identify those persons that were responsible for importing it. However such a result is becoming very unlikely. Usually there are so many gaps between the people that would be arrested for carrying the goods and the ultimate organisers, that it is quite difficult to get back to the sources. But if you can identify somewhere in the chain that the entire routing of that commodity depends on one specific element, for instance a transport system from Eastern Europe into the European Union, and that is the weakest link in the chain of distribution, you can share the intelligence that you have with the countries through which that route

passes and they can take action and make arrests. Even if they might not be capturing the people like Howard Marks, they could be disrupting the trade very effectively, because it takes a long time to restore the missing link. Sometimes the transport link which can be taken out well outside the European Union, and can have a far greatest impact on the movements of those goods than any effort in the UK.

In the last twelve to eighteen months, law enforcement agencies have been quite effective against people trafficking firstly by sharing intelligence and secondly by discussing how we can process that intelligence. Many of you will be familiar with a technique which is used in law enforcement to deal with drug trafficking called controlled delivery. When we establish that there are drugs in a vehicle, we allow that vehicle to move under controlled conditions across a route to a place where we believe we can seize the drugs, make arrests and disrupt the networks.

If you have intelligence that there are people in the back of the vehicle then controlled delivery is not really practical, because of human rights concerns. You cannot treat people like a commodity just like the trafficker. So we have realised in the last year or two that as people trafficking becomes a bigger and bigger problem, we have to develop some of the techniques which we have used against drug trafficking for many years and modify them quite considerably.

One of the ways in which we are doing that across Central and Eastern Europe is liaising very closely not just with the border authorities but also with the agencies responsible for gathering criminal intelligence, to try and identify the facilitators of these movements of people.

People trafficking and drug trafficking share a common thread with the legitimate trade; there are middle-men, there are people throughout the transaction who require money, are there for the profit and can be attacked by criminal intelligence being directed against them by agencies in the countries in which they are based.

In Central and Eastern Europe there are a number of facilitators who will firstly arrange contacts with the people that are being brought out of Eastern Europe, or China. These facilitators have contracts with shipping companies and freight forwarders. If we can identify the facilitator, we can go to the criminal law enforcement agency in the country concerned and seek help. The law enforcement agency in the country of origin can mount an investigation under their own laws, and we can provide them with the intelligence required for that investigation. By targeting the facilitator they would get to a stage where they can catch the facilitator both with people and sometimes with money as well, and in exactly the same way as with drugs, the network can be disrupted.

We have been doing that and I think we are having some success, but it is particularly difficult. The people that are trafficked across the world want to be trafficked, they want to be brought to the United Kingdom or Western Europe because they believe that is where their lives would be much better. So they are also becoming quite clever and are deciding that in many cases they want to be sure that their risk of being detected is minimised. So we find now that once they can be taken from the country of origin into Central-Eastern Europe, they do not need to be smuggled in bulk, but have ways of coming across borders, individually.

You will know of course that in certain European Union countries and a couple of additional countries now under the Schengen Agreement once in the Schengen zone, movement is comparatively free for these people, and they do not come to the attention of law enforcement agencies. So whereas probably two years ago we would have seen most people trafficking being done in bulk consignments from the country of origin to the country of destination, very often now there is a bulk consignment moved half way along the route and then broken down in smaller consignments of people coming to Western Europe and the UK.

All of this requires law enforcement agencies to do a number of things: we must share intelligence, and we must pay attention to what Howard Marks said about the lack of expertise, and the difficulties created by different jurisdiction. In the European Union we are very active now at eliminating those difficulties The European Arrest Warrant coming into effect in 2003 will give us an extra tool in our armoury. But we still need the traditional approaches. We still need to have close links with legitimate transport businesses, with trade organisations, with people who control data bases. Very often ability to access these data bases through the cooperation of the private sector will give us information and relevant intelligence about routings we would not otherwise know. So we can track consignments of legitimate goods where we think that it is likely that illegitimate goods can be concealed amongst them.

It is a challenging and very expensive work. It is considerably expensive to try and target activities of law enforcement agencies against the small proportion of the trade that is actually dealing with illicit substances.

Let me revert to the example of Dover, that I discussed earlier, through which pass 52,000 lorries a month. In the worst case, probably a thousand of those are used to transport an illicit substance or illicit people. But the cost of dealing with that thousand is totally disproportionate and European Governments are realising now that we have to work much more closely together and try and find ways of dealing with the illegal commodities, regardless of their nature in a quick and effective way, and disrupt criminal networks early before they get too established.

After oil, the global drug trade is one of the biggest and most profitable in the world. Fourteen years ago, I was working for the United Nations Fund for Drug Abuse Control (UNFDAC). We had a project funded by the Italian, the British and the Canadian Governments that was designed to curtail the production and distribution of morphine or opium from South West Asia. Part of the project was licensing the legitimate opium cultivation Rajastan, India. We were giving help to law enforcement and advising them in surveillance techniques. There were security advisors advising local authorities how to stop drugs coming out of the area. Another part of the project was crop substitution. Further, for those licensed to grow opium, we had a system with the relevant computer software that allowed us to knew how much opium they could legitimately grow within a piece of land as allocated. All this opium was for the legitimate market. The big problem was the shift from the legitimate market to the illegitimate market, so we decided to have a meeting with the farmers in Rajastan. We sat down one afternoon in the heat with a group of about 30 farmers. It was quite an uncomfortable situation for us because they were not welcoming us at all but there was an elderly farmer there who at the end of the discussion addressed himself to me. That farmer very eloquently put the drug problem in perspective when he said: “It is not actually a problem at all! You have been telling us about what we should grow and that we shouldn’t sell the opium outside. But we only do that because you are

prepared to pay so much for it." A particular crop being considered at the time as a substitute was mustard. The farmer was explaining about the economics of mustard saying that if he sold his legitimate consignment of opium (at the time 38 kilos per hectare) he would get a legitimate income from the Indian government that would be enough to feed and clothe his family for a year. If, however, he managed to provide 40 kilos per hectare and sold the two extra kilos on the black market, those two kilos would feed and clothe many families. The profits were enormous. And he said to me quite openly,: "We will never solve the problem until we stop the problem of demand in the West". I think that remains the case now. That argument is equally valid for people. We have people in various parts of the world who see, particularly through television, the life-style that we enjoy in the West, and compare it with their own and say: "That's a lot better, I'd like to go there!". There are so many analogies between the people trade and the drugs trade, while the people who are trafficked across the world are victims and not criminals, what the farmer told me a few years ago about the profit in drugs is valid also for those who export those victims. Profit is the driving force. Those trafficked pay huge amounts of money to be moved across the world and we have to find a way to make that trade unattractive. That is far greater challenge than the challenge we have been facing with drugs. It is certainly difficult. We do not have the ability to make the economies of the third world as strong as the economies of the West, certainly not in a generation. These difficulties create all the ingredients for illicit trafficking in people and lay the ground for the emergence of facilitators and middle men who realise that there is in this activity as much money, if not more, as in drug trafficking.

For the UK Government, identifying and dismantling people and drugs trafficking networks are top priorities.

This presentation was a brief overview of the problem. I have not offered any solution. But we must identify the problem and see how we can deal with it on a continuing basis, especially with the people trafficking phenomenon, which is really going to become prevalent in the next three or four years.

5. Trafficking in Firearms, Small Arms and Light Weapons

The Nature and Extent of Trafficking in Small Arms and Light Weapons with a Focus on Organized Crime

NICOLAS FLORQUIN
Researcher, Small Arms Survey, Geneva

Introduction

The aim of this presentation is to provide an overview of the issue of trafficking in small arms and light weapons (SALW), with a particular emphasis on the role of organized crime.

The presentation will cover 3 areas:

i. the global trade in SALW
ii. features of trafficking in SALW
iii. the impacts of trafficking in SALW

I hope that some of the issues raised in this presentation will be picked up, and expanded upon by the other speakers.

The word trafficking implies something that is illicit or illegal. Trafficking as a concept has two distinct dimensions:

- the trade and commerce in explicitly illegal commodities (e.g. cocaine)
- the trade and commerce in legal commodities (e.g. cigarettes, petrol, currency, diamonds, arms) in illegal ways.

This presentation will focus specifically on the second dimension – the illicit trade and commerce in a legal commodity - SALW.

Global Trend in SALW: Definition, Basic Issues

The overwhelming majority of SALW start out their lives legally. They are either domestically manufactured by the State or in factories authorized by the State, or are otherwise legally acquired by individuals, private actors, or government agencies from foreign producers or suppliers. In only a few cases do weapons start out their lives being illicitly produced, usually then remaining in the illicit market for the rest of their life span.

SALW are produced by more than 1000 companies in at least 98 countries worldwide.

Legal weapons tend to become illicit through *transfers*. These transfers can be intra-state (within a State) or inter-state (between States). Transfers themselves can be either legal (authorized) or illicit, with the legal transfer of weapons being governed by national and/or international law.

The United Nations Disarmament Commission 'Guidelines on Conventional Arms Transfers' have defined illicit trafficking as the 'international trade in conventional arms, which is contrary to the laws of States and/or international law'.

Therefore, in order for a transfer of SALW to be considered illicit, there must be evidence of the violation of national and/or international laws. However, while small arms may enter the illicit market through transfers that explicitly violate national and/or international laws, there are also a number of other ways by which weapons can be diverted to the illicit market.

The mechanisms or pathways by which weapons move from the legal to the illicit circuits include the following:

i) Domestic leakage (e.g. theft from State arsenals)
ii) False Documentation (false end-user certifications or violations of end-use undertakings)
iii) Ant Trade: The small-scale transfer of weapons legally acquired in one State and then trafficked illegally into a neighbouring State;
iv) Supplies to non-state actors or countries under embargoes or other restrictions.

These four pathways are not necessarily exhaustive, but it is important to underline that *in virtually all of these cases, the diversion of arms to the illicit circuit takes place in direct violation of stated government policy.*

The concept of illicit trafficking in SALW needs further clarification. When discussing illicit trafficking, or the illegal trade in SALW, it is useful to distinguish between the grey market and the black market. While the terms are not always analytically clear-cut, they are useful for helping us to understand the different aspects of illicit trafficking.

Grey Market Transfers:

There are transfers (usually covert) conducted by Governments, brokers or other entities sponsored by (or acting on behalf of) Governments, that exploit loopholes or circumvent current national and/or international laws. Such transfers can be in violation of an exporting State's own national laws or even stated national policy, or international law, or can contravene the national (importing) laws of the recipient State. While this trade is arguably illicit, recipients or brokers of such transfers often argue that they are legal, as a government somewhere has approved or initiated the transfer.

Grey market transfers include sales to a recipient country that has no identifiable legal authority or government (e.g. Somalia), or transfers by governments to Non-State Actors (NSA), i.e. rebel and insurgent groups. In addition there are cases where governments (legally) hire brokers to transfer weapons to illegal recipients (e.g. countries or groups under embargo). Some arms brokers also claim that, if some government somewhere knows of the transfer and does nothing to stop it, then the transfer is 'legal'. Thus passive involvement in illicit trafficking is no different from active involvement.

Black Market Transfers:

Transfers that occur in clear violation of national and/or international laws (ref. UN Disarmament Commission Guidelines). Normally such transfers occur without any official government consent or control.

The difference here between the grey market and the black market is that government involvement in the grey market usually entails a hidden policy agenda or operation driving the transfer, while the black market only includes those transfers where corrupt individual government officials are acting on their own, usually for personal gain.

In sum, there are three types of SALW transfers: legal, grey and black. For the purposes of our discussion today both grey market and black market transfers are included in our definition of illicit trafficking.

Let me provide basic information about the global trade in SALW

- At least 60 countries are involved in the legal trade in SALW. It is impossible to say how many countries are involved in the illicit trade.
- The major legal suppliers of SALW include the US, the Russian Federation, a number of European countries, and China. (p127 SAS 2002)
- The total trade in SALW is worth about US$5 billion a year– of which about 80% is legal trade (US$4 billion a year), and the rest is illicit (worth about US$1 billion a year)
- Thus, the illicit trade in SALW is much less significant than legal trade in economic terms, yet has a disproportionate impact in terms of its role in fuelling crime and conflict.
- We can document about 50% of the legal trade – from official and unofficial information.
- More than 20 countries now provide information, through annual or other reports on their arms exports, including small arms exports.
- It is difficult to distinguish between the trade (legal and illicit) in new weapons, and surplus weapons.
- The grey market is significantly larger (in value and volume) than the black market.
- The grey market appears to have the greatest impact in situations of armed conflict - i.e. where Governments are actively or passively supplying SALW to non-state actors that are involved in intra- or interstate conflicts.
- Black market transfers tend to be much smaller (in terms of value and volume) than grey market transfers – used mainly to supply individuals and/or criminal groups.

Features of Illicit Trafficking in SALW

Illicit trafficking (whether in arms, drugs, cigarettes, petrol, human beings, etc) is not a new phenomenon. Trafficking in SALW has some specific features, but it also shares some common features with trafficking in other commodities.

For example, trafficking in SALW (illegal commerce in legal goods) is usually institutionally embedded (through individuals or companies) in the structures of the legal industry (in this case the arms industry – either State owned, or Government authorized)

Most illicit trafficking in SALW has the following features:

- various clandestine or covert methods are used to move the weapons from supplier to end-user, and/or to mask the identity of some or all of the actors;

- a substantial part of the cost of the deal is due not to the costs of purchasing the weapons but the costs associated with the surreptitious movement of the merchandise from supplier to end-user.
- the involvement of intermediaries (brokers, dealers, transport agents, financial agents) is critical.
- funds usually need to be laundered to hide their origins or destination

Arms deals can be covert in two ways: either their nature is disguised (which implies deceiving supply-side regulators with fake documents, or their very existence is hidden, so that the regulatory system is avoided altogether. It is interesting to consider which method is more common today, and which method is used with regard to small scale and large scale consignments.

Actors

Trafficking in SALW (and other commodities) involves a number of actors:

- suppliers: arms trading companies, or producers involved in the illicit manufacture of SALW but also legal manufacturers, where part of the production is made "off the books" and sold outside official channels;
- intermediaries: criminal groups (usually involved in the illicit trafficking of several types of commodities) and arms brokers (usually focusing on arms) facilitate and organize arms transactions, can provide counterfeited documentation, and sometimes have their own transport facilities;
- financial agents and banks which arrange finance and payment;
- transport/shipping agents: who organize the transportation of goods;
- corrupt government officials: who provide the necessary documentation (i.e. in the exporting country: forged export licenses, in the importing country: forged end user certificates), sometimes act as intermediaries;
- end users: rebel movements, illegitimate non state actors, countries under embargo.

So actors can be both governmental and non-governmental. It is also important to note that these categories of actors are not mutually exclusive. Militias and armed groups, for instance, partly finance their activities through various forms of trafficking, including arms trafficking. Also, not all actors are involved in every case of illicit trafficking.

In terms of recipients, criminals or "terrorists" (or, for that matter, intelligence agents looking for "sterile" equipment) often demand SALW in small quantities, because their acts of violence are usually selective. Armies, whether regular or irregular, demand SALW in much larger quantities. It is interesting to note that the same actors (intermediaries, brokers, suppliers) might be used, or involved, in the supply of weapons to both types of recipients.

Countries might also have strategic motives to resort to illicit trafficking (to hide their military holdings from their neighbors' scrutiny) or financial motives (to protect clandestine bank resources from punitive asset freezes).

Usually brokering activities, and organized crime are treated separately, but brokers who facilitate illicit deals in SALW tend to also have links with organized crime, or criminal networks.

Criminal groups and criminal networks can of course play a key role in the illicit trafficking in SALW (and of course other commodities)

In general terms, criminal networks have a number of features:

- they can emerge spontaneously to complete a single transaction;
- they can be created by a core of different groups for a specific purpose;
- they can be involved in a range of different activities (i.e. trafficking in drugs, stolen cars, arms, prostitution, antiquities, endangered species, and extortion and fraud).

Thus, most criminal networks tend to maintain a relatively fluid structure. This has a number of advantages:

- their low visibility enables them to operate clandestinely;
- their lack of physical infrastructure makes them difficult to target by law enforcement agencies and enables them to move easily to countries where risks of enforcement are low;
- their ambiguous status creates jurisdictional confusion;
- they are difficult to dismantle (if part of the network is destroyed the network can still operate) and easy to rebuild.

Few criminal groups are only involved in illicit trafficking in SALW. These criminal groups tend to get involved in illicit trafficking in SALW as a supplementary or complementary activity to their other trafficking activities.

b) Link with other forms of trafficking (drugs, human beings, other commodities)

There are in some cases linkages between trafficking in SALW and other commodities. However, these linkages tend to be ad hoc, random, and not in any way institutionalized (i.e., created for a particular purpose and then dismantled). These linkages, where they exist, also tend to be context-specific.

The empirical evidence available to demonstrate the links between trafficking in SALW and other commodities is difficult to gather. In addition, some of the available data is highly questionable, as security agencies (intelligence, police, border guards etc.) have institutional incentives to exaggerate linkages, as this will help them get more state funds/resources.

The linkages between trafficking in various commodities seem to depend on context. Thus, in Central Asia, the drugs and arms trade are closely interlinked, with smugglers transporting arms in one direction and drugs in the other. In North Africa, human smuggling over the straits of Gibraltar is linked to the drug trade (both are smuggled from Morocco to Spain), but there is no known arms component. In the Balkans, various forms of smuggling are interlinked (human beings, drugs, arms etc.).

In recent years a set of interrelated black markets (in different commodities) with their own sources of supply, their own systems of information, and their own modes of financing have emerged. The result is that an illicit arms deal might take place within a matrix of various black market transactions. For example, weapons might be sold for cash,

exchanged for hostages, bartered for heroin or religious artifacts, or countertraded for grain or oil.' However, in most cases, the linkages between these various black markets are ad hoc, created for specific purposes and deals. Once the specific deal, or transaction is completed, the linkage is usually dismantled.

c) Financing of illicit trafficking

The costs of illicit SALW deals tend to be higher than for legal deals, for the following reasons:

1) cost of fake documentation (false end-user certificates (EUCs), export licenses etc.)
2) bribes
3) fees to brokers, transport agents, front men etc.
4) if payment is not in cash (i.e. in diamonds, etc.) an extra charge may apply
5) money-laundering costs

In an illicit SALW transaction, the pricing process is far more complex. Buying the weapons is only the initial step in a long and complex commercial chain that adds "service" charges at each stage.

The various parts of this cost chain are:

- the charge for the issuance of a letter of credit by a gunrunner;
- the costs of phony EUCs;
- sometimes the payments to ensure that the selling country issues the export license or to bribe obstructionist customs officers;
- costs associated with the use of front men and "subcontractors";
- costs of transportation;
- potential payments necessary, at the point of delivery, to ensure quiet cooperation at the port of disembarkation;
- kickbacks to officials responsible for steering the order to the particular dealer might also be added;
- if the deal is monitored by one or more intelligence services, each may demand a "covert action tax", with the funds used to top up a "black budget";
- additional costs might be represented by exchange discounts and commodity brokers' fees, if the payments are made in nonconventional forms;
- finally a profit percentage must be added.

The net result of this cost chain is a final sale price to the recipient that bears little relationship to the original cost of purchasing the weapons.

Impact of Trafficking in SALW

While illicit transactions in SALW tend to cost more than legal transactions, and are often more complex, illicit trafficking remains popular for a number of reasons:

- it guarantees anonymity (masks identity of some, or all actors);
- it has useful strategic and financial aspects (e.g. laundering of government money);

- it is often the only source of weapons for criminals and those actors who are prohibited from obtaining weapons legally (e.g. embargoed states, rebel groups).

The economic impact of trafficking in SALW can be examined in terms of the following issues:

- Corruption (role of government officials)
- Government Revenue and Resources
- Indirect impact

1) Corruption

Corruption on the part of government officials is a key feature of the arms business, and of course illicit trafficking in SALW. In most countries, the production of, and trade in, SALW is regulated by government. But in almost all cases of illicit trafficking (at the point of supply, transit and receipt), some government official is involved, either in terms of individual interest or corporate interest (e.g. security agency).

Corruption is also a key issue in customs services. This is an economic issue, linked to poor pay (sometimes no pay), in which brides are the only source of income for many customs officials.

Corruption and bribery affect both the legal and illegal arms trade. There is, indeed, little difference between the defense industry offering bribes to government officials to secure a contract, and arms brokers offering money in exchange for an official turning a blind eye on forged documentation.

A study by Transparency International (1999) shows that the defense sector is one of the most corrupt sectors of the global economy, only second to public works and construction. A 2000 US Dept. of Commerce (2000) report confirms this by revealing that about half of all identified cases of bribery between 1994 and 1999 involved the defense sector.

Corruption can have a negative impact on governance and the rule of law generally. If corruption amongst government officials is endemic, but is ignored or not dealt with, this creates a culture of impunity.

Such a situation undermines the government's legitimacy and its ability to enforce a reliable, consistent, legal framework for the normal functioning of markets, and regular economic transactions. In the long term this can have detrimental consequences for a country's macroeconomic environment.

2) Government Revenue and Resources

Illicit trafficking in SALW (and other commodities) means that the government's ability to collect revenue (in the form of taxes, import duties etc) is reduced. This in turn means that government has fewer resources to spend on basic services (health, education etc). Thus reducing illicit trafficking is critical in terms of revenue collection, particularly for developing countries, where resources are scarce.

The amount of money spent on combating illicit trafficking can also have adverse economic effects, by reducing the available resources for government spending on other social services.

The presence of a large informal (or black) economy which is fed by illicit trafficking (in different commodities) is economically inefficient, and can present a major obstacle to economic stability in terms of the following:

- prices are often artificially high or fluctuate widely;
- supply of goods is not guaranteed;
- no consumer protection (no guarantees for products, no repair).

3) Other Socio-Economic Impact

Most illicit arms go to actors who are most likely to use them: criminal groups, terrorists, rebel armies etc. Thus, illicit trafficking in SALW can play an important role in fuelling crime, conflict and insecurity.

As such, it can have an impact on a country's socio-political stability, which in turn has an impact on macroeconomic conditions, and investor confidence (both amongst domestic and foreign investors).

The presence of high levels of violent crime, or armed conflict, can have a number of other impacts, which can undermine a country's socio-economic prospects.

High levels of armed violence can lead to forced displacement (refugees and internally displaced persons), declining agricultural production and food security, declining access to basic services (if schools and clinics are attacked or targeted). In this context, a country's economic prospects will be severely diminished.

Conclusion

Because most weapons start out their lives legally, we have to focus on regulating the legal production of, and trade in, SALW if we want to do anything serious about illicit trafficking. But we have to start at home at the national level. Governments need to tighten legislation and regulations governing legal production and trade, and then invest significant resources in implementation.

We need more transparency. Until we have more transparency about the legal trade in SALW, we will never really know about the dynamics of illicit trafficking, and how legal weapons are being diverted into illicit channels.

But we have a problem. Decades of secrecy about the legal production of, and trade in, arms have created within many governments an information gap – where even senior officials in government simply do not really know, and may never know, the true picture about SALW in their own country. Without adequate information we will not be able to effectively tackle the issue of illicit trafficking in SALW.

The Use of Criminal Justice Measures to Prevent and Combat Trafficking in Firearms, Parts, Components and Explosives

CHRISTOPHER D. RAM[1]
United Nations Office on Drugs and Crime

Illicit commerce in commodities is often fuelled by the nature of the commodities themselves, and in particular characteristics which distort their economic value in legitimate or illicit markets. Trafficking in addictive substances, for example, derives revenues from the fact that addicts will pay inflated prices, and in the case of narcotic drugs, because legal restrictions increase risks and limit supplies. Firearms and other weapons share these same characteristics, and are among the more lucrative of illicit commodities. They can often be obtained in large quantities at artificially low costs, as military forces dispose of surplus or obsolete weaponry, and as conflicts end. They can also be sold at artificially high price in regions where conflict threatens, or to criminal offenders in regions where gun control restrictions increase scarcity, and for this reason, trafficking patterns often involve the flow of weapons from post-conflict regions to regions where armed conflict is either ongoing or seems likely to start.

The illicit traffic in weapons is particularly difficult to control because control options tend to straddle traditional legal and policy boundaries between individual and national security matters. As will be seen, firearms and other weapons represent a problem not only because they are actually used by criminals and because they are trafficked by criminals as a commodity, but also because, in sufficient quantities they can be a tool for exerting political or military influence and because they can actually generate armed conflict or at least make it possible. Boundaries between crime and security blur in almost every direction, when the commodity under consideration is weapons. A host of sources link trafficking in weapons with trafficking in narcotics and other commodities, as well as other organised crime activities.[2] Traffickers range from organised crime *per se* to a host of terrorist, insurgent and other groups, to those acting covertly or even overtly, on behalf of States. Traffickers may act on behalf of States, or with at least tacit approval in trafficking weapons, while acting entirely outside of the law in respect of other commodities. Talk of markets and transactions involving firearms, weapons and related technologies as being black, white and various shades of grey is commonplace, and the arms trade coined the term "dual-use technologies".

It is axiomatic that, to be effective against transnational organised crime of any sort, control mechanisms must be present in most, if not all countries, and must be coordinated to prevent offenders from evading restrictions, prosecution and punishment by simply structuring their activities so as to avoid regions where controls are strong and exploit those where they are weak. The same is true of the boundary between crime and security and between State and non-State actors and actions: if criminal justice controls are strong, traffickers will seek the shade of State protection wherever they can. If political arms-control restrictions are strong, trafficking will tend to be displaced into the criminal *milieu*.

[1] The author was a Crime Prevention Expert with the United Nations Centre for International Crime Prevention, Commission Secretariat and Legal Affairs Branch and had responsibility for supporting the negotiation of the Protocol. Views expressed are those of the author, and do not necessarily represent those of the United Nations.

[2] See for example, Geneva Graduate Institute of International Studies, *Small Arms Survey 2002*, Oxford University Press 2002, chapter 3, and various sources in Gasparini Alves, P. and Cipollone, D., eds., *Curbing Illicit Trafficking in Small Arms and Sensitive Technologies*, United Nations Institute for Disarmament Research, 1998, UNIDIR/98/16, UN Sales No.GV..E.98.0.8, and Singh, J. *Light Weapons and International Security*, Indian Pugwash Society and British American Security Information Council (BASIC), London, 1995.

Only if both are strong, and closely harmonised, is the overall objective of controlling the flows of firearms and other weaponry likely to be successful.

Negotiation of the *Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing United Nations Convention against Transnational Organized Crime*[1,2]

As a result of the growing concern of States about the problem of transnational organised crime, a series of steps which began in the early 1990s ultimately led to the adoption of the Convention against Transnational Organized Crime and its Protocols in late 2000 and early 2001. Generally, concerns were expressed that crime was globalising, expanding in both its geographical reach and the range of criminal activities undertaken. Disparate criminal groups, brought together by improvements in transportation and communications, began to merge, cooperate or form alliances with others active in different regions or in different criminal enterprises. Smuggling routes previously established for single commodities such as narcotic drugs began to be used for a wider range of commodities, and efforts to control money-laundering were confronted with a steady series of changes which enhanced the effectiveness of global economic systems, but also provided much greater opportunities for organised crime to conceal its profits, and an ever-increasing volume of legitimate transactions within which to conceal illegitimate ones. As the decade passed, high levels of concern sustained momentum. Organised crime, corruption and terrorism emerged as major threats, and links between them were seen not only as issues of crime-control and individual security, but of national security.

The specific process which led to the completion of the Convention and its Protocols can be traced through a series of General Assembly resolutions between 1994-2001. The Government of Italy hosted a World Ministerial Conference on Organized Transnational Crime in November 1994, which affirmed the commitment of those present to the fight against organised crime and proposed a series of steps to be taken to enhance international cooperation in this area.[3] In December 1994, the General Assembly approved the Naples Political Declaration and Action Plan against Transnational Organized Crime which had been produced by the Conference, and called on the United Nations Commission for Crime Prevention and Criminal Justice to seek the views of countries on the impact of a possible convention and the issues which such a convention might contain.[4] Between 1994 and 1996 discussions on possible provisions of a Convention took place among Member States. The General Assembly took note of a complete text proposed by the Government of Poland in 1996, while a number of other proposals were taking shape.[5] To bring together the various proposals, the Assembly established an open-ended intergovernmental group of experts to develop a preliminary draft text to serve as the basis of negotiations. The text was further developed during the 7th session of the Commission for Crime Prevention and Criminal Justice in April 1998, and by an informal preparatory committee held in Buenos Aires later that year.[6]

[1] This segment is an informal summary of the negotiation process and substantive content relating to the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing United Nations Convention against Transnational Organized Crime, as well as relevant provisions of the Convention itself. For authoritative information, the texts of the instruments themselves should be consulted. The Convention and two of its Protocols, those dealing with trafficking in persons and the smuggling of migrants, were adopted by the General Assembly on 15 November 2000 (GA/Res/55/25). The third (firearms) Protocol was finalized at the 12th session of the Ad Hoc Committee in March 2001, and adopted by the General Assembly on 31 May 2001 (GA/Res//55/255). Texts of these documents are available on-line at: http://www.unodc. org

[2] Hereinafter Protocol against trafficking in firearms.

[3] Report of the World Ministerial Conference on Organized Transnational Crime, U.N. Doc. # A/49/748, 2 December 1994.

[4] GA/RES/49/159 of 23 December 1994.

[5] GA/RES/51/120 of 12 December 1996.

A resolution formally creating a mandate to produce an international legal instrument and establishing an open-ended intergovernmental ad hoc committee to negotiate its provisions was prepared by the 1998 session of the Commission, and transmitted to the General Assembly *via* the Economic and Social Council, and was adopted by the Assembly as its resolution 53/111 of 9 December 1998.[1] As a result of earlier discussions about possible provisions to be included in the instrument, it was decided to create four separate instruments, consisting of a parent Convention, and three additional instruments, or Protocols. Details of the relationship between the Convention and Protocols would later be refined in the negotiations, but the initial content reflected the ultimate approach: the parent Convention would contain provisions to deal with organised crime as a general issue at both the domestic and transnational levels, and the Protocols would contain provisions which were more specifically focused on the three most serious problems identified in the preliminary discussions: trafficking in human beings, the smuggling of migrants, and trafficking in firearms. This approach offered flexibility in drafting and implementing the treaties and created the possibility of the creation of further Protocols at a later date using the general framework of the parent Convention. It also allowed parallel negotiations in which the Convention and one or more Protocols could be considered simultaneously, which accelerated the negotiations, but placed a severe strain on countries which lacked the resources to attend two meetings at the same time.

Following the adoption of its convening resolution, the Ad Hoc Committee began its work on 19 January 1999. Early sessions began refining the draft Convention text produced by the Crime Commission and the Buenos Aires informal preparatory meeting, and consolidated a range of other proposals into the texts of the three Protocols, with preliminary drafts of the Protocols being submitted by Argentina and the United States of America (trafficking in persons), Austria and Italy (smuggling of migrants) and Canada and Japan (trafficking in firearms). As a result of preliminary negotiations, the General Assembly adjusted the scope of the first Protocol from trafficking in women and children to "…trafficking in persons, especially women and children" in December 1999.[2]

Once preliminary texts were in hand, the negotiation of all four instruments also proceeded quickly, with many sessions reviewing two of the four instruments at the same time, in parallel negotiations.[3] The parent Convention was finalised at the 10th Session, from 17-28 July 2000, and the Protocols dealing with trafficking in persons and the smuggling of migrants were finalised at the 11th Session, from 2-28 October 2000. Several provisions of the third Protocol, on illicit firearms trafficking, required a further session to complete. That session was mandated by the General Assembly when it adopted the first three instruments, and the final Protocol was duly completed at the 12th session of the Ad Hoc Committee, from 26 February to 2 March 2001. As required by Resolution 54/126, all four were adopted by resolution of the General Assembly, and opened for signature and ratification.[4]

---

[6] GA/RES/52/85 of 12 December 1997; Report of the Commission for Crime Prevention and Criminal Justice at its Seventh Session, 21-30 April 1998, E/1998/30, Appendix I; and Report of the Informal Preparatory Meeting of the Open-Ended Intergovernmental Ad Hoc Committee on the Elaboration of a Comprehensive International Convention Against Transnational Organized Crime Held at Buenos Aires From 31 August to 4 September 1998, A/AC.254/3.

[1] Following GA/Res/ 53/111, which set the initial mandate, modifications were made during the negotiations by GA/Res/54/126 and 54/127 of 17 December 1999. Regarding the review of the proposed resolution by the ECOSOC, see also ECOSOC Res. 1998/18, 1998/19 and 1998/20 of 28 July 1998.

[2] GA/RES/54/126 of 17 December 1999, paragraph 3. In the same resolution, the General Assembly also decided that it would adopt the final texts of the instruments prior to opening them for signature.

[3] The procedure agreed was that parallel meetings would be conducted as informal sessions of the Ad Hoc Committee, with the resulting texts subject to later review and formal approval by the Plenary the next time the instrument involved appeared on the formal agenda.

[4] General Assembly Resolutions 55/25 of 15 November 2000, and 55/255 of 31 May 2001.

Having been adopted within the time originally allocated for the negotiations, the first three instruments were formally opened for signature at a conference held in Palermo, Italy in December 2000. The Protocol against illicit trafficking in firearms, not being completed in time, has subsequently gathered fewer signatures and fewer ratifications that the other instruments.[1] The Ad Hoc Committee itself, having completed its work in relation to the Convention and Protocols, is mandated only to prepare rules of procedure for the Conference of Parties to the Convention prior to the Conference's first meeting, and is expected to lapse once this last task is completed and its mandate has been fully exhausted.[2]

The Protocol against trafficking in firearms presented negotiators with several challenges not found in the other three instruments. The content of the Protocol is more subject-specific than that of the other instruments, and apart from the provisions of the Convention which apply to all of the Protocols, *mutatis mutandis*,[3] it has no subject-matter in common with the other instruments.[4] Where the other Protocols required technical expertise in areas such as immigration, measures relating to asylum-seekers and social matters such as the support, assistance and rehabilitation of victims, the Protocol against trafficking in firearms was largely the province of forensic experts. Technical issues relating to such elements as the development of a suitable forensic definition of "firearm", the unique marking of firearms, the definition and classification of parts, components and ammunition, the issuance of import/export authorizations needed to distinguish between legitimate transfers and illicit trafficking and the keeping of records needed to trace firearms many years after a transaction or transfer had taken place all raised issues unique to this particular Protocol.

The major obstacles encountered by the Protocol against firearms trafficking, however, were of a political rather than a technical nature. All arose in some way from the fact that the Protocol occupies a policy area which straddles the traditional boundary between criminal justice and individual or human security and national security and arms-control. Firearms and the other items covered by the Protocol represent three very different sets of problems for policy-makers. They can be seen as weapons frequently used in criminal offences such as murder or robbery, and as an illicit commodity to be smuggled or trafficked by criminals for profit in the same way as narcotic drugs or other contraband. Most countries deal with these two aspects using criminal justice measures, and these measures formed the basis of proposals that they made with respect to the Protocol. The third aspect was more problematic. Firearms, ammunition, and the broader category of small arms and light weapons are also a strategic commodity, which can be transferred or withheld as a means of exerting political or military influence or in pursuit of other national security objectives. Countries make transfers, sometimes of an irregular or covert nature, to arm allies, and seek to block transfers in order to prevent the arming of enemies.

The first major political issue for negotiators arose in late 1999. Initial proposals had been made to either include illicit trafficking in explosives within the Protocol or to

[1] All four of the instruments remained open for signature for two years from the date on which the first three were opened at the Palermo Conference, until 12 December 2002. As of that date, the Convention and Protocol against trafficking in persons had gathered more than half of the 40 ratifications needed to bring them into force, and the Protocol against the smuggling of migrants had almost half. The third Protocol had 52 signatures and 3 ratifications. Note that countries which did not sign may still become States Parties to any of the instruments by accession at any time, provided that no country can become a Party to a Protocol unless it is also a Party to the parent Convention.

[2] GA/Res/55/25 para.10.

[3] See Article 1, paragraph 2 of each Protocol.

[4] Articles 11-13 of the other two Protocols are identical, for example, and many other provisions are similar, reflecting a pattern in which text was first developed for one instrument and then modified as necessary to fit the different circumstances of the other. Another example is found in Convention Articles 24-25 and Article 6 of the Protocol against trafficking in persons, all of which deal with the support, assistance or protection of victims or witnesses.

deal with this issue in a separate Protocol.[1] Explosives had been included within the scope of the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and Other Related Materials, on which the original text of the Protocol was partially based,[2] and the delegations of Mexico and several other States sought their inclusion in the Protocol as well. However, no reference to explosives had been included in the mandate provideed by the General Assembly in its resolution 53/111, and as negotiations proceeded, it became apparent that there was not sufficient support for the proposal to find consensus. Some delegations expressed concerns that dealing with explosives would go too far into areas involving arms-control and national security, while others expressed more pragmatic technical concerns about seeking to regulate two very different commodities using the same technical provisions, and about the length of time it might take to develop appropriate alternative technical regulations more suitable for explosives.[3]

Following extensive discussions at its Third, Fifth and Seventh Sessions and the consideration of the scope of the mandate under which the General Assembly requested the Ad Hoc Committee to produce the Protocol, it was decided at the Seventh Session, to limit the scope of the Protocol to firearms, parts components and ammunition, and to delete the various references to explosives from the text.[4] While the debate concerning whether to include explosives was ongoing, some of the countries concerned also agreed that the matter required further study, and a separate mandate was sought and obtained from the General Assembly. In December 1999, the Assembly adopted a further resolution calling on the Secretary General to convene a group of experts to study the illicit manufacturing of and trafficking in explosives by criminals and their use for criminal purposes.[5] The resolution further called upon the Ad Hoc Committee, once the study was complete, to consider the elaboration of a further international instrument on explosives.

The group of experts was duly convened, but did not meet until March of 2001 and did not complete its work until December 2001. Since the Ad Hoc Committee had completed its work in relation to the original organized crime instruments by then, the report of the Group and the requested Study were presented to the Commission for Crime Prevention and Criminal Justice at its 11th session, in April of 2002.[6] The Group made no recommendation as to whether a further instrument on explosives was necessary, but did note that the misuse of explosives for criminal and terrorist purposes was difficult if not impossible to distinguish, and that this made the elaboration of a further Protocol to the Convention against Transnational Organized Crime impracticable because Articles 2 and 3 of the Convention limited the extent to which the Convention and its Protocols could be

[1] See Report of the Commission for Crime Prevention and Criminal Justice at its Seventh Session, E/1998/30 and ECOSOC Resolution 1998/17 of 28 July 1998.

[2] OAS Treaty A-63, adopted 14 November 1998. regarding the use of the OAS instrument in developing the Protocol, see GA/RES/54/127, paragraph 3.

[3] One frequently-raised point, for example was the difference between permanently marking firearms, with markings that can be read after a weapon has been fired one or more times, and marking explosives. Since explosives are consumed when used, marking consists of adding either chemicals to facilitate detection by sampling or "sniffing" equipment before detonation, or particles or chemicals which facilitate some aspects of identification after detonation. To address this issue during the negotiations, proponents of including explosives agreed to exclude them from the otherwise-applicable marking requirements, but a suitable alternative method of marking explosives was never proposed. This matter was later taken up by the Group of Experts on Explosives (below).

[4] See Report of the Ad Hoc Committee on its seventh session, A/AC.254/25, paragraph 23 and Revised Draft Protocol, A/AC.254/4/Add.2/Rev.5, footnote 1. As a result of the decision, references to "explosives" *per se*, were removed, but references to certain explosive devices, such as bombs, grenades and rockets were retained. These were later excluded as a result of negotiations during the eleventh and twelfth sessions as part of the general compromise on which the Protocol was finalized.

[5] GA/Res/54/127 of 17 December 1999.

[6] The original mandate, GA/RES/54/127, paragraph 8, actually requires that the Secretary General report on the work of the Group of Experts to the Commission, after which the Ad Hoc Committee was directed to consider the possibility of elaborating a further instrument. The Report and Study were duly reported as E/CN.15/2002/9 and E/CN.15/2002/9/Add.1, respectively and are discussed below. A reference directly to the Commission also enabled the issue of explosives to be dealt with more quickly, since the only mandate remaining to the Ad Hoc Committee, under Resolution 54/126, is to produce rules of procedure for the Conference of States Parties.

applied to terrorism.[1] Since the work of the Group was reported to the Commission, there have been no subsequent proposals to produce a further instrument. The research and other substantive recommendations of the Group are discussed in more detail below.

The other major political issues facing negotiators were gradually clarified during the negotiation process, but were not resolved during the 11th session of the Ad Hoc Committee, at which it was originally hoped that all three Protocols would be finalised. At the conclusion of the 11th session, three major and inter-related issues remained unresolved. These questions were finally agreed during the 12th session mandated by the General Assembly when it adopted the first three instruments.[2]

The first of these three issues was the question of the physical subject-matter to which the Protocol would apply. While the mandate spoke of "firearms", negotiators still found it necessary to define the term, which raised issues of whether very large "firearms" and other small arms or light weapons more commonly associated with arms control than crime control should be included. This was in some ways a continuation of the previous question of whether explosives should be included, since the decision to exclude them had been based in part on advice that they could not be considered as falling within the scope of the term "firearms" as it was used in Resolution 53/111. At the 11th and 12th sessions, the term was further narrowed by qualifying the description "barrelled weapon" with the term "portable", which clarified that very large barrelled weapons such as artillery pieces were not included.[3] A series of references to rockets, rocket-launchers, grenade-launchers and an assortment of explosive and incendiary bombs, most of which could be considered as "small arms" but not "firearms" were also excluded. These changes focused the other requirements of the Protocol on a narrow, forensic category of firearms similar to that found in the domestic gun-control legislation and criminal offence provisions of some countries,[4] and limited the extent to which those restrictions would affect a broader category of strategic and national security interests.

The second major question not resolved until the final negotiating session was the breadth of the requirement to mark firearms and the amount of information which such markings would contain. Most delegations, advised by law-enforcement experts, supported requirements that markings be sufficiently unique to identify each firearm to the exclusion of all others, in order to support accurate record-keeping and effective tracing. They also wanted a requirement that every firearm be marked at the time of manufacture, which was more controversial. Some delegations had concerns about the marking of firearms produced for military and law-enforcement personnel and/or national security purposes, having established separate marking systems to prevent such firearms from being identified and traced. Any provision which did not require unique marking of such weapons, on the other hand, would raise major concerns in the law-enforcement community, because the single largest source of both legal and illicit firearms is firearms originally produced for military or similar purposes. The legal disposal or illicit diversion of such weapons, it was

[1] E/CN.15/2002/9, subparagraph 30(d). Article 3 requires the involvement of an "organised criminal group" as a condition for applying the Convention, and Article 2, subparagraph (a) limits such groups to those seeking to obtain a "financial or other material benefit". These limits are applied to the Protocols, *mutatis mutandis* by Article 1 of each Protocol. This leaves open the theoretical possibility that a further Protocol on explosives might not contain the same limits, but this would probably create insurmountable practical problems because the various substantive provisions of the Convention were negotiated and are drafted on the general assumption that they would apply only to organised crime cases and that they would not apply to terrorism which was not also within the scope of organised crime as envisaged by the drafters.

[2] GA/RES/55/25, paragraphs 4-5.

[3] See also the agreed notes for the *Travaux Preparatoires*, A/55/383/Add.3, paragraph 3, which state that "portable" is intended to mean portable by one person without assistance.

[4] The language is in fact based on the definitional provisions of the Canadian *Criminal Code* (subsection 84(1)) and the U.K. *Firearms Act, 1968* (section 57).

argued, would produce a large class of unmarked weapons, frustrating the basic policies of the Protocol, import-export control, tracing and the investigation and prosecution of illicit trafficking.

While all delegations supported marking for purposes of basic identification, some wished to go further and establish standards for marking which would effectively encode basic information about the origin and history of each firearm, enabling these to be read directly from the marking without having to trace the firearm. Many forensic experts also sought a requirement that basic alphabetical and numeric characters be used to ensure that markings were easily recognisable as such and readable by untrained law-enforcement personnel, and to facilitate the use of information technologies in record-keeping and the transmission of information in the course of tracing firearms from one State Party to another. The resolution of these issues proved to be complex.

It was eventually agreed that the basic marking requirement, found in Article 8, would require "unique marking" of every firearm,[1] but it was necessary to provide for two options for the form of markings, one consisting of serial numbers and another using what are referred to as simple geometric symbols. The latter option allowed countries which use such markings on military and other government firearms to maintain such a system, which supports tracing, but only by insiders who understand the significance of the markings and have access to the necessary records. Outsiders must seek tracing from insiders, and such weapons must be marked so as to permit ready identification of the country of manufacture to ensure that the necessary insiders can be identified. The other major issue, the extent to which government, military and similar firearms would have to be marked at all, is dealt with partly in Article 8, which requires all firearms to be marked, and partly in Article 4, which sets out the scope of subject-matter included and excluded from the application of the Protocol. In excluding specified State- or national security-related matters from the application of the Protocol, Article 4, paragraph 2 provides that the Protocol does not apply to "…state-to-state transactions or to state transfers…" where such application would be prejudicial to the right to act in the interest of national security consistent with the U.N. Charter. Since marking and other elements of manufacture would not generally be considered to be a "transaction" or a "transfer", the basic marking requirement will generally apply to all firearms, even those made for military, law-enforcement or national security forces or similar applications, which avoids the problem of the creation of large volumes of unmarked weapons which could later be diverted or disposed of and then illicitly trafficked. At the same time, it can be argued that some marking, especially the marking of firearms required on import by subparagraph 8(1)(b) of the Protocol, might well be considered as part of a process of transaction or transfer, and therefore not required if the national security criteria of Article 4, paragraph 2 are met. Whether States Parties adopt such an interpretation remains to be seen.

The third major issue resolved at the 12th and final session of the Ad Hoc Committee was the basic question raised by Article 4: to what extent would the Protocol apply at all to matters considered by States Parties as falling within the ambit of national-security and not crime-control? Apart from the delineation of a basic boundary between national security and criminal justice matters, this question was also closely linked to the previous two issues and to numerous other less difficult elements of the Protocol. Generally, the broader the scope of the various substantive requirements of the Protocol, the broader an exclusion was

[1] In practical terms, the actual markings are not entirely unique, but they are sufficiently so to uniquely identify each firearm, when taken together with other basic identifying criteria, such as make, model, calibre and similar characteristics. Thus, for example, two handguns made by different manufacturers in different countries are not necessarily required to have different markings or serial numbers.

sought by some delegations for national security matters. Thus the decision to exclude explosives and an assortment of small arms or light weapons from the definition of "firearm", and the agreement to allow forms of marking not easily traceable by outsiders without assistance from officers of the country of manufacture created additional room for compromise on the basic national security issue.

Essentially, the search was for language which would not apply any element of the Protocol to basic transfers between States, and which would exclude sensitive national security activities from requirements such as tracing and record-keeping, while at the same time avoiding a national security exclusion that would exempt too broad a range of cases that would otherwise be considered as illicit trafficking. State-to-state transfers were never considered as suitable for regulation by criminal law, and would not have been considered as "illicit trafficking" by the General Assembly, and language excluding such transfers was included in early drafts of the Protocol. The second revision of the text, for example, refers to the exclusion of all "State-to-State transactions or transactions/transfers for the purposes of national security", and this language was consistently retained with minor variations.[1]

The more nebulous area of national security transactions or transfers was more problematic, however, requiring language which would allow legitimate national security activities, but not create an exemption so broad as to exclude almost any trafficking from the Protocol where traffickers could make a plausible claim to be acting on behalf of a State. The eventual compromise, found in Article 4, paragraph 2 was to exclude specified activities where the Protocol would, if applied, prejudice legitimate national security interests consistent with the U.N. Charter. This exclusion is further narrowed, as noted in the discussion of marking requirements, above, by applying it only to "state transfers", which would exclude most activities normally associated with manufacturing, including the basic requirement to affix markings as required by subparagraph 8(1)(a) of the Protocol. Effectively, all firearms must be uniquely marked at manufacture, whether they are made for government or private use, or for export, but the marking requirements may not apply to activities which constitute part of an excluded State or national-security transaction or transfer. The language of other provisions was also adjusted to limit the scope of application to matters considered by some delegations as impinging on national security. The basic information-sharing obligation of Article 12, paragraph 1 of the Protocol, for example, speaks of the sharing of "relevant case-specific information", to clarify that the obligation is to cooperate on specific trafficking investigations and does not extend to the general sharing of intelligence.

The Article 4 exclusion is broadened to some degree by including in paragraph 1 the phrase "…where those offences are transnational in nature and involve an organised criminal group…". Based on the language of Article 3 of the Convention, this effectively excludes purely domestic firearms trafficking, and cases where perpetrators are either individuals acting as such, or are groups which are not "organized criminal groups" as defined by Article 2, subparagraph (*a*) of the Convention. That definition includes a requirement that such groups be linked to the pursuit of some "financial or other material

[1] See A/AC.254/4/Add.2/Rev.2, Article IV. That text, previously examined by the First and Third Sessions of the Ad Hoc Committee, contains three options with identical language apart from the references to national security "transactions" or "transfers". A fourth option would have limited the scope to firearms which had been illegally manufactured or illegally traded, leaving the question of application to State activities open to interpretation. The four options were consolidated at the Fifth Session, but the basic language excluding State-to-State and national security transactions or transfers was retained. Further language was added by China which would have also exempted all firearms made exclusively for law enforcement or military forces, but this was later withdrawn when agreement was reached on the marking requirements which would apply to such firearms. See A/AC.254/4/Add.2/Rev.5, Article 4 and footnote 55.

benefit", a reference intended to exclude from the application of the Protocol some terrorist or insurgent groups whose activities were not linked to any financial or material benefits.

There are two important limitations to this principle, however. Article 34, paragraph 2 of the Convention requires that domestic criminal offences not include as a constituent elements the involvement of an organised criminal group or transnationality. In the case of firearms trafficking, the relevant Protocol definition and criminalization provisions specifically require the inclusion of an element of transnationality, because of the nature of trafficking, which should make domestic trafficking crimes applicable to individuals regardless of whether any link to a group of any kind was established or not. The second is that, under the Convention definition, which applies to the Protocol, *mutatis mutandis* by Article 1 of the Protocol, a group which has multiple objectives will generally be an "organized criminal group" if any one of its objectives includes the pursuit of financial or other material benefit. This will probably include groups of a dual nature, who claim to be terrorist or revolutionary groups, but who also engage in organised crime activities such as large-scale trafficking in narcotic drugs or other commodities or people. More clearly, it would almost certainly include groups whose primary activities were of an organised crime nature, but who trafficked firearms for terrorist or insurgent groups on a contract or cooperative basis.

Content of the Protocol against firearms trafficking

Relationship with the parent Convention

Article 1 sets out the relationship between the Convention and the Protocol, complementing Article 37 of the Convention. The same text appears in Article 1 of the Protocols against trafficking in persons and the smuggling of migrants. These codify the basic relationship originally envisaged by the Ad Hoc Committee: that the Protocols would not function as separate, stand-alone instruments, but would contain specific material focused on specific subject-matter, supplementing the measures directed against organized crime in general by the Convention. Thus provisions of more general application such as mutual legal assistance and extradition are found only in the Convention, while material which only applies to firearms trafficking, such as the basic offences, marking and record-keeping requirements, are found in the Protocol. There is some overlap, particularly in the area of legal assistance and other forms of cooperation. The provisions of Convention Articles 18 (mutual legal assistance) and 27 (law enforcement cooperation), for example, are supplemented by Protocol Article 3, subparagraph (f) and Article 12, paragraph 4, which define the term tracing as it applies to firearms, and require States Parties to cooperate in tracing firearms.

The Protocol supplements the Convention, and provisions of the two must be interpreted together. Thus, terms such as "organised criminal group" have the same meaning as the Convention definitions when used in any of the Protocols, unless otherwise specified. Provisions of the Convention also apply to the Protocol *mutatis mutandis* unless otherwise specified or the Protocol contains provisions which specifically vary or are inconsistent with those of the Convention. All Protocol offences are also regarded as Convention offences, which makes all Convention provisions applicable to cases which involve only Protocol offences. The effect of Convention Articles 2 and 3, when taken in combination with the Protocols is that the provisions of the Convention governing extradition, mutual legal assistance and other forms of cooperation apply to the

investigation and prosecution of three categories of criminal offences: the group of four offences established by the Convention itself; other "serious crimes" under the laws of the States Parties concerned; and all offences established by the Protocols, where the relevant States are also Parties to the relevant Protocol.[1] The Conference of States Parties, which is established by Article 32 of the Convention, will have similar functions for each protocol by the application of Article 32 to the protocol in question, *mutatis mutandis*.

Purpose and scope of application

The purpose of the Protocol, stated in Article 2, which is consistent with the parallel provisions of the other instruments, is: "to promote, facilitate and strengthen cooperation… to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components, and ammunition." As noted above, Article 4, dealing with scope of application, was not concluded until the 12th and final session of the Ad Hoc Committee. Article 4, paragraph 1 includes the prevention of illicit manufacturing and the investigation and prosecution of the offences it establishes, including illicit manufacturing, illicit trafficking and additional offences in relation to firearm markings. It also incorporates the language from Articles 2 and 3 of the Convention which require the involvement of an organised criminal group and transnationality. These therefore become general conditions for applying the Protocol, but as noted above, would not extend to the establishment of criminal offences in domestic law, because Article 34, paragraph 2 of the Convention, which excludes them, also applies to the Protocol *mutatis mutandis*. The element of transnationality is then effectively re-incorporated into some of the illicit trafficking offences by the definition of "illicit trafficking" in Article 2, subparagraph (e), which requires movement "…from or across the territory of one State Party to that of another State Party…". Article 4, paragraph 2, then contains the exclusions for State and national security activities as discussed above.

Definitions

As noted above, while the scope of application of the Protocol is governed by Article 4, the scope of application to actual tangible items is governed by the definitions of "firearm", "parts and components" and "ammunition" in Article 3. Once narrowed by negotiators to exclude a range of small arms, light weapons and other military hardware, the definition of "firearm" is, as noted above, a forensic one largely inspired by the domestic gun-control laws of Canada and the United Kingdom. It did not prove practicable to make any distinction between firearms which were designed, intended or used for specific purposes such as sporting, military or other activities, although language was adopted in Article 10, paragraph 6 allowing simplified regimes for firearms temporarily imported or exported for such purposes. It was also felt necessary to exclude antique firearms and replicas of antique firearms, and negotiators faced with a range of cut-off dates in their national laws, opted for 1899, which was the latest such date seen as feasible. This ensured that countries with earlier dates would be in conformity, since a narrower class of firearms would be excluded, and ensured that very few firearms capable of automatic or semi-automatic fire would be excluded, since most of these were developed after the beginning of the 20th century.

[1] The Convention offences are participation in an organized criminal group (Art.5), money-laundering (Art.6), corruption (Art.8) and obstruction of justice (Art.23). "Serious crime" is defined in Convention Article 2, paragraph (b). The Convention does not require the establishment of "serious crimes" in domestic law, but where they exist, it applies, as between States Parties which all have the crimes in question. Generally, the combination of the three categories is referred to in the instruments as "offences covered by the Convention".

The definitions of "parts and components" and "ammunition" proved more complex because of the broad range of sub-components potentially included, the technical difficulties of applying some of the substantive requirements such as marking and record-keeping, and the range of national approaches to their regulation. Generally, it was seen as necessary to apply the basic import, export and criminalization provisions to parts and components of both firearms and ammunition to prevent traffickers from avoiding the Protocol entirely by the shipment of parts to be assembled in the destination country. At the same time, it was recognised that many parts would be impossible to control, since they are commonly used in other devices and not only in firearms, and would be impossible to mark, due to their small size. The unique marking of parts, components and individual ammunition cartridges would also have generated significant additional costs, and would have vastly increased the complexity of systems needed to keep records and trace transactions, particularly for developing countries which lack access to the latest information technologies.

The result was to narrow the definitions of both terms, and to make specific adjustments or exclusions from various substantive provisions of the Protocol. "Parts and components" are only subject to the Protocol if specifically designed for firearms and essential to their operation, and the definition lists major parts such as barrels, frames and breech blocks for greater clarity. The definition of "ammunition" nominally includes all components,[1] but only where these are already regulated by the laws of the State Party concerned. The marking requirements of Article 8 do not apply to parts, components or ammunition at all, and the record keeping requirements of Article 7 only apply to them to the extent that this is "appropriate and feasible".[2]

Criminalization requirements

The criminalization provisions of the Convention and its Protocols bridge the gap between international and domestic law. As international legal instruments, the treaties are legally binding only on those countries which become Parties by ratification or accession. As criminal justice instruments, however, they must apply to the conduct of individuals. This is achieved by provisions which require States Parties to actually implement the treaties in domestic law, using provisions which apply to the conduct of individuals, and in particular, criminal offences which provide definitions of prohibited conduct and form the basis of powers governing investigation, prosecution and adjudication. The Protocol requires States Parties to establish import-export control regimes by making laws requiring natural and legal persons within their jurisdictions to obtain permits or authorizations for their activities. All of this is then enforced by requirements to establish and enforce offences which make it a crime to import or export firearms without the necessary documents or permission, or to circumvent the control regime in other ways.

Article 5 of the Protocol establishes a series of offences relating to the illicit manufacturing of and trafficking in firearms, their parts and components, and ammunition. As with the other instruments, the substantive content of the offences established by the

[1] With the exception of modern ammunition still in the experimental stage, all firearm ammunition consists of the same elements: explosive or chemical propellant, a cartridge case which contains the propellant, one or more bullets or projectiles, and a primer, which ignites the propellant when struck by a component of the firearm, usually the firing-pin. Some countries did not regulate ammunition at all, some regulated only the assembled cartridges, and a few had regulations governing key components, usually the primer and propellant, which are dangerous even when not assembled into ammunition units.

[2] This will depend on marking practices and how they evolve in future. At present, some producers do mark major components separately to facilitate tracing and the matching of specific components to specific firearms. Almost all ammunition is marked by "headstamping" in which information is stamped into the base of each cartridge, but this generally only identifies the manufacture, type and in some cases the batch or lot involved for quality-control purposes. Industrial experts saw the unique marking of individual cartridges as not being feasible due to the very large numbers involved.

Protocol are found in the definitional provisions, in this case Article 3, subparagraphs (*d*) ("illicit manufacturing") and (*e*) ("illicit trafficking"), which States Parties are then required to criminalize by Article 5. Additional offences in relation to the removal or alteration of serial numbers are also established by Article 5, without the need for further definition.

Generally, the Protocol offences are intended to ensure that States Parties establish a legal framework within which legitimate manufacturing and transfer of firearms can be conducted, and which will allow illicit transactions to be identified to facilitate the prosecution and punishment of offenders. Firearms produced within the legal framework must be marked for the purposes of unique identification, and records which are linked to the markings must be kept in order to ensure that past transfers involving the firearm can be identified and the history of the firearm itself can be traced.

The basic conduct of illicit manufacturing and trafficking can be seen as the "central" offences established by Article 5, subparagraphs (1)(*a*) and (*b*). Each of these is in fact a group of related offences, the details of which are set out in the relevant definitions in Article 3. Illicit manufacturing, for example, includes three individual offences dealing with: the assembly of firearms from parts or components which have themselves been trafficked; manufacturing without meeting the licensing or authorization requirements established by locally-applicable laws or requirements; and manufacturing without placing identification markings which meet the requirements of Article 8 on each firearm.

Similarly the offence of illicit trafficking actually includes specific sub-offences dealing with various kinds of transfer, including import, delivery, sale and other kinds of transfer or movement, and two distinct offences: movement, transfer, etc. without the necessary import and export permits or authorizations, and movement, transfer, etc. in any case where the firearms involved are not marked in accordance with the requirements of Article 8. In addition, each of these specific offences must be made equally applicable to conduct in respect of firearms, parts and components of firearms and ammunition for firearms, with the exception of the offence of manufacturing without marking, which applies only to firearms.[1]

As noted above, the Protocol imposes no requirement, and establishes no offence, in relation to the marking of parts, components or ammunition because, as mentioned earlier, marking these was seen as impracticable. In addition to the two groups of central offences, Article 5, subparagraph (1)(*c*) establishes a further group of offences criminalizing a list of activities which render the markings on a firearm unintelligible or inaccurate, making it impossible to uniquely identify the firearm or trace it against past records created using the original marking. Under Article 5, paragraph 2, as with the Convention and other Protocols, States Parties are also required to criminalize "organizing, directing, aiding, abetting, facilitating or counselling" any Protocol offence. Attempts and participation as an accomplice must also be criminalized, but only where this is consistent with the basic concepts of the legal system of the country concerned. It should also be noted that the Protocol may also apply to any other related offence which meets the basic requirements of the definition of "serious crime" in Article 2, subparagraph (*b*) of the Convention. Such an offence could also form part of the basis of an investigation, prosecution or adjudication in accordance with both the Convention and the Protocol.

[1] See Protocol Article 3, subparagraph (d)(iii)).

Adopting these three groups of offences will ensure conformity with the criminalization requirements needed to ratify the Protocol. Depending on the state of a country's existing laws and the methods chosen to implement the licensing, record-keeping and other requirements of the Protocol, however, governments may find it necessary or desirable to consider adopting further offences. Under the record-keeping requirements of Article 7, for example, States Parties may keep the records themselves, or require others, presumably the parties to firearm-related transactions, to keep the records and make them available to facilitate tracing. Countries which keep their own records may find it desirable to establish offences for failure to report transactions to the record-keeper or for giving inaccurate information. Countries which rely on outsiders to keep records may wish to adopt offences of not keeping the necessary records or doing so in a manner or to a standard which is not adequate to support tracing. Other possible offences include the reactivation of "deactivated" firearms, the making of false statements on applications for permits or authorizations, the actual forgery or falsification of documents, and the transfer of firearms using documents which do not fully cover the source, destination, type or quantity of firearms, parts, components or ammunition involved.[1]

Confiscation, seizure and disposal (Art.6)

The subject of confiscation, forfeiture and disposal is dealt with in Convention Articles 12-14, which cover both proceeds and instrumentalities of crime. The Convention definition of "proceeds", in Article 2, subparagraph (*e*), includes "…any property derived from or obtained, directly or indirectly, through the commission of an offence". Article 12, subparagraph (1)(b) of the Convention also includes within the confiscation and seizure regime any "…property, equipment or other instrumentalities used or destined for use…" in offences covered by the Convention. These categories may include trafficked firearms as "derived or obtained" from a past trafficking offence, or "used or destined for use" in a future trafficking offence, in which case the general regime of Convention Articles 12-14 would apply, requiring countries to cooperate in matters such as identification, tracing, freezing and seizure. It is arguable that the "tracing" requirement establishes a separate requirement for States Parties to cooperate in the tracing of firearms which parallels that of Article 12, paragraph 4 of the Protocol, but which would apply to countries which are not Parties to the Protocol[2] or to firearms (such as those actually used to commit offences such as murder) involved in crimes other than trafficking. In such cases, the firearm-specific definition of "tracing" in Article 3, subparagraph (f) of the Protocol would not apply, however, and the tracing of such firearms might be of a more general nature.

The Convention regime governing seizure and confiscation applies to the Protocols, *mutatis mutandis*, and the other two Protocols make no separate mention of confiscation. In the case of firearms trafficking, however, negotiators felt it necessary to include additional provisions modifying the general policy established by the Convention. This was seen as problematic in its application to seized firearms, because the customary method of disposal for proceeds and instrumentalities is generally to sell them and use the resulting funds for legitimate State purposes or to pay compensation or restitution to victims. Where firearms are concerned, many delegations felt that the better course was to simply destroy them, thereby ensuring that they could never enter illicit commerce or be used in crime. As a result, Article 6 of the Protocol creates an exception to the general principle established by

[1] Depending on national implementing laws, importing or exporting firearms using a permit which does not actually authorize the full extent of the transaction might fall within the ambit of one of the basic offences of illicit trafficking.

[2] Where one of the countries involved in an investigation was not a Party to the Protocol against trafficking in firearms, trafficking would not be an "offence covered by the Convention" as between the States involved, but it might still be a "serious crime" within Article 2, subparagraph (b) of the Convention.

the Convention, providing that, in the case of firearms parts, components or ammunition, the property should be disposed of by destruction, and that other forms of disposal should only be used where officially authorized and where the items have been specifically marked and the disposal recorded.

Marking requirements

Critical to the overall control of trafficking in firearms is the marking of firearms to ensure that they can be uniquely identified, and the keeping of records based on the markings to support determinations of whether particular transactions conformed to domestic law and Protocol requirements and support tracing, investigation and prosecution. As noted, the marking requirements were not finalised until the 12th session of the Ad Hoc Committee, the time being needed to develop language which took into account existing marking schemes in effect in some countries and national security concerns.

The basic requirement, found in Article 8, subparagraph 1(a), is to ensure the "unique" marking of all firearms at the time of manufacture, with failure to do so designated as one of the offences of "illicit manufacturing" under Articles 3 and 5. In practice, the necessary uniqueness will depend on the application and reading of the marking in conjunction with other identifying characteristics, such as make, model, calibre or type. A handgun and a shotgun made in different countries might coincidentally bear the same serial numbers, for example, but be distinguished from one another by the other features. Two handguns of the same calibre and type made by the same manufacturer, on the other hand would not meet the Protocol requirements unless their serial numbers or other markings were different.

As noted above, most forensic experts supported the use of alphabetical or numeric characters in marking to facilitate the recognition and reading of markings, as well as the use of computer and similar systems in the creation, storage and retrieval of records, but this was not acceptable to some delegations, whose countries used other characters instead. Ultimately, it was decided to require "unique" marking using the "…name of the manufacturer, the country or place of manufacture, and the serial number" as the principal option, but to allow countries already using "simple geometric symbols" in combination with a numeric or alpha-numeric code to maintain their existing practices. This means that these States Parties may continue existing practices that are already in place, but that States Parties which have not previously used such a system must apply the other option.

Record keeping requirements

The other major requirement to support tracing, investigation and prosecution is the keeping of records. Under Article 7, records must be kept "in relation to firearms", which would include not only records of international transactions, but also some domestic activities, and in particular manufacture. Added information, such as the dates and documentary information on specific transactions or transfers must then be kept in respect of import-export transactions under Article 7, subparagraph (*b*).

Exactly what records must be kept is not specified in detail, but these must be sufficient to support the tracing or identification of firearms that have been illicitly manufactured or trafficked. As noted above, this extends to parts, components and ammunition only to the extent that this is "appropriate and feasible", in recognition of the considerable technical difficulties in affixing unique markings and in keeping records in

such cases. Ammunition or parts might be recorded and traced as part of a batch, lot or shipment, for example, but not as individual unique items, as is required for firearms.

Negotiators presented the Ad Hoc Committee with two basic record-keeping regimes, and as a result the opening language of Article 7, "Each State Party shall ensure the maintenance…[of records]…" allows the options of either having an agency of the State itself keep records using information obtained from documents such as permit applications completed by transaction parties, or requiring records to be kept by the Parties themselves. Records must be kept for not less than 10 years, which reflects a compromise between the fact that the accumulation, storage and retrieval of records consumes resources and the fact that firearms are durable and may be encountered in trafficking or other crimes many years after records are created.

Import-export requirements

As noted, the offence of "illicit trafficking" consists of international transfer without the legal authorization of all of the States concerned. To support this, Article 10, paragraph 2 contains a requirement that exporting States verify that subsequent transit and import is authorized by the States involved before they license the export itself. Article 10 also provides standard requirements for the documents involved, which provide information about the transaction and identify the firearms involved for purposes of record keeping and any subsequent tracing or other investigative inquiries. After extensive discussion about whether to require the authorization of "transit" States and how to define "transit" for the purposes of imposing such a requirement, a simpler approach was adopted in this Article. The simplified scheme requires that documents identify any transit States and that such States be notified in advance of the transit. If a transit State does not give written notice that it does not object, the exporting State cannot issue an export permit for the transaction. To address concerns about the application of the Protocol to individuals who import or export firearms for temporary use for occupational or recreational purposes, Article 10, paragraph 6 provides for "simplified procedures" in such cases.

Deactivation of firearms

In most countries, the domestic records which track firearms are purged whenever the firearms to which they apply are themselves destroyed. Problems have arisen in some cases where firearms are not completely destroyed if the records are purged and the firearms are subsequently restored and used for criminal purposes. Firearms which have been "deactivated" in ways which make them inoperable but leave them intact from a standpoint of outward appearance are popular as display items, and this process is often used to preserve firearms such as war-trophies which would otherwise be prohibited by domestic laws. To deal with the problem of reactivation, Article 9 of the Protocol contains technical standards which ensure that firearms are not considered to have been destroyed for the purposes of a State Party's licensing and record-keeping practices unless the process is essentially irreversible. Article 9, subparagraph (a) also requires essential parts to be disabled and incapable of removal from the deactivated firearm, which precludes any re-circulation of individual parts, or the assembly of new firearms using parts from deactivated ones. As noted above, countries implementing the Protocol may wish to ensure that attempts to reactivate firearms are made a crime, either specifically or by including this as a form of illicit manufacture, but this is not a Protocol requirement.

Security and preventive measures

Some illicitly trafficked firearms are manufactured directly for the illicit market, but most are firearms originally made for lawful purposes and subsequently diverted into criminal hands. To address this, Article 11 calls for security measures to prevent theft or diversion at every stage of the manufacturing, storage, import, export, transit and distribution process. Diversions are in some cases accomplished by simple theft of the firearms or corruption of officials, but a common method is the use of false documents or genuine documents into which false information has been incorporated. This is not explicitly dealt with in Article 11, but document security is arguably covered by the general requirement to increase the effectiveness of import, export and transit controls found in Article 11, subparagraph (b). It was within neither the mandate nor the intention of the Ad Hoc Committee to delve into matters of domestic gun control, but national provisions such as domestic transfer and record-keeping requirements, the licensing of firearm dealers and other participants and domestic gun control offences will also support the security of international transactions in countries which apply them.

Information-sharing and tracing

Article 12 of the Protocol parallels Articles 27-28 of the Convention, covering the exchange of information ranging from very general scientific or forensic information about firearms to specific and potentially sensitive information about organised criminal groups, their means and methods and information about specific legal or illegal transactions. The intent of the drafters was to focus the general principles of the Convention on the specific types of information and scenarios likely to be seen as important in cases of firearm trafficking, but as with other areas of the Protocol, sharing information of this nature on this particular topic raises issues of national security intelligence as well as crime-control. As previously noted, it is for this reason that Article 12, paragraph 1 refers to "…relevant case-specific information…" to clarify that the obligation is to assist fellow States Parties in dealing with specific cases and not with a more general sharing of intelligence. Further limits also recognise that information about firearms and trafficking may be sensitive, not only as security or criminal intelligence, but also from a proprietary or commercial standpoint. Article 12, paragraph 5 contains obligations, based on the language of Convention Article 18, paragraphs 5 and 20, to keep shared information confidential. Recognising that this is not always possible, particularly in countries where there are legal or constitutional requirements for prosecutors to disclose all evidence to defence lawyers, the obligation is to comply with any specific restrictions placed on the information, to keep information confidential unless disclosure is authorized by the Party which provided the information, or unless confidentiality cannot be maintained. If disclosure must be made, there is an obligation to first notify the Party which provided the information.

The other major specific requirement to share information involves assistance with the tracing of firearms, contained in Article 12, paragraph 4. Tracing is a term of art among firearms experts, and is defined in Article 3, subparagraph (f). Generally, tracing involves the unique identification of a particular firearm by make, model and other characteristics in combination with the markings on the firearm, and then using records to identify each individual or company which has owned or possessed the firearm from its manufacture to the present. Often this is not possible, either because the necessary records have not been kept or are not available, or because the firearm has been transferred illegally or without creating any records. Fortunately, such comprehensive tracing is also often not necessary, since only those individuals associated with the investigation of a crime such as illicit manufacture or trafficking, or another offence such as murder or robbery in which the

firearm was actually used, need be identified. Since the Protocol deals only with transnational trafficking and not legal or illegal transfers within a State Party, the definition of tracing will apply in practice only to the identification of firearms and parties to transactions involving initial manufacture and any subsequent export-import transactions, although Parties which maintain domestic gun control systems may also be in a position to provide domestic tracing information. As noted above, some tracing of firearms may also be required under Articles 12 and 13 of the parent Convention, to the extent that firearms may be considered as either the proceeds of a trafficking offence or as being "used or destined for use" in any offence covered by the Convention, although this may require tracing in a more general sense than the defined term of Protocol Article 3.

Brokers and brokering

Many experts have observed patterns in both legal and illegal commerce involving firearms in which those who actually arrange transactions or transfers are never actually in possession of firearms, parts, components or ammunition, and may operate from countries not otherwise connected in any way with the actual transactions.[1] This led to proposals to incorporate provisions requiring States Parties to regulate brokers and establish criminal or other offences for various forms of non-compliance. There was not sufficient consensus among delegations to support mandatory requirements, partly because of the complexity of brokering and of the provisions that would have been needed to effectively regulate it. License requirements might have applied in countries of origin, transit, destination, or in countries where the broker resided, from which he or it operated, or from which a particular transaction was arranged. They might also have involved a general license to conduct brokering activities, possibly accompanied by requirements for auditing or inspecting records, or a specific license for each transaction or transfer.[2] These possibilities then triggered further questions of what records should be kept, by whom, and in which jurisdiction(s). Ultimately, negotiators elected to insert only a discretionary provision, calling on States Parties to consider the regulation of brokers using means such as registration and licensing, but leaving the mechanics up to national legislatures and regulatory authorities.

Results of the study on the illicit manufacturing of and trafficking in explosives by criminals and their use for criminal purposes

As noted above, the subject of the illicit manufacturing of and trafficking in explosives had been included in the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and Other Related Materials, on which the original text of the Protocol was partially based,[3] and had been proposed by some delegations for inclusion in the Protocol against trafficking in firearms. Explosives *per se* were excluded at the 7th Session of the Ad Hoc Committee because they exceeded the mandate set by General Assembly Resolution 53/111, for technical reasons, and because there was not sufficient support from among delegations to include them. Explosive devices such as bombs and grenades were excluded at a later stage, during the 11th and 12th Sessions. During the course of the legal and policy debate over whether the

[1] See, for example, Wood, B. and Peleman, J. "Making the deal and moving the goods: the role of brokers and shippers", in Lumpe, L., ed., "Running Guns: The Global Black Market in Small Arms" , Zed Books, London, 2000.
[2] The question of regulating brokers was discussed at the 7th and 8th sessions of the Ad Hoc Committee. For the range of proposals made, see A/AC.254/4/Add.2/Rev.5, Article 18*bis* and footnotes 151-162. A decision to streamline the provision and make it optional was made at the 11th session, but not formally agreed until the 12th and final session. See A/AC.254/4/Add.2/Rev.6, Article 18*bis*.
[3] OAS Treaty A-63, adopted 14 November 1998. regarding the use of the OAS instrument in developing the Protocol, see GA/RES/54/127, paragraph 3.

Protocol should deal with explosives, the General Assembly was asked to consider a further mandate, under which the Secretary General was called upon to convene an expert group to study the issue, and the Ad Hoc Committee was called upon to consider the possibility of a further instrument, depending on the results of the study.[1]

The expert group was duly convened, but due to a lack of resources, its initial meeting did not take place until March of 2001, after the texts of the Convention and its Protocols had been finalised. It met twice, from 12-16 March, and 18-21 December 2001, and then reported to the 11th Session of the Commission for Crime Prevention and Criminal Justice, as required by its convening resolution, in April 2002.[2] Within the Commission, there was no consensus on the question of whether a further instrument was desirable, and the Report and Study were accepted without further action.[3]

Within the expert group, there were also a range of views about whether an instrument was needed, but most experts saw the exercise as a useful opportunity to gather information and produce analysis and recommendations which would be useful in developing national and international policy. As with firearms, the misuse of explosives straddles the boundary between crime, terrorism and national security, and the experts were aware that previous attempts to study the problem had met with government reluctance to provide information in many countries.[4] The group decided to gather information from all available sources. At its first meeting, it developed a survey questionnaire for transmission to Member States and agreed that individual members would personally research specific issues and report back to the group. The survey results were a success: a total of 50 of the 191 Member States had responded by the time the group met to review the research and draft its conclusions in December 2001, and 5 further responses were received after the Study had concluded.[5] At its second meeting, the group produced a detailed analysis of its research and a covering Report to the Crime Commission which included a series of recommendations.

In the survey questionnaire, information was sought from each country about the general availability and use of explosives, the nature and extent of explosive-related incidents, and the legal or other measures in place to deter misuse and control or regulate explosives. As expected, incident reports demonstrated a pattern in which incidents of any kind were relatively infrequent, but occasional incidents could be quite serious. This represented some statistical concerns: for example, the explosive attack on a United States government building in Oklahoma City on 19 April 1995, significantly altered statistics reported by the U.S. for the entire 5 year (1995-1999) period of the study.[6] The small numbers of "normal" incidents also meant that repeated explosive attacks by terrorist or insurgent groups significantly increased occurrence rates in countries or regions where such groups were active. Another factor noted by the study is the availability of military

[1] GA/RES/54/127 of 17 December 1999.
[2] The Report of the expert group is E/CN.15/2002/9, and the results of the Study are found in E/CN.15/2002/9/Add.1.
[3] Report of the Commission at its 11th Session, E/2002/30, paragraph 64.
[4] In particular, a previous expert group convened pursuant to GA/RES/52/38J of 9 December 1997 to study the problem of explosives and ammunition as part of more general work of the Assembly on issues relating to small arms encountered this problem. See Note by the Secretary General (Small Arms): Report of the Group of Experts on the problem of ammunition and explosives, A/54/155, paragraphs 9, 10, 22, 27, 34, 36, 38, 47, 102, 104 and 105(a) and (b).
[5] The Study indicates that 52 States took part in the Study. 50 responses were received in time to be reviewed and considered by the experts. Two further responses were received after the meeting, but in time for inclusion in the Study report, and did not affect the analysis or conclusions of the Study. Two further responses were received after the document was finalised and one further response was not received until after the Crime Commission had considered the Study. For the methodology and a list of the original responses considered, see E/CN.15/2002/9/Add.1, paragraph 14, *et seq.*
[6] E/CN.15/2002/9/Add.1, paragraphs 18, 30, footnote 11 and Table #1. The Study notes that this single incident killed more than eight times the number of Americans killed in all explosive-related incidents in an average year, more than doubling the five-year average compiled for the Study. The effect is illustrated by Table #1, which shows 5-year fatality rates calculated with and without this incident.

explosives in post-conflict regions or areas of military buildup. This was believed to be responsible for relatively high incident rates in southern Africa and parts of eastern Europe. This was particularly notable where consideration included incidents in which explosives were not actually detonated, such as incidents of theft or illegal possession.

The question of whether to consider terrorism and terrorist incidents, and if so how to define or classify terrorism, confronted the group as it has other bodies. The group noted that its mandate was to examine the illicit manufacture and misuse of explosives by "criminals" and for "criminal purposes", but it also noted that, where explosives are misused, this is considered as a crime regardless of the motives of the users or whether they are considered to be terrorists or not. Some countries made a distinction between terrorism and crime or identified specific incidents as being of a terrorist nature, but most did not. Accordingly, it was decided that, in the absence of any scientifically-valid distinction between criminal and terrorist misuse of explosives, the group would simply consider all incidents as crime, and would classify incidents as terrorist incidents if and only if they were so reported by the State concerned.[1]

The research showed that virtually all responding countries considered explosives sufficiently dangerous to warrant placing some form of restrictions or regulatory controls on basic activities such as manufacture, possession, transportation, storage and use, and most had criminal or other offences which applied when such requirements were breached. This was also illustrated by the departments or ministries tasked with developing and enforcing the regulations. The most common were ministries responsible for justice, law enforcement or internal security. Others commonly used were ministries for defence, mining, industrial development and specific areas of safety, such as transport.[2] As noted, explosive-related incidents were rare in comparision with common offences such as assault or overall crime rates, often occurring only 1-2% as frequently as crime in general. A wide range of occurrence rates was reported, with individual reports as high as 10 times the overall average rate. Those countries which reported high rates in some cases noted correlations with the activities of terrorist or organised crime groups or ease of access to explosives due to surpluses (eastern Europe) or post-conflict conditions (southern Africa). Other countries which reported high rates did not make any attribution but have raised concerns about terrorist activities in other *fora*.[3]

One of the reasons for the study was to provide information to support deliberations about whether a further international instrument should be developed or not, and if so, what the nature of such an instrument should be. This led to consideration of the extent to which reported incidents involved elements of organised crime and transnationality, and Member States were asked to provide this information. Generally, an international legal instrument would only be warranted if the problems to be dealt with were sufficiently international or transnational to require a collective response from Member States. Similarly, a further Protocol to the Convention against Transnational Organized Crime would only be feasible if such incidents were both "transnational in nature" and involved "organized criminal groups", as these are triggering conditions for the application of the Convention and its Protocols.[4] This also led to further consideration of the distinction between terrorism and crime, since the definition of "organised criminal group" in Article 2, paragraph (a) of the Convention contains language intended to exclude terrorist groups, at least in many of their activities.

[1] E/CN.15/2002/9/Add.1, paragraph 20.
[2] E/CN.15/2002/9/Add.1, paragraphs 21-24.
[3] For incident rates and analysis see E/CN.15/2002/9/Add.1, paragraphs 25-31.
[4] Convention, Articles 2-3, which apply to the Protocols, *mutatis mutandis* by Article 1 of each Protocol.

Generally, reported incidents which involved transnational elements were only a small portion of the overall reports, and most of the incidents involved conduct which the reporting State considered to be of a terrorist or insurgent nature. Misuse, and in one case illicit transnational trafficking, by conventional organised criminal groups was reported, but was not common. Several countries also reported transnational incidents without giving any information as to their nature. Countries were asked separately about whether they were concerned about smuggling or trafficking, and a number reported concerns even where no actual incidents were reported: about half of the respondents expressed concerns, but only 6 of the 50 States actually reported incidents involving either transnationality, organised crime, or both.[1]

Five of the six reports which involved either organised crime or transnationality were identified by the reporting countries as having had some link to terrorism, including one in which conventional organised crime groups were reported as being used by terrorist groups on a cooperative or contract basis to smuggle explosives or finished devices. Another factor cited in some reports was the availability of a supply of surplus military munitions. One country reported a criminal organisation which had salvaged explosives from surplus military devices and used them to produce improvised explosive devices, which were then sold to organised crime in another country.[2]

The group also noted that cases of illicit manufacture tended to involve either isolated cases of offenders, often juveniles, experimenting, or cases of sophisticated groups making large quantities or producing explosives on an ongoing basis, and that the latter also tended to be terrorist groups.[3] It also noted that, while explosives did offer some advantages to conventional organised crime for offences such as murder and "safe-cracking", the high profiles generated by detonation incidents tended to be more suitable for terrorist objectives and were often inconsistent with the interest of conventional organised crime in keeping a low profile.[4]

These results led the group to conclude that, while criminal misuse of explosives was considered by many to represent a serious threat, actual misuse was more likely to occur within a single country than across borders, with the exception of crimes committed by terrorist groups. As noted above, the group made no recommendation as to the desirability of developing of further international instrument, but it did recommend that, should such an instrument be developed, it should apply equally to all types of misuse, whether of a terrorist or criminal nature, and that it should therefore be adopted, if at all, as a separate instrument and not as a further Protocol to the Convention against Transnational Organized Crime.[5] As technical experts in the field, the group was aware of political difficulties in defining terrorism and distinguishing it from organised crime, but it saw no reason to make such a distinction in developing law or policy relating to explosives, since

[1] E/CN.15/2002/9/Add.1, paragraphs 32-35 and Tables 2 and 3.
[2] E/CN.15/2002/9/Add.1, paragraph 34.
[3] Reports of such cases were rare, but several group members had been personally involved in or were otherwise aware of incidents in which groups such as the Irish Republican Army or the Basque group ETA had produced large quantities for use in single car- or truck-bombs or had operated laboratories for ongoing production. Some of these had produced sophisticated military-type explosives, but most had produced substances which have lower detonation velocities but which use easily-available ingredients and are much simpler to produce.
[4] E/CN.15/2002/9/Add.1, paragraphs 50-51. It was also noted, although not included in the Report, that cases in which conventional organised crime groups had used explosives in high-profile applications such as the assassination of public officials might themselves be considered of a terrorist nature. One prominent example was the assassination of Giovanni Falcone by the Italian Mafia on 22 May 1992 using a large explosive device buried under the road. This allowed the attackers to circumvent security precautions, including the armoured sedan in which Judge Falcone was travelling, but was also presumably intended to send a very high-profile message to others involved in anti-Mafia efforts.
[5] E/CN.15/2002/9, paragraphs 20 and 23, and subparagraph 30(d).

virtually any detonation of explosives which caused or was intended to cause harm of any kind would generally be considered a crime regardless of motivation.

The group also considered regulatory and technical issues relating to the control of explosives. Noting that most countries already had offences and regulatory regimes, it considered elements such as licensing and made a series of recommendations for the enhancement of such regulations.[1] It also considered the feasibility of imposing controls on precursor chemicals and physical components used for the illicit manufacture of explosives or improvised explosive devices. Generally, strict legal controls on chemicals and components were not seen as feasible because these had too many non-explosive uses and because key components such as primers or detonators which did not have alternative uses were usually already regulated. The group felt that less-formal controls on some key chemicals might be feasible in some circumstances, and gave as an example the establishment of "know your customer" requirements for vendors of such chemicals similar to those used successfully against money-laundering.[2] It was noted that the alteration of chemicals such as ammonium nitrate to make them inert for explosive purposes was still under research, but ways had not yet been found to do so without adverse effects on non-explosive applications and recommended further research in this area.[3]

The group also considered ongoing efforts to develop systems for marking explosives, noting that these were different from the serial numbering of firearms. Since explosives are destroyed when used, any marking efforts had thus far consisted of either the addition of chemical substances which would ensure detection by sampling or "sniffing" equipment such as that used at airports, or the addition of small particles, threads or chemical substances intended to leave a residue after detonation which could be used to identify the explosive which had been used. These offered much less uniqueness or detail than firearm markings and could usually only provide general information about the explosive. The group noted that more detailed systems were under research and recommended that this continue.[4]

The group also noted that several countries had identified the increasing ease of access to technical information needed to make explosives and explosive devices as a concern. While such information had always been available from sources such as chemistry textbooks and military manuals, it was becoming much more widely available, particularly on the Internet. This was a concern because incidents involving children and others who would not otherwise have been able to produce explosives were likely to increase as a result. It also noted that there were both technical and legal difficulties inherent with attempts to suppress the dissemination of such information, but recommended that governments nevertheless explore legal means of discouraging the dissemination of such information.[5]

[1] E/CN.15/2002/9, paragraph 29.
[2] E/CN.15/2002/9, subparagraph 31(h).
[3] E/CN.15/2002/9, subparagraph 31(i).
[4] E/CN.15/2002/9/Add.1, paragraphs 55-63 and E/CN.15/2002/9, paragraph 26.
[5] E/CN.15/2002/9/Add.1, paragraph 33 and E/CN.15/2002/9, subparagraph 31(g).

6. Trafficking in Stolen Natural Resources, Cultural Objects, Works of Arts and Endangered Fauna and Flora

Assessing Aspects of Natural Resources Trafficking in Central Africa

JEROEN CUVELIER
International Peace Information Service

Introduction

Undoubtedly, the analysis of resource trafficking contributes to a better understanding of the procurement strategies of rebel movements and their ability and motivation(s) to survive as warring parties. The recent reports of the United Nations Panel investigating the illegal exploitation of natural resources and other forms of wealth from the Democratic Republic of Congo (DRC) are a clear case in point.[1] Through a detailed account of the multiple ways in which the military, officials and businessmen have managed to enrich themselves through the illegal trade in Congo's abundant resources such as diamonds, copper, gold, coltan and timber, the Panel has convincingly shown that 'greed' should be considered at least as important as 'grievance', when it comes to determining the root causes of the prolonged conflict in the DRC. As a result, there is a great need for measures to stop the pillage of Congo's riches. A thorough understanding of the plunderers' modus operandi is necessary to render the punitive measures of the international community as efficient and effective as possible.

The importance of natural resources for the warring factions in the DRC

Basically, there are two reasons why the belligerents in the current DRC conflict have an interest in resource trafficking. First, Congolese rebel movements are able to use the revenues from the taxes levied on the exports of mineral resources to finance their war effort and buy arms. And second, the foreign army commanders supporting the Congolese rebel movements feel more motivated to continue their military assistance, when they can combine fighting with doing business for personal benefit: in exchange for tax exemptions, the traders often allow the army commanders a share in the profits.

The worldwide dispatch of Congolese resources

Exporting through the 'official' channels

Contrary to what one would think, the rebel conquest of large parts of Eastern DRC after August 1998 (i.e. the beginning of the second Congo war) did not have a big impact on the existing administrative apparatus and mining legislation. In fact, most of the institutions and government bodies from the Mobutu era have been kept in place by the different rebel movements, with only the top levels of these structures being filled in by rebel cronies. This 'bureaucratic conservatism' has helped the rebels to focus all their attention on finding foreign business partners and introducing harsh tax measures.

For the purpose of the first part of this presentation, I will use the example of the coltan trade. Coltan is a contraction of colombo-tantalite, the name of an ore combining two

[1] Report of the UN Panel of Experts on the illegal exploitation of natural resources and other forms of wealth from the Democratic Republic of Congo (April 2001), Addendum to the report of the UN Panel of Experts (November 2001), Final Report of the UN Panel of Experts (October 2002).

rare metals with similar structures: niobium (Nb), also known as columbium, and tantalum (Ta). Before it can be used, coltan needs to be refined. Tantalum powder is used to manufacture highly heat-resistant electronic components needed for mobile phones, laptop computers, and entertainment consoles. Niobium is mostly used in heat-resistant steel and glass alloys in the construction industry. The trade in coltan grew enormously at the end of the year 2000. The reason for this expansion was the arrival of the second generation of cell phones, the so-called UMTS. Seeking to meet the growing demand on the technology market, the international trading community started a feverish search for new coltan reserves. In the Democratic Republic of Congo, this caused a veritable rush into the mining areas. In the territory controlled by the RCD-Goma rebel movement, thousands of Congolese farmers left their land to dig coltan and sell it to trading posts in Goma and Bukavu, which, in turn, offered it to international coltan traders based in Kigali.

In order to give the reader a clear idea of the complexity of the business transactions in the coltan trade and the large number of actors involved, I will discuss two specific deals, studied by researchers of the International Peace Information Service. The first transaction took place between the Congolese company Gemicom and the German company Masingiro. While Gemicom was established in April 2001 by Namegabe Mudekereza and Byaboshi Muyeye, two veteran Congolese traders, Masingiro is a German corporation run by Karl-Heinz Albers, who is also the director of the Congolese state company Somikivu. The coltan delivery arrived in Germany on 12 June 2001. The cargo left from Bukavu to Goma by ship on 9 June 2001 through the services of a certain Mr. Mihigo of the Congolese expedition company Trafca. Trafca contracted the Belgian company A.B.A.C. to fly the coltan from Goma to Ostend airport in Belgium. A.B.A.C. subcontracted Air Memphis, which leased an airplane belonging to Tristar Air. Both Air Memphis and Tristar are based in Heliopolis (Egypt). From Ostend, the coltan was transported by lorry to Masingiro in Germany through the Belgian expedition company N.V. Steinweg. From there on, it presumably went to H.C. Starck, which is reportedly Masingiro's most important consumer. The second delivery was handled by TMK (Transports et Messageries au Kivu), a company based in Goma. TMK shipped the coltan to Antwerp via the seaport of Mombassa, in Kenya. Steinweg then transported it to Germany[1].

With regard to the export of mineral resources through official channels, the following trends can be distinguished. First of all, some commodity traders appear to have negotiated exclusive business agreements with air cargo companies operating in the Great Lakes region. A good example of this is the British company 'DAS Air Cargo', which was involved in at least one preliminary agreement with the Ugandan-based Kenvic Mineral Ltd, for the transport of coltan originating from the territory controlled by the RCD-ML movement in North Kivu. Secondly, certain commodity traders have diversified their export routes, in an attempt to assure an uninterrupted supply of coltan and other mineral resources, and probably also to protect themselves against the sometimes unpredictable and inconsequent behaviour of certain central African governments. After the Tanzanian customs authorities impounded a container holding 36 barrels of presumably Congolese coltan in the port of Dar-es-Salaam[2], companies like Eagles Wings Resources International started using different harbours as points of exit, while at the same time buying coltan both from comptoirs in Eastern Congo and from trading posts in Kigali. Thirdly, the transport networks involved in the trafficking of natural resources from the DRC have gradually grown more and more complex. This is best exemplified by the vast network of air

[1] '*Supporting the war economy in the DRC: European companies and the coltan trade'*, Jeroen Cuvelier & Tim Raeymaekers, IPIS, January 2002: pp. 17-19.
[2] *'Is coltan trafficking returning* ?', 19 October 2002, The Indian Ocean Newsletter.

companies of the infamous Victor Bout. Bout is a Russian arms broker, who, in the past, supplied military equipment to embargoed non-state actors such as the Revolutionary United Front (RUF) in Sierra Leone and the UNITA rebels in Angola. He runs several airline companies, cargo charter companies and freight-forwarding companies used for shipping illicit cargo. In the DRC, Bout's planes have been transporting arms, diamonds and coltan to Congolese rebel movements such as the MLC and the RCD. Finally, some expedition companies seem to have specialized in the shipping of Congolese resources. IPIS has been able to establish that several European coltan traders have availed themselves of the services of NV Steinweg.

Smuggling

Having discussed the first level on which resource trafficking has been important for the warring factions in the Congolese war, I will now proceed by highlighting some aspects of the smuggling of mineral resources. As I already pointed out, a small group of powerful businessmen maintains strong ties with the regimes in Congo's neighbouring countries as well as with the ruling elites of the rebel movements supported by Rwanda and Uganda. I will use the example of the Ugandan-based Victoria Group to clarify the modus operandi of these smuggling networks.

In an IPIS report released in October 2002, Tim Raeymaekers described the Victoria Group as one of the companies used by top-level commanders of the UPDF to organize its looting activities in the DRC. According to the UN Panel of Experts, it is led by Muhoozi Kainerugabe, the son of President Museveni, along with Salim Saleh and his wife Jovia Akandwanaho. Significantly, almost no information is available as to the members of the Group's commercial management. However, it has been suggested that, in the Congolese towns of Kisangani and Gbadolite two Lebanese traders by the names of Mohammad Gassan and Mr. Talal are overseeing the activities of the Victoria Group, reporting on a regular basis to a central coordinator named Mr. Khalil Nazzeem Ibrahim. Besides enjoying a privileged relationship with the brother of the Ugandan President himself, the Victoria Group has also been heavily protected and supported by the Ugandan army general James Kazini. In July 1999, for instance, Kazini wrote a letter to the headquarters of the UPDF and the Congolese rebel movement MLC in eastern Congo, stating that '*the company Victoria has the authorization to do commerce in coffee, diamonds and gold in the region under your command (...) Everything that concerns the payment of this company to assure its security will be treated directly by the general headquarters in Kisangani*'[1].

On the basis of a recent Ugandan police report on a mysterious theft in Kampala, it can be assumed that, at least until very recently, the Victoria Group played a prominent role in the smuggling of diamonds from Eastern DRC. On 14 July 2000, Nasser Murtada, a courier in the Antwerp diamond business, arrived at Entebbe airport with a sealed envelope containing 550,000 USD. The money was supplied by the Antwerp-based diamond company Nami Gems and was meant to finance the purchase of a parcel of diamonds from the Victoria Group. Yet, to the great dismay of the members of Victoria, Ismail Dakhlallah, a Lebanese diamond dealer working for the diamond smuggling network, was robbed shortly after the transaction took place. Subsequently, Daklallah's partners went to the Ugandan police and told their story in great detail. Judging by the information in the latter's testimonies, the conflict diamond smuggling network set up by the Victoria Group was run by Khalil Nazzeem Ibrahim[2]. Together with another partner called Abbas Khazal, Khalil

[1] '*Network war: an introduction to Congo's privatised war economy*', Tim Raeymaekers, IPIS, October 2002: p. 15.
[2] cfr. Supra

has bought diamonds in the Congolese towns of Buta and Kisangani. The diamonds were usually exported through Picaddily Import Export, a company in Kampala which has been involved in diamond trading since 1983.

In accordance with the observations of the UN Expert Panel regarding the development and the evolution of the smuggling networks operating in eastern DRC, the diamond smuggling network of Khalil Nazzeem Ibrahim has undergone a number of significant changes over the past few years. While, in the beginning, the network used to have its own trading posts in the heart of the Congolese mineral-rich areas, it eventually decided to shift the center of its activities to Kampala, following the Kisangani wars between Rwanda and Uganda. Several sources told IPIS that diamonds have been funneled through the 'Achmed & Mr Cash' trading post in Beni, which is also said to have sold gems to the company Beldiam in Kampala. So, although it looks as if the smuggling network has ceased to exist and has withdrawn itself completely from Congolese territory, in reality, it has started operating through different channels. This change in tactics can be attributed to the evolution of the DRC conflict and, more specifically, to the withdrawal of the Ugandan troops from the occupied territory in eastern DRC. Due to the diminishing support of the UPDF, the Victoria Group has had no other option but to engage more Congolese collaborators. According to Tim Raeymaekers, the case of the Victoria Group is illustrative of the extent to which foreign military actors and other members of the elite networks have been manipulating the scramble for Congolese resources. The diamonds from the Victoria Group pass the border undeclared, to the sole profit of a limited circle of UPDF officials and their Congolese allies[1].

Some problematic aspects of the resource trade in Eastern DRC

In summing up the problematic aspects of the resource trade in Eastern DRC, it is – first of all – important to make mention of the uncertainty about corporate social responsibility and the legality of certain business transactions. For coltan traders operating in Eastern DRC, it is not always easy to know what is legal and what is not. While the first UN Report on the illegal exploitation of natural resources from the DRC strongly denounced the payment of taxes to rebel administrations – arguing that these taxes enabled the warring factions to sustain their war effort – the latest UN report suggested that it is even worse to smuggle minerals to Congo's neighboring countries. This inconsequent attitude of the international community has pushed some companies to pay taxes on a small amount of their exports, while at the same time buying smuggled minerals in the capitals of Rwanda and Uganda. A second problematic aspect of the resource trade is that, in some cases, there seem to be links between the minerals trade and the arms trade. A good example of this is the case of Aziza Kulsum aka Madame Gulamali. Between November 2000 and April 2001, Kulsum had a monopoly on the export of coltan from RCD-Goma-controlled territory, but – at an earlier stage – she had also brokered arms deals for the Burundian Hutu rebels of the CNDD-FDD. A third problematic aspect of the resource trade in DRC relates to the high profits derived from violation of sanctions. According to the UN Panel of Experts, these profits have encouraged the members of the so-called elite networks to set up new mechanisms for the continuation of the looting after the foreign occupation armies have withdrawn from the DRC. Fourthly, the working conditions of the local Congolese population are deplorable. When the coltan hype was at its peak, near the end of the year 2000, traders on the international market earned between 270 and 380 USD per pound of tantalum, while the Congolese coltan diggers were only paid 1 USD per kilo.

[1] Ibidem: p. 18.

Finally, the absence of institutions capable of monitoring the resource trade in the Great Lakes region is also highly problematic. The existing administrative institutions are not only controlled by the rebels, but also lack the financial and logistical means to exercise an effective control over the export of minerals (and the payment of taxes on these exports). This does not bode well for post-conflict reconstruction.

The tricks of the trade

As far as the transport by air is concerned, the following techniques have been identified by researchers investigating the central African resource trade: staging an emergency landing in a rebel-held area to divert a plane from its scheduled course, issuing a flight schedule for a destination other than the rebel-held area and diverting the plane as soon as it is out of reach of the radar and navigation controllers, delivering the cargo at a legitimate destination, where another plane picks it up for further delivery into an embargoed zone, and operating aircraft without visible registration marking.

Very frequently, the actors involved in resource trafficking use fraudulently obtained or fictitious documents, flight plans, pro-forma invoices or end-user certificates. In November 2001, Zulfkarali Panju was arrested in Brussels, while carrying five gold bullion bars worth 500.000 USD. Belgian police charged him with money laundering for the benefit of the RCD-Goma rebel movement. During the press conference following the arrest, Begiam Police spokesman Glenn Audenaert clarified that Panju had for four years, every two weeks, carried fake corporate invoices, along with 50kg of gold, destined for Belgium, the UK, the USA and Switzerland. Reportedly, the gold was sold and the proceeds aundered through non-resident bank accounts[1]. According to Belgian press reports, Congolese rebels owned 25 per cent of Panju's companies, in addition to levying a 0,75 per cent tax on all gold exports[2]. The revenues from the gold sales were allegedly used to purchase jeeps, busses, shoes and coats from the Belgian army, for use by the RCD-Goma rebel movement[3]. During his testimony before the Belgian Commission of Inquiry, Belgian businessman Alain Goetz acknowledged that his Antwerp company 'Tony Goetz & Zonen' had been asked to smelt Panju's gold. He added, however, that – to the best of his knowledge – Panju had always paid his taxes to the Congolese customs authorities and had also respected Belgian import legislation[4].

Conclusions

The aim of the presentation has been to illustrate the importance of resource trafficking for the understanding of the current conflict in the DRC. While, on the one hand, the taxes imposed on the mineral exports from the rebel-controlled areas have enabled the warring factions to sustain their war effort, on the other hand, a limited group of powerful businessmen has managed to use its privileged relationships with the ruling elites in the conflict zone to obtain special tax benefits and to set up smuggling networks. The chaotic situation in the occupied zones and the lack of democratic oversight have made it incredibly difficult to draw a clear line between legal and illegal economic transactions. Unfortunately, the prospects for combating the negative effects of natural resource trafficking are very

[1] '*Man arrested in Belgium with gold worth 500.000 euros from South Kivu',* 20 November 2002. Source*: http://www.allafrica.com*.
[2] '*Gerecht zoekt tweede spilfiguur in coltandossier'*, Belga, 20 November 2002.
[3] '*Belgisch leger verdient aan goudsmokkel',* De Standaard, 21 November 2002.
[4] Hearing of Alain Goetz, 6 December 2002, Belgian Commission of Inquiry on the Great Lakes.

bleak: there is a lack of local monitoring capacity, the struggle for control over Congolese resources continues unabated despite the numerous peace talks, and, finally, there is an unwillingness on the side of the international community to follow up on the recommendations of the UN Expert Panel investigating the matter of resource trafficking in central Africa.

Trafficking in Stolen Works of Art and Cultural Objects

MALCOLM KENWOOD
Recoveries Director, The Art Loss Register Limited, London

The principal observation in assessing the illicit trade in stolen works of art and cultural property is its role in the destruction of the world's cultural heritage. Such destruction occurs most obviously where historic sites or monuments are plundered for artefacts. Destruction can also occur, however, where objects are unlawfully removed from such institutions as a museum, church, municipal authority, commercial entity, sovereign State or indeed from private individuals. In each case, however, there is often a common purpose between the person, institution or entity that has lost the work of art, law enforcement agencies, insurers and commercial organisations such as The Art Loss Register to attempt to recover and enable restitution of these artefacts to their rightful owners. These efforts often extend over years or even decades, especially when dealing with looted works of art from the World War II period.

Throughout the economic turmoil of recent years and particularly in the currently depressed financial markets, cultural property has proved to be a constant hedge against any inflationary pressures. It affords criminals a high-value commodity, often poorly protected, difficult (but thankfully not impossible) to identify, that can transcend boundaries and reach those eager to deal with the discreditable and more unsuspecting members of the trade. In addition, the Art Market is truly international and its ability to deal in high value assets make it vulnerable to involvement in money laundering. Indeed two New York dealers are under investigation for offering legitimate valuable pictures to launder illicit drug money, as a result of a successful undercover sting operation.

The worldwide licit art market is a significant contributor to notional economies. A survey commissioned by The European Fine Art Federation calculates that the European market comprises of 28,600 businesses directly employing 73,600 people, accounting for 12 billion euros in 2001. The ancillary goods and services utilised virtually double these figures.

Quantifying the value of illicit cultural trade is difficult due to a variety of factors. Firstly, in these periods of economic stress many art owners who lose works of arts simply cannot afford to insure their items, or under-insure, settling on a sum, which represents a fraction of the true worth of an item. Insurers frequently are unable to separate fine art claims from other insured risks. Secondly, a high percentage of the world's law enforcement agencies fail to publish statistics relating to cultural crime. Thirdly, the illicit trade in cultural property is by its nature clandestine and therefore accurate calculations are difficult.

Nonetheless, there is a large body of evidence that suggest the enormity of the problem; the illicit trade is third in value only to drugs and arms. Published estimates of worldwide losses reflect figures in the region of 7 billion euros per annum.

It is, therefore, in this climate that The Art Loss Register (ALR) was formed in 1991 and operates. It was established largely at the behest of the Insurance and Art Market, for during the late 1970's and 1980's the value of fine art showed a dramatic increase. This trend did not go unnoticed by the criminal fraternity with a corresponding increase in theft

and insurance claims. The legitimate art market suffered adverse publicity by unwittingly selling much of the stolen art in their salesrooms.

The ALR inherited a research project database from the International Foundation of Art Research (IFAR) in New York. This was the initial step towards a global commercial database of stolen cultural property. Today this data base contains in excess of 130,000 uniquely identifiable objects.

Our offices in London, New York and Cologne receive details of stolen objects from law enforcement agencies, private owners, insurance companies, art traders, museums and galleries.

ALR staff are qualified Art Historians and possess a multi-lingual capability. We conduct due diligence for major auction houses, dealers, art fairs and prospective purchasers. We provide a complimentary service to law enforcement agencies, providing details of all matched stolen items, expert advice and confidential intelligence research. As a former specialist police officer myself, I work closely with Police and Customs globally to provide this support.

Given time constraints, I wish to demonstrate just two examples of trafficking in cultural property.

The first is a still life of fruits by Paul Cezanne, stolen from a private home in Boston, Massachusetts in 1978. The theft of a major work of art such as this provides the thief with a dilemma; media attention, law enforcement and art trade circulation would insure its notoriety as a stolen work instantaneously. Thus it would be unsaleable on the legitimate market. Therefore, it is feasible that it may pass to more expert members of the criminal fraternity. It could be traded in a commodity swap, significantly below the legitimate market value, but still have substantial value in, for example, a drugs deal. The picture could circulate within the underworld for many years, moving from country to country, and criminal organisation to organisation. The holder could consider allowing the work to remain "dormant" for a number of years before re-entering the legitimate art market at a national or international level. This may be a deliberate ploy in order to take advantage of the law of title within a given country, whereby the statute of limitations can elapse after a certain period and the item could cease to be condemned "stolen". In the case of the Cezanne, it was identified following a due diligence search by an insurance underwriter who had been approached by a man seeking to insure a paintings shipment from Russia. There followed a covert operation with law enforcement agencies, The Art Loss Register and lawyers representing the "holders" interest. Ultimately this led to the surrender of the picture, without any reward payment. The origin of the "holder" and its exact history during the twenty years remains a mystery, but the scenario of its use as a commodity tool is in little doubt. The painting was sold on behalf of our client at Sotheby's London saleroom for €27 million.

The second case relates to an Assyrian relief, valued in the region of €7 million. The looting of archaeological sites goes back to ancient times. Modern archaeology, however, relies upon a far greater range of techniques and places a far greater emphasis upon information. Archaeology is now concerned with the context of finds, with the inter-relationships between objects and their location. Many archaeologists regard the acquisition of objects through unrecorded excavation as inherently damaging and against the proper purposes of archaeology. Collectors, dealers and museum curators vehemently deny that

they are responsible for looting many of the world's cultural sites, and stress that the vast majority of the trade acts in a responsible and ethical manner. The demand for these often-priceless cultural objects on the world markets is extremely high. Many of the art-rich "source" countries are to be found in global "hotspots", i.e. involved in conflict situations. The vast profits to be gained in this trade, have not unnaturally attracted those willing to reap these benefits, such as organised criminal groups and terrorist groups. The latter is amply demonstrated by the well-publicised destruction of Afghanistan's cultural history by the Taliban. Despite this destruction vast quantities of that country's heritage were looted and are appearing on the world markets. No doubt the proceeds have been appropriately channelled.

This trend is reflected in the case of the Assyrian relief. It was submitted to The Art Loss Register for a due diligence search by a United Kingdom-based antiquities dealer earlier this year. As a commercial organisation we provide a service of issuing search certificates to the enquirer, as to the provenance of title. The certificate affords the requestor with evidence of their element of due diligence when conducting acquisitions. The judiciary in any legal proceedings increasingly examines this factor. From The Art Loss Register perspective, we are careful to word the contract to exclude any object illegally excavated or exported. In this case no doubt the dealer was confident that the relief would not appear on our database or on any police database for that matter as stolen. His assumption was correct, however, our antiquities expert identified the importance of the object and suspected that it formed part of a legal and authorised excavation in the Middle East in 1975. We contacted archaeologists in America who had worked on the project and confirmed that this tablet formed part of a major relief. They were able to provide photographic and written evidence of the provenance of this item. Armed with this information, we were able to provide evidential data to the art and antique unit at New Scotland Yard. The dealer and his associates were interviewed and fraudulent documentation seized. The source country claimed that the relief was stolen; it is strongly suspected however that its appearance on the Western art market is a funding operation for that country's regime or affiliated terrorist groups.

I am certain that a greater understanding of all of the issues and the partnership approach between commercial, governmental and law enforcement sectors can help combat these areas of criminal activity.

Illegal Trade and the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES)

JOHN M. SELLAR
Senior Enforcement Officer
CITES Secretariat

The aim of this presentation is to provide a brief overview of the Convention, the illegal trade in wildlife and its links to other criminal activities.

Background

Since time immemorial, that most dangerous of species, *homo sapiens*, has used animals and plants to his own ends. He has fed upon them, clothed himself with their skins and treated himself with their medicinal properties. Throughout the centuries of Man's existence, this exploitation of wild fauna and flora has, in essence, probably changed little.

It was not until perhaps the 1800's that Man began to reflect on the ways that he used the species with which he shares Earth. Even then, many of the first pieces of legislation adopted by 'developed' nations tended to concentrate on animal welfare issues and were designed simply to punish acts of cruelty. Initial international discussion on what we might now regard as conservation centred on the colonial powers' anxieties that the hunting of 'big game' in African range states was threatened by over-exploitation. Many people would argue that, even today, we still place too much emphasis on what has come to be known as 'megafauna'; elephants, rhino, large cats, etc.

Several forms of crime are referred to as being the second largest in the world behind drugs and this is sometimes said of wildlife crime. The CITES Secretariat no longer engages in such claims. What is not in question, though, is that unregulated wildlife trade is now the second greatest threat to endangered species in the world, behind habitat destruction.

Whilst a number of international treaties were drafted, and some even ratified, most environmentalists agree that it was with the signing of a draft convention by 21 countries, in Washington on 3 March 1973, that the first effective steps in wildlife conservation truly began at a global level. Although still known in some parts of the world as the Washington Convention, what entered into force on 1 July 1975 is more properly called the Convention on International Trade in Endangered Species of Wild Fauna and Flora. It is commonly known by its acronym of CITES.

CITES is widely regarded as one of the most successful of all conservation treaties. The mere fact that it now has 160 signatory States (known as Parties) illustrates the manner in which it has grown and continues to be viewed as relevant. 'Producer' countries appreciate that the import controls of CITES, as well as control at the place of export, offer support to their efforts to combat exploitation of their natural resources by poachers and illicit traders. On the other hand, 'consuming' nations welcome the controls that enable their legitimate dealers to obtain supplies at what should be sustainable levels.

There are a number of misconceptions about CITES. Not the least of these, and widespread amongst law enforcement officers, is that a principle aim of CITES is to ban wildlife trade. Whilst it is certainly true that the Convention recognizes, and seeks to

address, the dangers of uncontrolled trade, it should rather be viewed as a regulating mechanism for trade. Indeed, it has been noted at meetings of the Convention that "commercial trade may be beneficial to the conservation of species and ecosystems and/or to the development of local people when carried out at levels that are not detrimental to the survival of the species in question."

A vital element of the Convention is its appendices. The first three list the species controlled by CITES and determine the level of control, as follows:

- Species threatened with extinction that are or could be affected by trade (Appendix I)
- Species not necessarily in danger of extinction but which could become so if trade in them were not strictly regulated (Appendix II)
- Species which individual Parties to the Convention choose to make subject to regulations and for which the co-operation of other Parties is required in controlling trade (Appendix III).

Why enforce CITES?

- To aid conservation;
- To detect illegal trade;
- To deter illegal trade;
- To assist detection and deterrence of wildlife crime at national levels;
- To gather revenue.

Most of the above points are self-explanatory. It is important to recognize that action by importing countries, when detecting violations of the Convention, can identify illegal harvesters or dealers in exporting countries. Similarly, detections by exporting States can reveal illegal consumers and traders in other parts of the world. This is why the exchange of information and intelligence is vital, if crime and criminals are to be combated effectively.

The final bullet point, relating to revenue, is of considerable importance. Politicians and senior Police and Customs managers often say that they cannot afford to devote more resources to combating wildlife crime and illegal trade in wildlife. However, States that fail to tackle illegal trade lose considerable revenue, such as licence fees, taxes and import/export duties. Enforcement has the potential to pay for itself to a significant extent.

Illegal activities

The potential profits available illustrate why the trade is attractive to the criminal element. In many ways it replicates the narcotics trade. Drugs and wildlife often originate in 'developing' countries, are collected at relatively little cost, will be smuggled via a chain of couriers and dealers to the developed world, and then retailed to customers and end-users. All along the chain the price of the product increases, with each individual player raking off his percentage.

For instance, it may cost very little to capture an exotic bird somewhere in the Southern Hemisphere, yet there will be customers willing to pay tens of thousands of

dollars once it reaches North America or Europe. Rhino horn, used in traditional Asian medicines, may attract prices per kilogram that exceed those of heroin or cocaine.

Shawls made from the wool (called Shahtoosh) of endangered Tibetan Antelopes have been seized with individual price tags of over USD 15,000.

Experience has shown that wildlife crime may often be linked to other unlawful activities. Import inspection controls in the United States have revealed shipments of venomous snakes, each of which had condoms filled with narcotics stuffed into them. Another seizure in 2002 followed the discovery of dead beetles stuffed with amphetamines that had been shipped from the Lao People's Democratic Republic.

It is also important to acknowledge that many of the methods involved in capturing animals are inhumane, the conditions in which live species are transported and smuggled may often be worse, and that high mortality rates have been observed.

The sheer volume of international trade (in all goods, not just wildlife) makes the lives of border control staff extremely difficult. It is estimated that 225 airlines carry 450 million passengers around the world each year. Imagine how much baggage those passengers have, which potentially is liable to inspection. Customs records in Hong Kong show 16.9 million containers passed through the port in 1999. One courier express company in the Netherlands processes 60,000 items through its depot every night.

Lack of awareness, limited resources, corruption in some cases, poor training and ill-equipped Customs and Police, all combine to make life easier for the wildlife criminal. The huge number of species regulated by CITES (over 30,000) and the variety of forms which they take make distinguishing between legal or illegal shipments difficult.

In-country, many enforcement officials have to operate in conditions and terrain that are hazardous because of their physical nature, weather conditions and the presence of disease. We must also not overlook the fact that many of the animals those men and women seek to protect are extremely dangerous and take no account of the fact that the presence of those particular humans is well intentioned.

How is illegal trade conducted?

Smuggling

- Across a border without a Customs or control point.
- Across a border by hiding the specimens:
  - in luggage;
  - under clothes;
  - inside vehicles;
  - using boats and planes;
  - inside containers;
  - in crates containing dangerous animals (allegedly or not).
- By post (including eggs, parrots, birds of prey, stuffed animals and their skins, live reptiles, ivory, medicines and plants).
- By changing the appearance of the specimen.

Fraud

- By false declarations.
- By bribing officials.
- By altering or modifying genuine CITES permits and certificates.
- By forging permits, certificates, security stamps and authorizing officers' signatures.

A caviar case study

Intelligence suggests that the Russian Mafia is closely linked to illegal poaching of sturgeon fish species in the Caspian Sea and the subsequent production of caviar. Poor quality and unhygienic fish eggs are also fraudulently traded as high-grade caviar. Illegally produced caviar is then smuggled abroad. An investigation by the CITES Secretariat revealed re-exports from the United Arab Emirates of caviar of suspicious origin that had a wholesale value of over USD 20 million in one ten-month period in 2001. This, combined with other concerns, led to a recommendation by CITES for a suspension of all wildlife trade to and from the United Arab Emirates (subsequently withdrawn in November 2002). This demonstrates the effectiveness of the Convention in responding to large-scale illegal activities.

Illegal trade from the United Arab Emirates bore many of the 'classic' features of organized criminal activity, including extensive use of fraudulent and forged documentation:

- Presenting forged export permits or re-export certificates to obtain re-export certificates fraudulently.
- Making false declarations regarding the origin of specimens to obtain re-export certificates.
- Making false declarations of caviar being of pre-Convention origin.
- Making false declarations quoting genuine export permits that were subsequently cancelled or never used to trade caviar internationally.
- Re-exporting caviar from species different from those originally imported to the United Arab Emirates using both genuine and false export permits or re-export certificates.
- Re-exporting caviar in excess of the quantities originally imported, using both genuine and false CITES permits or certificates.
- Making multiple imports of caviar to the United Arab Emirates, using the same export permit to clear shipments through Customs (the export permit actually being a forgery).
- Importing shipments of caviar through smaller airports in the Emirates, when Dubai was the actual destination and it would have been more logical to use Dubai International Airport.
- Sending faxes to a CITES Management Authority and to an airline company in Asia in which the author falsely claimed to be a CITES investigator of the Russian Federation based in Dubai. Advice was given on the acceptance of re-export certificates, where a false certificate was certified as genuine and another (being used by a competing trading company) was declared as invalid. In actual fact, both certificates were invalid.

- Making threats to officials of the CITES Management Authority in the United Arab Emirates, indicating that they or their families would be killed or seriously injured if re-export certificates were not issued.

Links to other criminal or terrorist activities

The connection between trafficking in narcotics and wildlife has been mentioned above. The following is by no means an exhaustive list of other links that have been noted.

- Illegal trade in ivory has funded rebel activities, including the purchase of weapons, in Angola.
- Tiger and leopard skin trade en route to China has been 'taxed' by insurgent groups in eastern Myanmar.
- A corrupt policeman controlled couriers smuggling caviar from Poland to the United States of America.
- A corrupt Police chief in far east Russian Federation controlled sales and smuggling of tiger and leopard skins and parts to China.
- A murder in Canada was suspected of being connected with sales of bear gall bladders to an organized crime group in the Republic of Korea.
- The Russian Mafia is suspected to have been responsible for the bombing of a Federal Border Guards building in Dagestan that caused multiple deaths and injuries.
- Three officials in China, responsible for anti-poaching of Tibetan antelope, have been murdered or died in suspicious circumstances.

What is needed to combat violations of CITES?

Greater awareness of the Convention and the serious threats posed to conservation by illegal trade among:

- The public
- Traders
- CITES Management and Scientific Authorities
- Customs
- Police
- Other enforcement agencies
- Prosecutors
- The Judiciary

Increased international cooperation between relevant authorities, especially law enforcement organizations:

- The CITES Secretariat already has an excellent working relationship with ICPO-Interpol, the World Customs Organization and regional enforcement networks.
- The CITES Secretariat has established contacts with its UN colleagues in United Nations Office on Drugs and Crime and looks forward to building upon these.

Targeted inspections and seizures:

- Employing modern risk assessment and targeting techniques.
- Backed and led by 'real-time' intelligence, freely exchanged between relevant organizations.

Use of technology and science:

- Especially forensic science, including morphology, chemistry, pathology, ballistics, fingerprints, questioned document examination and DNA profiling.

Prosecutions and adequate penalties:

- Including, where appropriate, enacting adequate legislation to implement CITES.
- Ensuring that wildlife crime and illegal trade can be treated as criminal offences.

Most important of all, the political will to ensure that trafficking in wildlife is treated seriously and that resources are devoted to tackling it.

CITES successes

The CITES Secretariat, whilst acknowledging the many difficulties faced by Parties to the Convention, believes that considerable success has been achieved. The following are some of the initiatives and work it has undertaken:

- A National Legislation Project to analyse the domestic laws of Parties, to assess their legislative ability to implement the Convention adequately.
- Formal Memoranda of Understanding with ICPO-Interpol and the World Customs Organization (WCO).
- Undertaking verification, technical and enforcement assessment missions to Parties focusing on a range of issues, including trade in ivory, sturgeon and tigers.
- The distribution of Alerts to CITES Management Authorities, Interpol, WCO and national enforcement agencies containing intelligence and targeting advice on current illegal trade activities.
- The preparation and delivery of specialized training and training materials at international and regional levels, often in conjunction with enforcement agency partners.
- The appointment in the CITES Secretariat of specialized staff, including lawyers, ex-prosecutors and senior police and specialized enforcement officers.
- The recent establishment of an international repository for ballistic evidence to help identify and combat cross-border illegal killing of endangered species.

7. Trafficking in Human Beings and Smuggling of Migrants

Human Rights and Human Trafficking

BERTRAND G. RAMCHARAN
Deputy UN High Commissioner for Human Rights

Overview

Trafficking in persons

One of the most serious human rights challenges facing the international community today is the phenomenon of human trafficking and the host of problems it represents: migration, organized crime, prostitution, security, labor, and health. The sheer scope of the scourge almost defies description. Every year millions of individuals - the overwhelming majority women and children from less developed countries - are tricked, sold, forced or otherwise coerced into situations of exploitation. They become the commodities of a transnational industry which generates billions of dollars and, almost without exception, operates with impunity and occasionally with official complicity. Research has confirmed a rapid increase in the incidence and extent of such practices, as well as their systematic nature and exploitative effects.

The human rights implications of trafficking are beyond dispute. Trafficking and related practices such as debt bondage, forced prostitution and forced labour are associated with slavery, and are accompanied by multiple violations of a whole spectrum of fundamental human rights resulting in lives devastated. The right to life; the right to dignity and security; to be free from torture and other ill treatment; the right to just and favourable conditions of work; the right to health, and the right to equality are fundamental rights, which all individuals possess – irrespective of their sex, nationality, social status, occupation, or other difference. Trafficking is the very antithesis of the Universal Declaration of Human Rights and, in this sense, it represents one of the most comprehensive challenges to human rights in the world today.

Women and girls are the individuals most vulnerable to trafficking which has already been identified as a form of gender-based violence. The reality is that they too often become doubly victimized as a result of their status as trafficking victims. In most parts of the world, trafficked women are initially jailed and then deported without much consideration for their needs or desires. Jail, deportation and confinement in homes are usually the price they pay for freedom.

The Causes of Trafficking

Root causes of human trafficking are complex and vary from situation to situation. The most commonly cited contributing factors include:

- Economic factors: such as poverty, food scarcity, unemployment and indebtedness;
- Social and cultural factors: including domestic violence, gender discrimination in the family and the community and by the State, and protracted social conflicts;
- Political and legal factors: increasingly restrictive and exclusionary immigration policies, scarcity of appropriate legislation and weakness of its enforcement, lack of

political will, public sector corruption, governmental hypocrisy over prostitution policies;
- Market factors: demand caused by the rapidly expanding global sex industry;
- International factors: the growing feminisation of labour migration, increased power and involvement of transnational organized criminal networks.

Overall, human trafficking is not only the cause of human rights violations - it is itself the result of widespread poverty, discrimination and social exclusion, which undermine the dignity and deny enjoyment of human rights, ruining the lives and destroying the choices of many of the world's women, men and children.

Responses to Trafficking

For these reasons the issue of trafficking is now high on the international human rights agenda and Governments, non-governmental organizations and United Nations bodies are becoming increasingly involved in the search for effective solutions. One reason for this is the connection between trafficking and smuggling of migrants. The link between trafficking and organized crime is another factor which has prompted anti- trafficking efforts at the national level and mobilised action at the international level. The organized crime and migration perspectives became a motivating force behind a number of recent legislative initiatives including the two protocols supplementing the United Nations Convention against Transnational Organized Crime. At regional and national levels, similar initiatives have resulted in the adoption of the South Asian Association for Regional Cooperation Convention(SAARC) on Preventing and Combating Trafficking in Women and Children for Prostitution, the possible drafting of a convention by the Council of Europe, or the adoption of the European Union Framework Decision on Combating Trafficking in Human Beings and of US legislation to combat trafficking for sexual purposes. For some States and for large sectors of the relevant NGO community, the human rights and gender dimensions of the problem have provided the impetus for action.

Despite this increased attention to the problem (and perhaps because of different perceptions and approaches on how to address it), attempts to deal with trafficking and related exploitation at the national, regional and international levels have not been effective. Overall, current efforts reveal a tendency to give insufficient attention to the human rights and gender dimensions of trafficking. As a result, the rights of trafficked persons and the human rights violations, which are a root cause of the trafficking phenomenon, are still not adequately addressed.

Ohchr Focus on Trafficking

Mandate

The High Commissioner for Human Rights and his Office are committed to working for the elimination of trafficking in human beings, especially women and children, in response to the following imperatives:

- The High Commissioner is mandated to provide leadership and substantive support in ensuring that human rights principles are integrated throughout the entire UN system, in accordance with Secretary-General Kofi Annan's 1997 and 2002 UN

reform proposals. The issue of trafficking provides a concrete case of the critical role which the High Commissioner can play in this broader process, as well as on the specific issue of trafficking.

- The overarching priorities of the Office of the High Commissioner derive from the 1993 Vienna Declaration and Programme of Action and the UN Charter, as reflected in the UN "Medium Term Plan". It contains a wide-ranging mandate, which includes, inter alia, promoting the right to development, increasing recognition of economic, social and cultural rights, integrating the rights of women and girls into the UN system, all of which have direct bearing on the "solution" of the trafficking phenomenon.
- Trafficking has emerged as a compelling human rights issue and no other UN agency focuses on trafficking from the standpoint of the human rights of the victims. Both the UN General Assembly and the Commission on Human Rights have recently emphasized the critical human rights dimensions of the problem of trafficking in women and children. The Office has both the regional expertise (in high-trafficking areas such as Cambodia and Bosnia, where it has field presences) and the expertise in the wide range of human rights violations involved, to be actively involved on this issue.
- There is a need for a coordinated and comprehensive effort to address what is the paradigmatic "international human rights" problem, especially in terms of development and clarification of international legal standards. The only way to combat such a problem is through effective international cooperation that is based on a comprehensive, long-term strategy which gives priority to human rights.

Activities

The work of the High Commissioner for Human Rights in the area of trafficking is based on two fundamental principles:

- that human rights must be at the core of any credible anti-trafficking strategy; and
- that such strategies must be developed and implemented from the perspective of those who most need their human rights protected and promoted.

OHCHR action takes place on two fronts. Firstly, the Office continues to provide support to the relevant mechanisms dealing with trafficking and related issues, such as the independent expert bodies that monitor the implementation of the core human rights treaties (notably, the Committee on the Elimination of Discrimination against Women, the Committee on the Rights of the Child, Human Rights Committee, and Committee on Economic, Social and Cultural Rights), the special rapporteurs of the Commission on Human Rights (notably, the Special Rapporteur on violence against women, Special Rapporteur on the sale of children, child prostitution and child pornography, and Special Rapporteur on the human rights of migrants) and subsidiary bodies of the Commission on Human Rights (notably, the Working Group on Contemporary Forms of Slavery). All of these mechanisms are serviced by the Office of the High Commissioner for Human Rights and involved in addressing the trafficking of women and children in the context of their respective mandates.

On a second front, OHCHR has developed a specific anti-trafficking programme. Its objective is to work towards the integration of human rights into international, regional and national anti-trafficking initiatives. The emphasis is on the development and promotion

of legal standards and on providing policy advice. The programme does not undertake large projects or otherwise duplicates the various initiatives which are being undertaken elsewhere. Instead, the Office endeavours to act as a catalyst and a support for the work of others and seeks to work, whenever possible, in collaboration with other UN agencies. OHCHR action is essential because trafficking is too often seen not as a human rights issue, but in terms of only migration, or organized crime, or development, or public order. The High Commissioner uses his voice to ensure that UN agencies adopt a human rights approach when they address trafficking.

At the international level, the Office focused a great deal of attention on the negotiation of the Protocol Supplementing the Convention against Transnational Organized Crime. An informal note by the High Commissioner, analysing the instrument from a human rights perspective, was submitted to the Ad Hoc Committee drafting the Convention and its two Protocols. Calls for increased attention to human rights in the Palermo protocols were accepted by those Governments involved in the drafting process, as well as by UN agencies, including Centre for International Crime Prevention as well as ILO, UNHCR, UNICEF, or IOM. This resulted in the adoption of an instrument, the Palermo Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, which has become a crucial reference for international legal standards regarding the protection of the rights of victims of trafficking. OHCHR welcomed the adoption of the Protocol and looks forward to its entry into force and to the preparation of a legislative Guide for its implementation.

At the regional and sub-regional levels, OHCHR has undertaken a number of different activities, especially in Europe and Asia. The Office provided input to the formulation of the SAARC Convention and the EU Framework Directive. Within Europe, OHCHR has worked in partnership with UN agencies, as well as the Council of Europe and the Organization for Security and Co-operation in Europe(OSCE) Office for Democratic Institutions and Human Rights (ODIHR) to develop rights-based trafficking prevention programmes in Eastern and Central Europe comprising a series of awareness-raising and training activities which target vulnerable groups, in particular, refugees and displaced women and girls. Through its field office in Sarajevo and in conjunction with local NGOs, the UN Mission in Bosnia and Herzegovina (UNMIBH) and other international organizations, including IOM, OHCHR is involved in UN system-wide activities intended to assist victims of trafficking, to facilitate the prosecution of traffickers and to promote law reform and governmental responsibility.

In Asia, OHCHR has focused particularly on Nepal and Cambodia. A series of workshops organized in Nepal in 1999 resulted in the formulation of recommendations to the Government, civil society and the UN system for dealing with the problem, as well as in the development of a pilot human rights-based anti-trafficking project. OHCHR has also been involved in the UN system Project against Trafficking for the Mekong Sub-region.

OHCHR has also encouraged national human rights institutions - particularly human rights commissions of the Asia-Pacific region - to take up the issue of trafficking. The Office also established an IGO Contact Group on Trafficking and Migrant Smuggling involving several of the key UN/ IGO agencies and programmes dealing with trafficking (including IOM, ILO, UNICEF, UNHCR, etc.). Consultations have been organized with the international NGO community active on the trafficking issue, including on "Trafficking and the Global Sex Industry".

In July 2002, the High Commissioner adopted "Recommended Principles and Guidelines on Human Rights and Human Trafficking", a basic tool providing guidance on the adoption of rights-based approaches to the prevention of trafficking of human beings and the protection and assistance to its victims. The Recommended Principles and Guidelines are already being used as a reference for the work of several UN agencies, as well as for work carried out within the European Union. The Office is preparing a legal commentary that will elaborate further on the international legal standards underpinning the principles regarding the adoption of rights-based approaches to combating trafficking, including those contained in the Palermo Protocol, as well as in the Optional Protocol to the Convention on the Rights of the Child(CRC) on Sale of Children, Child Prostitution and Child Pornography and other human rights, anti-slavery and other international treaties.

Towards a Rights-Based Approach to Trafficking

A consistent and concerted approach to trafficking presupposes, above all, a common understanding of the problem and general agreement on preferred approaches and solutions. OHCHR acknowledges that trafficking is not one event but a series of constitutive acts and circumstances implicating a wide range of actors. It is essential to ensure that anti-trafficking measures take account of this fact and that efforts are made to address the entire cycle of trafficking. This will involve improving the information base, ensuring an adequate legal framework and effective law enforcement, prevention, which addresses the causes of economic deprivation, protection and support for trafficked persons, cooperation and coordination between national, regional and international responses.

In developing detailed responses to each stage of the trafficking cycle, it is essential that certain very basic policy principles guide and inform any anti-trafficking initiative. These principles must ensure a uniform adherence to a human rights-based approach and can also provide with a means of measuring the success of anti-trafficking measures.

State Responsibilities

While private individuals and groups are primarily responsible for trafficking, States have legal responsibility under international law to protect and promote the rights of all persons within their jurisdiction. This responsibility translates into a legal obligation on governments to work towards eliminating trafficking and related exploitation, by:

- addressing the root and immediate causes of trafficking, through, inter alia, dealing with economic conditions;
- strengthening and harmonizing existing legislation with a view to providing better respect and protection of all human rights and fundamental freedoms for victims of trafficking, criminalizing trafficking in persons in all its forms, and punishing perpetrators, including intermediaries;
- ensuring that legislation, policies and programmes related to combating trafficking are gender and child-sensitive.

This responsibility must be undertaken with sufficient clarity and flexibility to deal with new forms of trafficking as and when they arise.

Definitional Aspects

The Palermo Protocol made a major contribution to the development of international law, by providing in its article 3 a clear and recently agreed international legal definition of trafficking. The lack of such an agreed definition had been a fundamental drawback in addressing the problem.

That definition allows clearer distinctions between trafficking and migration, trafficking and smuggling, trafficking and illegal migration, and trafficking and prostitution. Law enforcement efforts must differentiate clearly among those concepts and identify clearly those who need protection.

Basic elements of the definition of trafficking, from a human rights perspective, include:

- The element of exploitation, as an end purpose of the trafficking cycle, is a key concept which refers to conditions of slavery, forced and/or bonded labour, and servitude that violate the fundamental human rights of trafficked persons. The term "servitude" when used in this context should be understood to include practices which have been elsewhere defined as "contemporary forms of slavery", such as forced prostitution.
- The element of coercion, be it in the form of the threat or use of force, violence, abduction, fraud, deception, coercion, or abuse of authority, or the use of other means which may take place at any point of the trafficking process.
- The element of engagement by use of various methods including but not limited to sale or purchase, through commercial marriage bureaus, job recruitment agencies, Internet, etc., all of which may be broadly referred to as recruitment.
- The element of transportation, either within national or across international borders, which often results in the increased vulnerability of the trafficked persons vis-à-vis the protection of their human rights due to their dislocation. As such, it refers to transportation, transfer, harbouring or receipt of a person being trafficked and should be viewed in a broader context of migrations.

Trafficking constitutes a specific human rights violation, which consists of a four-element process involving recruitment and transportation of persons under conditions of coercion to put them in servile and exploitative situations. Such a definition legally distinguishes it from its component parts, which are themselves distinct violations of both national and international law.

The definition adopted in the Palermo Protocol is particularly valuable because it also reflects existing international human rights standards with regards to children, consistent with the Convention on the Rights of the Child and its Optional Protocol on sale of children.

Protection and Assistance

The protection of the human rights and dignity of trafficked persons must be given the highest priority. Under international law, victims of human rights violations should be provided with access to adequate and appropriate remedies. At a minimum, States should:

- provide information to trafficking victims on the possibilities of obtaining remedies, including compensation for trafficking and other criminal acts to which they have been subjected to, and
- render assistance to such victims, giving particular attention to the special needs of children, to enable them to obtain the remedies to which they are entitled.

Within the scope of protection and assistance to trafficked persons as victims of serious human rights abuses:

- trafficking victims should not be criminalized for the involuntary illegality of their entry or residence in countries of transit and destination, or for the involuntary activities they perform as a consequence of their status as trafficked persons;
- victims of trafficking, including those with "illegal" immigration status, should be granted protection and necessary physical and psychological care by the authorities of the involved countries;
- they should be provided with legal and other assistance in the course of any criminal, civil, and other actions against traffickers / exploiters, including a temporary or permanent residence permit and a safe shelter.

Children (all those under eighteen) have special rights under international human rights law and the special needs of child victims of trafficking must be recognized and protected:

- in dealing with child victims of trafficking, the best interests of the child are to be at all times paramount;
- clear recognition must be given to fighting impunity of those responsible and at the same time ensuring that the child is not criminalized in any way;
- assistance and protection of child victims of trafficking should not be made discretionary or otherwise dependant on the decision of national authorities. In accordance with Article 2 of the CRC, child victims of trafficking are entitled to the same protection as nationals of the receiving State in all matters including those relating to protection of their privacy and physical and moral integrity.

Traffickers and their collaborators must be prosecuted and adequately penalized paying full attention to due process rights and without compromising the rights of the victims.

Return and Repatriation

Safe and, as far as possible, voluntary return, instead of forced deportation and repatriation, must be at the core of any credible protection strategy for trafficked persons, particularly in cases of involvement of organized criminal groups.

The identification of an individual as a trafficked person must be sufficient to ensure that immediate expulsion against the will of the victim does not occur and that protection and assistance must become immediately available.

Women and children should be treated differently in the identification, rescue and repatriation process. Women have the right to personal autonomy and should not be treated as the objects of protection.

Border Measures

The strengthening of border controls is clearly an important aspect of preventing trafficking, however such measures should not operate to restrain the free movement of the persons who are in need of protection as a result of being trafficked. Given that the majority of trafficked persons are women and girls, the imposition of restrictions would be, *prima facie*, discriminatory. Therefore, emphasis should be placed on measures which will assist border authorities in identifying and protecting victims as well as intercepting traffickers.

While States have a legitimate interest in strengthening border controls in order to detect and prevent trafficking, these measures should not impinge upon human rights of individuals as set out in the major international instruments, including the International Covenant on Civil and Political Rights, the Convention on the Rights of the Child and the Convention and Protocol relating to the Status of Refugees. It is especially important to ensure that border measures do not limit the right of individuals to seek in other countries asylum from persecution as provided for under the Refugee Convention. In particular, the fundamental principle of *non-refoulement* must not be undermined.

Prevention

It is important that prevention measures be based on an understanding and acceptance of the root causes of trafficking. Of critical importance are campaigns aimed at providing accurate information about opportunities, limitations and rights in the event of migration so as to enable women and men to make informed decisions and to prevent them from becoming victims of trafficking. Discrimination should not become an unintended side-effect of preventive efforts which may entail repressive repercussions on the already precarious position of women, e.g., by restricting their freedom of movement.

Concluding Remarks

The experience of the Office of the High Commissioner and others involved in anti-trafficking initiatives shows that law enforcement must emphasize the protection of victims. Without ensuring protection for and assistance to women, men and children who have been trafficked, there is little likelihood of ensuring their cooperation. Without adequate provision for protection and assistance, victims will be reluctant to approach law enforcement officials and identify themselves or denounce traffickers, for fear of prosecution – including for offences such as illegal entry or residence - or fear of reprisals from the criminal networks involved in trafficking. The result is that lack of provision for protection of and assistance to victims makes law enforcement and crime prevention infinitely harder given the absence of evidence.

Trafficking is a complex issue, and efforts to address it should take into account the different political contexts and the geographical dimensions of the problem, the ideological and conceptual differences of approach, the mobility and adaptability of traffickers, the different situations and needs of trafficked persons, the still inadequate development of a comprehensive legal framework, and the insufficient research and co-ordination on the part of the actors involved, both at the national and international levels. Given these complexities, there will be no quick or easy solutions. Elimination of trafficking will require holistic, interdisciplinary, and long-term approaches which address each aspect of the trafficking cycle and which explicitly recognize the links between trafficking, migration and transnational organized crime. Human rights are not a separate consideration or an

"additional" perspective. They are the common frame that should unite all anti-trafficking efforts animated by a host of various players. The High Commissioner's "Recommended Principles and Guidelines on Human Rights and Human Trafficking" represent a contribution to the identification of the basic principles on which that common frame must be built.

Annex – Recommended Principles on Human Rights and Human Trafficking[1]

The primacy of human rights

1. The human rights of trafficked persons shall be at the centre of all efforts to prevent and combat trafficking and to protect, assist and provide redress to victims.

2. States have a responsibility under international law to act with due diligence to prevent trafficking, to investigate and prosecute traffickers and to assist and protect trafficked persons.

3. Anti-trafficking measures shall not adversely affect the human rights and dignity of persons, in particular the rights of those who have been trafficked, and of migrants, internally displaced persons, refugees and asylum-seekers.

Preventing trafficking

4. Strategies aimed at preventing trafficking shall address demand as a root cause of trafficking.

5. States and intergovernmental organizations shall ensure that their interventions address the factors that increase vulnerability to trafficking, including inequality, poverty and all forms of discrimination.

6. States shall exercise due diligence in identifying and eradicating public-sector involvement or complicity in trafficking. All public officials suspected of being implicated in trafficking shall be investigated, tried and, if convicted, appropriately punished.

Protection and assistance

7. Trafficked persons shall not be detained, charged or prosecuted for the illegality of their entry into or residence in countries of transit and destination, or for their involvement in unlawful activities to the extent that such involvement is a direct consequence of their situation as trafficked persons.

8. States shall ensure that trafficked persons are protected from further exploitation and harm and have access to adequate physical and psychological care. Such protection and care shall not be made conditional upon the capacity or willingness of the trafficked person to cooperate in legal proceedings.

9. Legal and other assistance shall be provided to trafficked persons for the duration of any criminal, civil or other actions against suspected traffickers. States shall provide protection and temporary residence permits to victims and witnesses during legal proceedings.

10. Children who are victims of trafficking shall be identified as such. Their best interests shall be considered paramount at all times. Child victims of trafficking shall be provided with appropriate assistance and protection. Full account shall be taken of their special vulnerabilities, rights and needs.

11. Safe (and, to the extent possible, voluntary) return shall be guaranteed to trafficked persons by both the receiving State and the State of origin. Trafficked persons shall be offered legal alternatives to

[1] As contained, together with the more detailed «Recommended Guidelines on Human Rights and Human Trafficking » in UN doc. E/2002/68/Add.1 or available in the website of the Office of the High Commissioner for Human Rights, see http://www.unhchr.ch/women/focus-trafficking.html.

repatriation in cases where it is reasonable to conclude that such repatriation would pose a serious risk to their safety and/or to the safety of their families.

Criminalization, punishment and redress

12. States shall adopt appropriate legislative and other measures necessary to establish, as criminal offences, trafficking, its component acts[1] and related conduct.[2]

13. States shall effectively investigate, prosecute and adjudicate trafficking, including its component acts and related conduct, whether committed by governmental or by non-State actors.

14. States shall ensure that trafficking, its component acts and related offences constitute extraditable offences under national law and extradition treaties. States shall cooperate to ensure that the appropriate extradition procedures are followed in accordance with international law.

15. Effective and proportionate sanctions shall be applied to individuals and legal persons found guilty of trafficking or of its component or related offences.

16. States shall, in appropriate cases, freeze and confiscate the assets of individuals and legal persons involved in trafficking. To the extent possible, confiscated assets shall be used to support and compensate victims of trafficking.

17. States shall ensure that trafficked persons are given access to effective and appropriate legal remedies.

[1] For the purposes of the present Principles and Guidelines, the "component acts" and "component offences" of trafficking are understood to include the recruitment, transportation, transfer, harbouring or receipt of persons over eighteen years of age by means of threat, force, coercion or deception for the purpose of exploitation. The recruitment, transportation, transfer, harbouring or receipt of a person under eighteen years of age constitute component acts and component offences of trafficking in children. Source: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, articles 3 (a) and 3 (c).

[2] For the purposes of the present Principles and Guidelines, conduct and offences "related to" trafficking are understood to include: exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery and servitude. Source: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, article 3 (a).

Trafficking in Human Beings

NANCY ELY-RAPHEL
Director, Office to Monitor and Combat Trafficking in Persons at the Department of State, USA

Of all the transnational crimes, trafficking in persons is the most insidious because traffickers heartlessly convert human lives and misery into quick cash. With surprising ease and so far great success, traffickers are essentially enslaving people into sexual or labor exploitation on every continent. Often, those captors are already involved in other transnational or organized crimes. From Latin American drug cartels to Eastern European mafias to the Japanese Yakuza and Chinese Triads, trafficking in persons is proving to be a lucrative business.

"Trafficking in Persons", as it is called, is something of a euphemism. Like many "catchall" phrases in popular currency that minimize or conceal complex problems, the term itself falls short of self-definition. This helps account for public awareness or bewilderment as to what it means. "Trafficking in persons" is the exploitation of human beings, a form of commerce in which the only value of an individual is measured by the price he or she can be sold for, like soybeans, livestock or oil futures. Such so-called commerce violates every moral principle that governs our societies.

Trafficking exists in almost every society where you find vulnerable populations and the victims are typically women and children. These people may be economic migrants, political asylum seekers, those rendered homeless or jobless after natural disasters or civil conflict, or individuals looking for a better way of life. Many times, traffickers are successful at taking advantage of these vulnerable populations because the traffickers' links with other transnational crimes such as trafficking in arms, drugs and other contraband have provided them with safe and tested routes, access to cash, and known corrupt officials to bribe. Many times, they trick their victims into travelling to another country, where they are promised a better life.

In the Balkans, trafficking of women for prostitution is now a larger business than heroin, although organized crime groups continue to do both. Italian authorities report that boats have been intercepted in the Adriatic with a combination of illegal weapons, tobacco, heroin and women. We also see the collaboration of crime groups in different countries, for example, Romanian, Moldovan, and Serbian criminals cooperate to traffic women and girls from Romania and Moldova to the Balkans. In the United States, Immigration and Naturalization Service raids on trafficker-controlled brothels have also netted heroin and counterfeit currency. The Wah Ching, an Asian organized crime group engaged in smuggling and trafficking in Asian women, is also involved in murder, robbery, gambling, drug trafficking and loan sharking.

Because we are often targeting the same criminals, those that address trafficking in humans must work closely with those who work on other trafficking crimes. We must share best practices and intelligence on the bad guys. We must tighten border controls and wipe out corruption. We must work together where we can and be aware of innovations in our respective fields to be the most effective. We must coordinate because the criminals are certainly doing it and so far, they are doing better than we are.

As with trafficking in arms or drugs, combating trafficking in persons cannot be successful without effective law enforcement. In most countries, including the United States, that means looking at legislation to make sure adequate laws and tough penalties are in place. The United States law known as the "Trafficking Victims Protection Act of 2000" provides a comprehensive approach to eliminating trafficking in persons through a three-pronged strategy: prevention of trafficking, prosecution of traffickers, and protection and assistance for victims.

The law does a number of things. First, it creates a definition of trafficking that gets at the whole pipeline of trafficking activity including the recruiter, transporter, buyer, seller, harborer, brothel owner, and manager. Second, it increases the maximum penalties from 5 years to 20 years or even life imprisonment and allows victims to seek compensation for damages from the traffickers. This is important because it sends a message to traffickers that we take human trafficking seriously – and that the penalties will be commensurate with the crime. Third, it incorporates a victim-centered approach, which treats the victim like a victim not a criminal. It includes a new status for victims of severe forms of trafficking which allows them to stay in the US while they are helping prosecute their traffickers, and provides for shelters and services.

But for most countries, new legislation is not enough. There is also a need for training police, judges, and prosecutors on implementation of laws, investigation techniques, preserving of evidence and appropriate treatment of victims. The US Department of Justice conducts training and gives classes to many foreign police forces and judiciaries. The US Department of State has sponsored programs through other organizations including a very successful initiative by the United Nations Center for International Crime Prevention with the Government of the Philippines.

Additionally, I cannot stress enough the need for Governments to confront the rampant corruption which allows all traffickers to flourish. This is as much an issue of political will as law enforcement. The lure of easy money for underpaid officials and a sexist culture in which some officials believe a woman's places in the brothel help keep trafficking alive and well. Governments must take aggressive steps to end these crimes.

Finally, with respect to law enforcement, foreign Governments and police forces must cooperate with each other. That means collaborating on investigations, extraditing traffickers, improving border control and doing a better job of monitoring and documenting migration flows.

What makes trafficking in people distinct from other trafficking crimes is the victim. It is not enough to simply put traffickers behind bars. We have the challenge of educating vulnerable populations, and protecting and reintegrating victims so they can become healthy, productive members of society and also provide testimony against their traffickers. In those efforts, NGOs can play an important role and be even more effective when Governments collaborate with them.

We need to promote strategic public-private partnerships between Governments and NGOs worldwide. Practically speaking, many governmental bureaucracies are often unable to provide the long-term, personal assistance that victims need to recover from their extraordinary physical and emotional trauma. By contrast, specialized NGOs are often best suited to meet these demands. Some governments with limited resources have bolstered anti-trafficking efforts by providing in-kind assistance to NGOs, such as providing office

space in a government-owned building. Wealthier governments can assist NGOs doing good work that operate on a shoestring budget.

Many times, victims do not bring cases against their traffickers out of fear or distrust of the police. Some NGOs may facilitate judicial processes by reaching out to traumatized victims and providing legal services for those who are afraid or do not understand their legal options. In some countries, such as Thailand and Brazil, NGOs have helped train and sensitize police so that victims are treated as victims, not criminals.

All around the world, experienced advocates rightly contend that without appropriate prevention and protection measures, the "rescued" victim is likely to fall back into desperate straits. While prosecutors in the United States have begun seeking indictments under the new anti-trafficking law, we are also funding programs to protect and assist victims. New requirements include victim access to legal information and translation services, and training for government officials responsible for these cases.

In recognition of the need to take a comprehensive approach to fighting trafficking in persons, the United States created the President's Interagency Task Force to Monitor and Combat trafficking in Persons. This Cabinet-level task force is chaired by the Secretary of State and its other members include the Attorney General, the Secretary of Health and Human Servics, the Secretary of Labor and the heads of the United States Agency for International Development and the Central Intelligence Agency. The Task Force's responsibilities include overseeing the development of strategy, planning and implementation of domestic and international policies to combat trafficking in persons.

The State Department's Office to Combat and Monitor Trafficking in Persons is the Secretariat for the task force. The office works through diplomatic channels to encourage other coutries to improve efforts and increase bilateral and regional cooperation. The annual Trafficking in Persons Report is one of the major foreign policy tools to help increase our dialogue with other countries and provide an impetus for serious action. This year's report lists 89 countries and is the most comprehensive international review of anti-trafficking efforts issued by any single government. The office also has a section for international programs which supports governments' and NGOs' efforts to improve prevention, law enforcement and victim protection efforts. We work closely with the UN Center for International Crime Prevention, and in fiscal year 2002 have contributed nearly one million US dollars towards the Center's worldwide technical assistance activities. In terms of public outreach, the office participates in numerous public events and is sponsoring, in collaboration with a consortium of NGOs, an international conference on trafficking in persons in Washington DC February 2003.

In closing, I want to urge you to share best practices with those of us who are working to stop all forms of trafficking. We must employ every tool in our arsenal against organized crime groups to shut down their organizations, assist victims and prevent those vulnerable populations from ever falling prey to their horrible crimes.

The Nature and Logistics of Trafficking in Human Beings

IRENA OMELANIUK
Director, Migration Management Services,
International Organization for Migration

The International Organization for Migration is not a United Nations organization, but we work very closely with most United Nations agencies, in particular in the field of counter trafficking and to a certain extent also in combating the smuggling of migrants.

We come to the issue of smuggling and trafficking from the perspective of migration management. We find that on the ground, for example, the distinction between smuggling and trafficking is rather blurred. People are often smuggled or trafficked for the same reason. They are looking for work, and for better life prospects. We find that the two Protocols supplementing the Palermo Convention are probably the most useful international instruments for purposes of migration management. As Ambassador Ely-Raphael indicated, you need to have the international framework and context within which to enforce changes of approach and policy to extremely complex and sensitive areas like trafficking and smuggling.

Smuggling is clearly something that involves a breach of immigration law. It is in a sense a breach against the State. Trafficking is a breach of human rights law, and is in effect a crime against the individual; and so they need different policy responses. Now that we have the Protocols, they provide the international framework for guidance to Governments to put in place the right legislation to deal with these two different facets of irregular migration.

However, there is no mechanism in place to enforce them. That is the first point about the Protocols. The second point about the Protocols is: how can a government sign or ratify conventions and protocols it has no capacity to enforce? And so what Ambassador Ely-Raphael was talking about with regard to the US Bill and the US Annual Report, which look at how governments are enforcing the principles and the intentions of the Protocols, is a very interesting phenomenon for us in the world of migration management – an effective way of filling the enforcement gap on international law, that has never really been tried before.

The Annual State Department Report on how governments are performing in terms of enforcing these protocols is an important report, because it gives governments not just guidance on what they could and should be doing under the Protocols, but also how governments more advanced in this area could help others build their capacities to be able to enforce the Protocols.

Let me be a little more specific, and focus on trafficking, which, as I said, involves a breach of human rights, yet from a migration perspective often sees the victims punished as law breakers or criminals. Another very important aspect of the Protocols is that they both criminalize the activity of trafficking and smuggling and protect the victims of trafficking. They also give guidance on how to build institutional capacity and work with other governments to address this as a global problem.

Let me turn to the Balkans. IOM works in all of the Balkan countries, and we have established a database of some 572 sample cases. In a world where between 700,000 and 2,000,000 people are estimated to have been trafficked, we know that 572 case studies are probably not a critical mass; but the database is growing, and the lessons we are learning now will also grow as more cases are added. IOM has established shelters and provides assistance to the victims; and gives technical support to the governments, undertakes training in schools, with the police, the judiciary, government officials and NGOs. We have conducted international campaigns as prevention measures throughout all of the Balkan countries and some Central East European and South-West European countries that have become countries of origin, transit and unfortunately also of destination.

In this presentation, I am looking at some 572 interviewed cases of trafficked victims in the countries of Albania, Serbia and Montenegro, including Kosovo, Former Yugoslav Republic of Macedonia and Bosnia and Herzegovina. It is interesting to see what is happening in the Balkans as a region where experiences, caseloads and movements are shared among the countries.

Our global map of trafficking flows shows how multi-directional the movements have become. Just about every country has become potentially a country of destination, even countries that traditionally have been origin countries. So, for example, people are being moved from Moldova, the Ukraine, Romania, Russian Federation, Tajikistan, the Dominican Republic, Nigeria, Cambodia, Bangladesh, Nepal, Vietnam to all kinds of other locations. We have assisted young women between the ages of 16 and 20 in Cambodia, who came from Romania and Moldova. Women are found in Thailand, who come from other parts of Asia, but also for example from Russia. Peruvians are moved to Korea; Cambodians, Vietnamese, Burmese and Chinese are being trafficked to Thailand. It has become a very global business.

The trafficking process can be understood as a continuum, so that we know where to address it, and how to advise governments on appropriate policies. I will come back to this continuum later in the presentation, but just to show that trafficking sets itself apart from smuggling in terms of the exploitation, the coercion, the pressures that women, children and men can experience at any point along the continuum between the country of origin or any country where people are recruited and the country of destination. The exploitation can be en route, and the case studies I am looking at today were mostly young women and children referred to and assisted by IOM in countries of transit, not in countries of destination - in other words they never actually reached their destination.

Who are the victims of trafficking in the Balkans? Looking at the age range, one notices that the majority of the victims are between the ages of 18 and 24. 79 cases out of 572 are children under the age of 18, which is typical, compared with other parts of the world. That will be different in some parts like Africa and the Mekong region in South East Asia where we know that the children are even younger. We have also noticed that from Central and Eastern Europe some of the girls are younger again, and we will watch this trend over the coming years.

What are the origins of the victims, i.e. the towns, villages or the capital cities they come from. It is interesting to see that the majority of them do not come from rural areas, or necessarily depressed areas, but from urban areas, not necessarily the capital city. One of the reasons for this is that the increasing number of information campaigns conducted by IOM and other agencies, particularly the United Nations agencies involved in combating

trafficking, have helped lower the numbers of women and girls from the capital cities, because that is where they are best informed and, we expect that with information comes awareness about traffickers. The majority of these victims come from towns, still in the urban areas. In Albania, more and more of them are coming from the rural sectors, where the deterrent information has still not reached everybody. We will watch this trend in the coming months and years as well, and target our information campaigns accordingly.

What is the marital status of the victims? Out of the 572 cases, 367 were single; 68 were divorced, 43 separated, and 8 are widows. So more than 88% of the cases were un-partnered persons. But another trend is also emerging, namely young women between the ages of 18 and 24, mostly single, mostly without children (64% are single, approximately 64% have no children).

What is the level of education of the victims? Not entirely uneducated, the majority of them have had some middle school or high school training, i.e., some pre-university education. There is even a fair percentage – 17 of them – who have gone to university. This is a trend we have also seen in the caseload from Central and Eastern Europe – Russians, Bulgarians, Poles, Czechs and so on.

To sum up very quickly, the cases are mostly young, educated, unemployed, and literate. This is largely the case in the Balkans, not necessarily replicated in Africa, where we have a very high percentage of children and persons from the rural sectors being trafficked. It is also not necessarily reflective of the situation in Southeast Asia. These persons have limited future prospects, and try their luck abroad, often with the aid of travel agents, who place advertisements in newspapers for jobs that do not exist, or for fake marriage opportunities in countries like Germany, Belgium, the Netherlands and so on.

In some extreme cases, the people are kidnapped. This is not a high percentage of those in our caseload. Sometimes, people are sold. In some parts of the world, it is quite common for girls and women to be sold for the survival of the family. The travel is arranged for them, and documentation provided; they are transported across the border, given lodging, put on sale, sometimes sold by one pimp to another pimp. There's very little protection available. In Germany, where it is estimated that up to 20,000 migrant women have been trafficked into the sex industry, they are quickly and frequently moved from one small town to another, so that the police cannot find them.

The exploitation of trafficked persons typically involves forced labor in the construction and agricultural industries for men, enforced prostitution for women and children in the sex industry, conscription in the military forces, domestic servitude, begging, etc. Large numbers of young children from countries like Bulgaria end up as beggars in the streets of Vienna. Delinquency, medical problems and such criminal activities as drug peddling are some of the related problems.

How were the victims recruited? The case studies show that most of them were recruited privately, i.e. by a friend, by a relative, by somebody they knew. This suggests that the criminal groups who are behind most of this trafficking are not directly contacting the victims, and are rather using friendly middle men and women close to the victims. Many of the recruiters are women. The majority of the victims in other words knew or know their recruiter.

What induces women, children and men to be trafficked? The majority (75%) of persons are induced to go to another country through the promise of a lucrative job. They want work, they are promised jobs as entertainers, as secretaries, as nurses, as domestics, as construction workers, and are even sometimes offered a marriage. From our statistics, marriage promises accounted for 1% only; so the job promise was the largest inducement. Of this caseload, really only 5% were forced into the decision, which suggests a high degree of victim gullibility.

What is the gender of the recruiter? 43% of the recruiters in this instance were female. The recruitment seems to be cleverly organized. As I said before, the Mafia and others behind this, are using recruiters who are known, who have the confidence of the victims, i.e. using relatives, and increasingly women.

What is the relationship of the recruiter to the victim? As already stated, most are acquaintances, friends, neighbors or family friends, boy friends, husbands, parents, relatives and so on. As I said, this is a trend that needs to be analyzed more carefully: who and what's behind the friend and the relative?

Did the victim accept to work in a specific country? Yes. 50% knew exactly where they wanted to go - and the country attracting the largest numbers of people as a destination is Italy. After Italy, come Bosnia and Herzegovina, Yugoslavia, Greece, Former Yugoslav Republic of Macedonia, Romania, Germany, Turkey, etc. When we look at where these women come from, we could question why they have selected countries like Bosnia and Herzegovina and Yugoslavia as destinations, rather than, say, Austria, Belgium, Germany and so on! Our analysis here is that the majority of these people, at least in this caseload, were not very professional in the way they organized it with the trafficker, and preferred to be as close to home as possible. This would require further analysis. Italy is the closest developed country for persons from Moldova, Romania, Ukraine, Albania and so on (these are the key countries of origin of this caseload). Why Bosnia and Herzegovina? It is in a reconstruction and rehabilitation phase, and has large amounts of international money flowing in, and like Kosovo, hosts a large international presence – which in turn attracts a market for illicit services.

What are we doing to address the problem? We try prevention activities in the countries of origin, including information campaigns in the schools, through television, radio, newspapers, and seminars, where we bring trafficked victims in to talk about their experiences. We have developed a long-running series on television in the Ukraine, Bulgaria, Moldova, and other typical source countries. We try capacity building and training of the authorities, the police forces, the judiciary, the teachers, the governments and NGOs to establish appropriate laws and operational practices to implement legislation. We have an excellent inter-agency referral system in countries like Albania and Bosnia and Herzegovina, involving where possible UNHCR, IOM, governments and NGOs, (in Bosnia and Herzegovina also the International Police Task Force) to identify cases and agree on which stream of migration management they belong to: are they asylum seekers and require protection? or do they need to go to one of the shelters that either IOM, an NGO or the Government runs? This is the kind of cooperation on migration management we would strongly recommend for all governments subjected to the trafficking problem.

We have set up shelters in both countries of origin and destination, to care for the victims both before and after they return from abroad. Women who have worked as prostitutes abroad often cannot easily return to their villages, their homes, their families; and

need to stay in a shelter for a few weeks, where they receive vocational training, psycho-social counselling and in some instances small scale micro-enterprise development assistance, to prepare them for reintegration into their home society. We also provide direct assistance with voluntary return and integration. We have a global programme supported by the US Government to assist women and children all over the world to come home again in a dignified and safe way.

IOM's assistance to victims also includes medical attention, which is very important, because as one of the NGO's we work with has observed, many women forced to work in the sex industry without access to medical assistance usually reach a point within four years where they are either very ill or die. We thus offer immediate medical assistance to women off the street, including psycho-social counselling and trauma therapy, regardless of their status in the host country. We are trying to set up centres in as many countries of transit and destination as possible.

To conclude, this small cross-section of cases in the Balkans is just a sample of the much larger problem world-wide; but it sheds some light on those aspects most urgently in need of longer term strategies to eradicate this criminal form of human rights abuse.

Trafficking, Smuggling and Refugees: the Contribution of UNHCR

GRAINNE O HARA
Legal Officer, Protection Policy and Legal Advice Section,
Department of International Protection, UNHCR

UNHCR's interest is motivated by our mandate for the protection of refugees. This presentation is intended to provide an update on UNHCR's perspective and engagement on the issues of trafficking and smuggling over the years. My comments will focus primarily on trafficking as the main topic of interest in this conference and should be understood throughout in the context of current international legal norms defining what constitutes the criminal offence of trafficking and smuggling. UNHCR uses the Palermo Protocols as its point of reference in this regard.

Criminal smuggling in migrants and trafficking in persons poses a growing problem to States and to other actors. Trafficking in human beings has been an increasing concern for UNHCR, especially over the last few years when it has come to the fore as a serious human rights concern. Our engagement in trafficking related issues can be roughly grouped under two main headings (*i*) standard setting; and (*ii*) operational.

Under the general heading of standard setting, I would like to say a few words about the emerging legal framework for combating smuggling and trafficking in human beings, that is, essentially the two Protocols against smuggling of migrants and trafficking in persons, which supplement the United Nations Convention against Transnational Organized Crime. UNHCR participated as an observer in the preparatory work of these instruments, with a view to ensuring that the texts of these treaties did not prejudice international refugee law obligations. Our aim was to reconcile anti-trafficking and anti-smuggling measures with the basic tenets of international protection. This will be a challenge for any new legislation and as the colleagues from the United Nations Office on Drugs and Crime(UNODC) move forward with their efforts to assist States with the implementation of the Protocols, UNHCR stands ready to support these activities by providing our input on the asylum related implications.

As a result of our participation in the drafting process, the Protocol against Trafficking contains a saving clause[1], intended to safeguard the rights of asylum-seekers and refugees under the 1951 Convention and the 1967 Protocol. It seems to us that the primary effect of this saving clause is to ensure access to some form of identification and screening process so that persons in need of international protection are able to submit applications for refugee status. The clause, along with the definitions contained in the Protocol, would also in effect exclude persons whose illegal entry is procured by traffickers from the penalties that the Protocol envisages against traffickers.

We continue to call for accession to the Palermo Protocols, which is also reflected in the current draft Agenda for Protection. We also continue to advocate the adoption of similar safeguards in bilateral or regional agreements or operational arrangements in this area, particularly when they are designed to implement or enhance the provisions of these Protocols.

[1] The Smuggling Protocol contains a similar clause.

This is why the issue was highlighted and incorporated in our process of Global Consultations on International Protection and found its reflection in the Declaration of States Parties at the Ministerial Meeting held on 12-13 December 2001 (the Declaration was adopted by consensus by 141 State parties participating in the Ministerial Meeting). Moreover, the resulting Agenda for Protection identified as one of its goals the protection of refugees within broader migration movements. The objectives of the Agenda for Protection include the strengthening of international efforts to combat trafficking and smuggling through the promotion of accession to the 2000 UN Convention Against Transnational Crime and its Protocols.

From a more operational perspective and with a view to understanding the asylum related concerns of the trafficking debate, UNHCR's interest is essentially two-fold:

- First, there is the fact that refugee women are particularly vulnerable targets for trafficking rings, particularly in camp situations. Refugee women are often without or become separated from family members during flight, and as a result become targets for sexual abuse generally and sexual exploitation in particular. A lack of access to legal integration possibilities in host communities has seen refugee women agreeing to take up low-paid jobs in the host community, later finding themselves in situations of forced prostitution and sexual slavery. It has also been seen that trafficking rings and their activities flourish in armed conflict and other situations of insecurity and chaos. In such situations, refugee women and girls are particularly susceptible to being targeted in a general situation of lawlessness. UNHCR has been involved in these issues in particular in Bosnia and Herzegovina, Kosovo and Albania.

- Second, some trafficked women may in fact be refugees under the 1951 Convention refugee definition, as a result of the trafficking experience and the inability or unwillingness of their country of origin to provide protection against such harm[1]. This may sound self-evident but in reality for many States it is a relatively new phenomenon for their refugee status determination procedures. The jurisprudence relating to the trafficking of women has had to confront some strong prejudices, born of the fact that trafficking issues have traditionally been analysed within the migration framework, with trafficked women and girls unable to overcome the bias towards seeing refugees as having been victims essentially of "political persecution". Certainly the asylum system cannot offer a panacea for all society ills. Nevertheless, ills having their root in a combination of severely depressed economies, ineffective border controls, disinterested or corrupt police and government officials and no legal safety nets. This leads to trade in women and children becoming lucrative, highly organised and heavily participatory. Then, the asylum system has to be able - is obliged - to

[1] Possible examples: aa)Where a woman suffers trafficking, for example, within the borders of her *country of origin* and the State has been unable or unwilling to protect her against such harm, and she later flees claiming refugee status, she could qualify as a refugee. Her trafficking experience in this case could amount to persecution. bb) Where a woman has been trafficked into a *neighbouring country*, one of the principal questions in a refugee claim would be whether she has a well-founded fear of persecution in her *country of origin.* The possibility of reprisals or retaliation from the trafficking rings or individuals, real possibilities of being re-trafficked, or even severe family or community ostracism, or discrimination, may amount to persecution in an individual case, coupled with an inability or unwillingness of the State to offer effective protection. The UK Immigration Appeal Tribunal in 2000 offered the same legal reasoning to find a woman trafficked from the Ukraine to Hungary as a refugee, finding that the claimant belongs to a particular social group of "women in the Ukraine who are forced into prostitution against their will".

accommodate individual situations they may generate. There are situations where there is no inclination or capacity in countries of origin to protect trafficked victims against reoccurrence of their plight or silencing of their testimony. This is due to corruption and complicity at the highest levels or throughout the law enforcement agencies, coupled with anyway inadequate legal systems (absence of laws, etc.) which are often accompanied by a vicious social stigmatisation of victims. In recognition of this fact, jurisprudence in a number of countries is starting to emerge in favour of recognising, in the individual case, trafficked victims as refugees. This trend should be positively recognised from the UNCHR perspective.

The linkages between trafficking and asylum has also been the subject of some debate in the context of UNHCR's Global Consultations process, particularly in relation to the asylum/migration nexus and gender-related persecution. We are committed to issuing guidelines on the application of the refugee definition to trafficked persons.

The valuable contribution of the UN Convention against Transnational Organized Crime and its supplementary Protocols to the fight against trafficking and smuggling as forms of transnational organised crime is beyond question and UNHCR is committed to the objective of universal ratification and implementation of these instruments. From our perspective, it is crucial that the protection aspects of the instruments are considered on a par with the crime control aspects in order to ensure that the Convention can effectively meet its overall objectives. We therefore reiterate UNHCR's willingness to continue our close collaboration with the UNODC in pursuit of common objectives.

8. The Network and Logistics of Trafficking: Emerging Threats and New Challenges

Links between Terrorist and Organized Crime Networks: Emerging Patterns and Trends

ALEX SCHMID[1]
Terrorism Prevention Branch
United Nations Office on Drugs and Crime

Six years ago, I published an article on *The Links between Transnational Organized Crime and Terrorist Crimes*[2]. At that time, these links were still a matter of dispute. Today, Security Council resolution 1373 openly acknowledges the existence of such links.

Table 1: Security Council Resolution # 1373 (28 Sept. 2001) on Links between International Terrorism and Transnational Organized Crime

"4. *Notes* with concern the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and in this regard *emphasizes* the need to enhance coordination of efforts on national, subregional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security".

In my article, I noted a number of differences between terrorist and organized crime groups, the most important being the political motivation behind much of contemporary terrorism.

Table 2: Differences between Terrorist and Organized Crime Groups

- Terrorist groups are usually ideologically or politically motivated while organized crime groups are profit-oriented;
- Terrorist groups often wish to compete with governments for legitimacy, organized crime groups do not;
- Terrorist groups usually relish in media attention; organized crime groups do not;
- Terrorist victimization is generally less discriminate than the violence used by organized crime groups;

Source: Alex P. Schmid. The Links between Transnational Organized Crime and Terrorist Crimes. *Transnational Organized Crime*, Vol. 2, No. 4, Winter 1996, pp. 40-82.

I also noted a number of similarities, including the role of intimidation, based on the threat of violence, characterizing both terrorist and organized crimes.

[1] The views and opinions expressed in this paper are solely those of the author and do not represent in any way official position of the United Nations Office on Drugs and Crime.
[2] Alex P. Schmid. The Links between Transnational Organized Crime and Terrorist Crimes. *Transnational Organized Crime,* Vol. 2, No. 4, Winter 1996, p.40-82.

Table 3: Similarities between Terrorist and Organized Crime Groups

- Both operate secretly and usually from underground;
- Both use 'muscle and ruthlessness' and produce mainly civilian victims;
- Intimidation is characteristic of both groups;
- Both use similar (though not entirely overlapping) tactics: kidnappings, assassination, extortion ("protection money", "revolutionary taxes");
- In both cases, the control of the group over the individual is strong;
- Both use front organizations such as legitimate businesses or charities.

Source: Alex P. Schmid. The Links between Transnational Organized Crime and Terrorist Crimes. *Transnational Organized Crime*, Vol. 2, No. 4, Winter 1996, pp. 40-82.

Such generalizations, as contained in the two tables above, inevitably downplay the diversity and heterogeneity of the groups involved. An unpublished study of the United Nations Office on Drugs and Crime on 40 organized crime groups in 16 countries found that "…the most striking outcome of the criminal group data collection exercise is the variety of groups on which information has been collected.[1]". The same is probably true for terrorist groups.

International Terrorism and Transnational Organized Crime: Alliance, Association, Connection, Cooperation, Confluence, Symbiosis or Convergence? Questioning the Nature of Links

Have the similarities increased and the differences decreased? Is there a convergence of terrorist and organized crime groups taking place, as some analysts' claim?[2] Or are there only ad hoc links between such organizations or networks?[3] It all depends on what one wishes to understand by terms like 'links' and 'convergence'.

[1] United Nations. Office on Drugs and Crime. Towards a Monitoring System for Transnational Organized Crime Trends: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, ODC, 2002 , p. 7.

[2] E.g. Carlos Resa and Flavio Mirella. Terrorism, Drugs Trafficking, Weapons and the Caribbean: not so far away… Unpubl. Paper, 2001;Tamara Makarenko. Transnational Crime and Its Evolving Links to Terrorism and Instability. *Jane's Intelligence Review*, 11/2001; Phil Williams and Ernesto Savona posed this possibility still as a question in 1995, stating: "If the means and ends of criminal and terrorist organizations are very different, however, they may be a growing, and perhaps irreversible, trend towards convergence". - Phil Williams and Ernesto U. Savona. Introduction: Problems and Dangers Posed by Organized Crime in the Various Regions of the World. *Transnational Organized Crime*, Vol. 1, No. 3, Autumn 1995, p.25.

[3] R.T. Naylor phrases the question in this way:" The central question then becomes whether crime and insurgency are really coalescing into a long-term strategic alliance (as distinct from the occasional tactical combination) within the ambit of a growing worldwide black market economy." – R.T. Naylor. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002, p. 45.

Table 4: 'Links' between international terrorism and transnationa organized crime: some lexical (near-) synonyms of 'links''(italics) and 'convergence'.

- ***Association:*** alliance, brotherhood, cartel, coalition, *partnership*, syndicate, *merger, union*.

- ***Alliance***: *affiliation*, *connection*, consortium, pact, *relationship*.

- ***Cooperation***: assistance, collaboration, coordination, help, *join*t action, mutual support.

- ***Symbiosis***: (usually mutually advantageous) *association* of two different organisms living attached to one another.

****

- ***Convergence***: approaching each other; move toward the same point or place; the formation of similarities in unrelated organisms living in the same environment.

Source: Oxford Dictionary & Thesaurus. Oxford, Oxford University Press, 1997.

It is hard to generalize and make statements covering hundreds of terrorist and organized crime groups or networks. Network is also an awfully broad and vague concept.[1] So are the concepts of association, alliance, symbiosis or convergence . Take, for instance, 'convergence'. It can mean at least three things:

1) ´approaching each other´. It can also mean;
2) ´move toward the same point or place´ (confluence). In biology, convergence means;
3) the formation of similarities in unrelated organisms living in the same environment.

If one takes the last meaning, one could, for instance, say that this common environment is the clandestine underworld in which both transnational organized crime and international terrorism have to act. If one takes that particular meaning, one could say that there is a certain degree of convergence in that some traditional organized criminal groups

[1] Phil Williams defines network as "….a series of nodes that are connected. The nodes can be individuals, organizations, firms, or computers, so long as they are connected in significant ways". - Phil Williams. Transnational Criminal Networks. In: John Arquilla and David F. Ronfeldt (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. St. Monica, Rand Corporation, 2001, p.66.

have discovered the advantages of cell-structured organizations over hierarchical ones.[2] Some of them have moved towards this classical terrorist model or organization.

There are three basic ways for protecting an underground organization from the eyes of the police and the security services (Table 5). In the first model, members have to make a pledge of secrecy. In the second model, the cell-structure of the organization itself ensures a degree of secrecy. In the third and most recent model, the protection of the movement is done by having no leaders at all in the underground.

Table 5: Three Models of Underground Organizations:

1. The conspiratorial secret (parallel) society with a hierarchical *pyramid organization*, commanding obedience and loyalty, sometimes mimicking a military hierarchy, sometimes based on ancient local traditions and organized as "families" or syndicates, each headed by a boss. The rank-and-file are subject to strong discipline and all members' risk of being killed if they violate "the law of secrecy". This is the classical model of a secret society.

2. The secretive *cellular-structured organization* wherein each cell consists of 3-5 persons[1]. All but one person in the cell do not know other members of the terrorist organization. The cell leader is the contact person with the cell above him. The organization is based on the principle of compartmentalization, which serves to control damage in case of penetration, desertion or arrest. There is usually a central commanding committee at the top, and each cell is specialized for a specific task. For an operation, cells with complimentary skills are organized into a "column"[2]. This is the classical model for terrorist organizations;

3. *'Leaderless resistance'* – an agglomeration of wholly autonomous units, often consisting of only one lone actor, whose information and ideological needs are satisfied by external channels (produced by a legal political movement advocating the same goals but not overtly advocating violent means for their realization, and mass media, including the internet). Immune to infiltration, the lone wolf terrorists are self-reliant and do not take orders but act on their individual initiative when and where they see it fit to advance a common cause.[3] This model was developed in the United States by right-wing patriots.

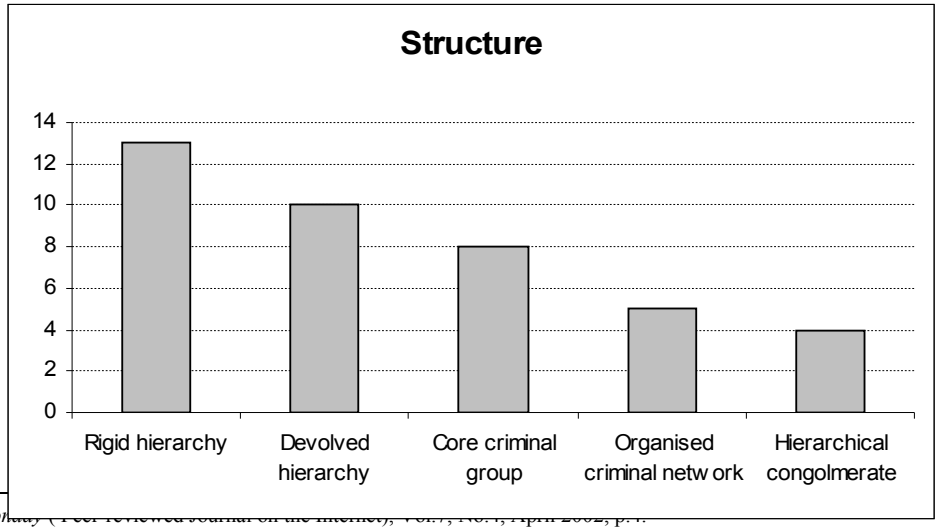
[2] For instance, a number of Mexican drug cartels, formerly organized as large pyramid structure under the control of a single person now consist of a series of cells which enjoy a certain degree of independence. – United Nations, Drugs and Crime Office. Toward a Monitoring System for Transnational Organized Crime Trends: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, ODC, 2002. The same study found that "…just under one third of the groups have a rigid hierarchical structure. A further ten have a devolved hierarchical structure. Four groups are conglomerates of a number of hierarchical groups. The remainder (again, about a third) are more loosely organized; either consisting of a core criminal group of individuals or a criminal network. Thus, the overall majority of groups (two thirds) have some form of hierarchy to their structure". The remainders (one third) are more loosely structured, ranging from small groups of core individuals around which criminal activities are organized, to a series of individuals operating in a more loosely structured criminal network". It should be noted that the sample of 40 groups studied was not representative. – Ibid., pp. 21-25.

[1] Ed Mickolus found in 1981 that the average acting terrorist cell has 4.4 members. – Edward F. Mickolus. Combating International Terrorism: A Quantitative Analysis. Ph.D. Diss. New Haven, Yale University, 1981; cit. Kent Layne Oots. A Political Organization Approach to Transnational Terrorism. Westport, Conn., Greenwood Press, 1986, p.39.

[2]Osama bin Laden remarked, in a videotape released by the US State Department, with regard to the 9/11 attackers: "Those who were trained to fly didn't know the others. One group of people did not know the other group". – Valdis E. Krebs. Uncloaking Terrorist

In the real world, specific organizations rarely correspond to such ideal-type models.[2] Many terrorist organizations, which are usually seen as belonging to the second type, are still showing features of the first organizational type.[3] Organized crime, on the other hand, is said to be moving away from hierarchical forms of organization to criminal networks. However, a recent pilot study of the Office on Drugs and Crime found that only about ten per cent of the groups in a sample of forty groups showed network characteristics. If this is the wave of the future, and if this sample is representative, organized crime has still some way to go to catch up with the trend.

Table 6: Structure of 40 organized criminal groups in ODC pilot study sample.[4]



Networks. *First monday* (Peer-reviewed journal on the internet), Vol.7, No.4, April 2002, p.4.

[3]Louis R. Beam.' Leaderless Resistance'. *The Seditionist,* 12 (February 1992); cit. J. Kaplan. 'Leaderless Resistance'. , in: David C. Rapoport (Ed.). Inside Terrorist Organizations. London, Frank Cass, 2001, p.267.

[2] Some observers used the familiar business corporation model to describe Al Qaeda. CNN, for instance reported on 5 October 2001:"Analysts say al Qaeda needs to be viewed as a corporation, with bin Laden as the chairman of the board" Bin Laden is a totally multinational enterprise", said terrorism analyst Magnus Ransdorp." He has tentacles and followers all around the world". Like many global companies Al Qaeda is a combination of partnerships, experts say. It has strategic alliances with other groups, as well as some wholly owned subsidiaries. (…)A new business partner for bin Laden appears to be the GIA, Algeria's Armed Islamic Group. (…)The problem of countering the bin Laden organization is that it mutates continuously", "Ransdorp said. It is not only a multinational enterprise with followers with financial infrastructure across the globe, it mutates, continuously shifting in order to insulate the organization from … attempts at removing top leadership". – Al Qaeda has complex terrorist networks, analysts say. *CNN*, Atlanta, 5 October 2001, 18:05 GMT (<http://www.cnn.com/2001/US/10/02/inv.binladen.friends/>

[3] James Fraser, a counterterrorism specialist, describes a terrorist group as organized something like a pyramid. "At the very top are a few leaders who make the overall policy and plans. Below them is a somewhat larger group of terrorists who actually carry out attacks. This is called the *active cadre.* Members of the active cadre often specialize in particular activities, such as intelligence or surveillance, bomb-making, or communications. The next lower and broader level of the pyramid is composed of the "active supporters". These people are crucial for the sustained operation of the terrorist campaign, because they provide intelligence and warning, weapons and supplies, communications, transportation, and safe houses. Finally, there is a diffuse group of "passive supporters" who agree with the goals of the terrorists, help spread their ideas, and provide money and other support". Cit. Harry Henderson. Global Terrorism. The Complete Reference Guide. New York, Checkmark Books, 2001, p. 17.

[4] *1. Rigid hierarchy:* Single boss. Organization or division into several cells reporting to the centre.
Strong internal systems of discipline.
2.*Devolved hierarchy*: Hierarchical structure and line of command. However regional structures, with their own leadership hierarchy, have a degree of autonomy over day to day functioning.
3. *Hierarchical conglomerate*: An association of organized crime groups with a single governing body. The latter can range from an organized umbrella type to more flexible and loose oversight arrangements.
4. *Core criminal group:* Ranging from relatively loose to cohesive group of core individuals who generally regard themselves as working for the same organization. Horizontal rather than vertical structure.
5. Organized criminal network. Defined by the activities of key individuals who engage in illicit activity together in often shifting alliances. They do not necessarily regard themselves as an organized criminal entity. Individuals are active in the network through the skills and capital that they may bring.

Source: Crime Trends: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, ODC, 2002, p.20.

Al Qaeda

How would you, for instance, place Al Qaeda in an organizational model? Bin Laden's organization has been described by some as an "umbrella organization"[1]. Others see Al Qaeda and Bin Laden as part of a Global Jihad Network in which Al Qaeda is but one component. They hold that a number of autonomous groups are united together by a shared common ideology of global Jihad to destroy the secular democratic world, and impose Islamic Caliphates.[2] Al Qaeda is a nebulous, apparently sophisticated, decentralized transnational network – or perhaps even "network of networks" – which includes militants, sleepers, front organizations, legitimate business enterprises and nongovernmental organizations, operating in more than 60 countries.[3] The influence of the charismatic leader, Osama Bin Laden, might be even more far-reaching than the actual financial support he provides to far-away sleepers.[4] A number of cells of this Islamist network are apparently able to finance themselves through criminal activities such as kidnapping, trafficking in narcotics and petty crime. Some attacks – such as the killing of Americans in the Middle East and South Asia – are apparently perpetrated by Al Qaeda sympathizers with no known connection to the network beyond what they learn about Al-Qaeda from the media. Their activities resemble in some ways those of the "leaderless resistance" paradigm which Valery Tishkov from the Russian Academy of Sciences sees as a possible paradigm for the future. He postulates that

> "To avoid capture, terrorists will increasingly adopt new organizational models and move toward a form of organization called 'leaderless resistance'. The premise is that if there are no chain-of-command and no communications between headquarters and operatives in the field, the risk of penetration and discovery is minimized – assuming basic principles of tradecraft are practiced. The idea is that small, totally independent cells of individuals will strike when they find a lucrative target and believe the moment propitious".[5]

[1] Rohan Gunaratna, in interview with *Der Spiegel* (Hamburg), No. 48, 2002, p. 155. See also: Rohan Gunaratna. Inside Al Qaeda. Global Network of Terror. London, Hurst & Company, 2002. – Al Qaeda operates under various aliases: The World Islamic Front for Jihad Against Jews and Crusaders, the Islamic Army for the Liberation of the Holy Places, the Islamic Salvation Foundation, and the Group for the Preservation of the Holy Sites. Al Qaeda encompasses members and factions of national Islamic militants such as Egypt´s Islamic Group and Al-Jihad, Algeria´s Armed Islamic Group (GIA), Pakistan´s Harakut ul-Mujahidin, the Islamic Movement of Uzbekistan and opposition groups in Saudi Arabia. It has links to the Abu Sayyaf Group in the Philippines and to Islamic militants in Indonesia. - Kenneth Katzman (Foreign Affairs, Defense, and Trade Division). Terrorism: Near Eastern Groups and State Sponsors, 2001. In: John Prados (Ed). America Confronts Terrorism. Chicago, Ivan R. Dee, 2002, pp.191-193.

[2] M.J. Gohel, Asia Pacific Foundation, summarizing findings of a conference on 'Militant Islam in Asia – The Challenges', London, RUSI, 21-22 November 2002 (private communication).

[3] Executive Summary. Countering the Changing Threat of International Terrorism. Report of the National Commission on Terrorism, June 7, 2000. Repr. In: John Prados (Ed.). America Confronts Terrorism. Understanding the Danger and How to Think About It. Chicago, Ivan R. Dee Publ., 2002, p. 44. – Phil Williams discussing criminal networks made an observation which is also worth keeping in mind when talking about terrorist networks:" One of the most significant points about [criminal] networks is that they are not immediately and obviously visible. Criminal networks can hide behind various licit activities, can operate with a lower degree of formality than other types of organization, and can maintain a profile that does not bring them to the attention of law enforcement". – Phil Williams. Transnational Criminal Networks. In: John Arquilla and David F. Ronfeldt (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. St. Monica, Rand Corporation, 2001, p.71

[4] R. T. Naylor, goes even further when he writes:" In reality, El Qai´da seems less an organization than a loose association of independent cell-like entities that changes form and personnel ad hoc in response to threats and opportunities. Just as the Mafia is less a formal institution than a type of behavior, so too El-Qaída seems less an entity than a shared state of mind, less a political organization than a cult of personality that the United States seems committed to strengthening". – R.T. Taylor, op. cit., p. 290.

[5] Valery Tishkov. Roots of Terror. Unpubl. MS, Nov. 2002. – Jeffrey Kaplan defined ' leaderless resistance' as " a kind of lone wolf operation in which an individual, or a very small highly cohesive group, engage in acts of anti-state violence independent of any movement, leader or network of support. This violence may take the form of attacks on state institutions or operatives, or it may take the

Advances in communication technology – especially the ubiquity of the World Wide Web on the Internet and the possibility to encrypt messages - might in fact make the leaderless-resistance model more feasible, providing remote guidance and instruction to self-appointed militants.

Lately, public domain encryption has become so powerful, that the reading of communications of terrorists and other lawbreakers has become increasingly difficult. It has been suggested that Al Qaeda not only used encrypted e-mail but also hides encrypted message texts within picture files (steganography) or other data that could be downloaded from a Website. Advances in secure communication have turned the Internet into a powerful tool for the transfer of encrypted messages.[1] This not only helps terrorists but also organized criminal groups, allowing them, with the help of stolen and reprogrammed cell phones and encryption, to network with each other – both horizontally with other cell members and vertically with their leaders – in ways which are hard if not impossible to trace. [2]

The global access to information, which the Internet provides and transmits, allows the preparation of dispersed but simultaneous activities with a growing degree of secrecy. This advance in communication technology is one of four major features that have allowed a 'quantum leap' forward for transnational crime and international terrorism, creating a lead which national law enforcement in most countries still has to catch up with.

Table 7: Globalization Features Facilitating Transnational Organized Crime and International Terrorism

1. Border Porosity (incl. opening of Iron Curtain)
2. Population Transfer (diasporas)
3. Financial and commercial developments (e.g. electronic banking, trade liberalization)
4. Communication technology (internet, encryption)

Source: Tamara Makarenko. Transnational Crime and its Evolving Links to Terrorism and Instability. *Jane's Intelligence Review*, 11/2001.

Let me come back to the question I raised earlier: "Are the trajectories of international terrorism and organized crime converging?"

If one takes the second meaning of 'convergence'– confluence or moving toward the same point or place' where they overlap, there are indeed examples for this. In July 2002 the US Attorney-General, John Ashcroft said that he had asked federal law enforcement agencies to draw up a single list of the major trafficking groups responsible for the U.S. drug supply. He then found that:

form of random targets of opportunity selected on the basis of their perceived vulnerability and their symbolic importance". J. Kaplan. 'Leaderless Resistance'. In: David C. Rapoport (Ed.). Inside Terrorist Organizations. London, Frank Cass, 2001, p.260.

[1] Stephen Budiansky. Losing the Code War. *http://theatlantic.com/issues/2002/02/budiansky.html* Budiansky noted that "it is now virtually impossible to break the encrypted communication systems that PCs and the Internet have made available to everyone – including, apparently, al Qaeda".

[2] Michele Zanini and Sean J.A. Edwards. The Networking of Terror in the Information Age. In: John Arquilla and David Ronfeldt, op. cit., p. 38.

"Nearly one third of the organizations of the State Department's list of Foreign Terrorist Organizations (33 at that time, AS) appear also on our list of targeted U.S. drug suppliers".[1]

How representative this sample of the US government is, I do not know. There are many hundreds of terrorist groups and thousands of organized crime groups active in the world and their trajectories have never been studied in combination. But this type of convergence, which is also sometimes labeled *narco-terrorism*.[2]is certainly disquieting.

Depending on the level of analysis, and on the semantic load of the term convergence, convergence is more or less total: On the most general level it is of course true that terrorist groups commit crimes and many of their serious crimes actually fall under the terms of the United Nations Convention against Transnational Organized Crime. To that extent there is already a very large degree of convergence. Much, but not all terrorism, depends on crime as a means for generating income for political violence.[3] Terrorist organizations have also, for more than one hundred years, been trying to engage criminals because of their skills, their propensity to take risks and their disregard for the norms of society.[4]

Yet one also sees that criminal organizations which use extortion, corruption and intimidation as their main tools, also resort occasionally to the use of terror, which is an enhanced form of intimidation. Phil Williams and Ernesto Savona noted that Colombian drug cartels and the Italian Mafia were both using terrorist attacks against the state and its representatives for five different reasons (Table 8).

Table 8: Uses of Terror Tactics by Organized Crime Groups

i) disrupt investigations;
ii) deter the introduction or continuation of vigorous government policies;
iii) to eliminate effective law enforcement officials,
iv) to coerce judges into more lenient sentencing policies, and
v) to create an environment more conductive to criminal activity.

Source: Phil Williams and Ernesto U. Savona. Introduction: Problems and Dangers Posed by Organized Crime in the Various Regions of the World. *Transnational Organized Crime*, Vol. 1, No. 3, Autumn 1995, p.25.

[1]U.S. Says Many Drug Traffickers on Terrorist List. Reuters, 30 July 2002 10:20Ashcroft added: Law enforcement has been aware for some time of significant linkages between terrorism and drug trafficking. But we have not had the tools to quantify the drug-terrorism nexus until now". Michael Chertoff, Assistant Attorney General for the Criminal Division of the U.S. Department of Justice added: "Drugs not only directly (threaten) the fabric of our society but they provide funding and support for terrorist organizations that take up arms and commit acts of violence. Drug traffickers have a symbiotic relationship with terrorists". – Such views were more recently echoed by the British Home Secretary, David Blunkett: "The funding generated by networks perpetrating organised crime are the same funds and same networks that have a direct relevance to the development of sales and support for terrorism. Therefore, there is a shared and common interest in tackling organised crime and terrorism". – Balkan Gangs More Organized than Police, says Blunkett. *PA News*, 25 November 2002 13:45.

[2] The US Drug Enforcement Agency defines narco-terrorism as a subset of terrorism, in which terrorist groups, or associated individuals, participate directly or indirectly in the cultivation, manufacture, transportation, or distribution of controlled substances and the monies derived from these activities. Further, DEA uses the term to characterize the participation of groups or associated individuals in taxing, providing security, or otherwise aiding ort abetting drug trafficking endeavours in an effort to further, or fund, terrorist activities. – U.S. Department of State. The Nexus Between Drug Trafficking and Terrorism. Fact Sheet. Washington, D.C., Bureau for International Narcotics and Law Enforcement Affairs, 10 April 2002.

[3] Statement by Hon. Batty Weerakoon, Minister of Justice, Sir Lanka, 13 Dec. 2000 on the occasion of the high-level political signing conference for the United Nations Convention Against Transnational Organized Crime, Palermo, Italy.

[4] Isaac Cronin, in introduction to I. Cronin (Ed.) Confronting Fear. A History of Terrorism. New York, Thunder's Mouth Press, 2002, p.xii.

Another example of organized criminal groups using terrorist methods occurred in Dagestan when in November 1996 a bomb attack on border guards killed 50 people. The attack was a reprisal for state intervention in their criminal caviar smuggling business.[1]

While there is overlap in the sources of income as well as in some of their tactics between terrorist groups and organized criminal groups, this does not necessarily mean amalgamation or fusion. Their relationship is in many cases only a pragmatic alliance of sorts where each side keeps its own identity - a more political one in the case of terrorists and a more predatory one in the case of organized crime, at least in the early stages of development.[2]

Organized crime has a number of bedfellows of which terrorist groups are but one. Their pragmatic alliances include domestic and foreign partners[3]. The following table provides a non-exhaustive list of some "marriage of convenience" that have been empirically observed:

Table 9: Types of Links of Organized Crime with Non-Terrorist Entities

1. One organized criminal group with another national organized criminal group, at home or abroad, to expand respective geographic areas of operations or dividing territory (e.g. Sicilian Mafia – Colombian drug cartel)[4];
2. One national organized criminal group with governing political party (e.g. in 1950s S. Vietnamese government and Bin Xuyen river pirates)[5];
3. One national organized crime group with a legal business group (allegedly Mafia with parts of the legal tobacco industry);
4. One national organized criminal group with an ethnic immigrant group in host country (e.g. Italian organized crime and Albanian groups in Italy);
5. 'Rogue state' engaging in drug trafficking and other organized crime activities (Yugoslavia under Milosevic) [6]

What is known about the frequency of such links? Louise Shelley, one of the foremost experts on transnational organized crime, holds that "The links between organized criminals and terrorists are much less frequent than the links between organized criminals

[1] James Morton. Gangland International. The Mafia and Other Mobs in the Twentieth Century. London, Warner Books ,1999, pp.848-849.
[2] See Appendix I: Stages of Organized Crime, by Peter Luphsa.
[3] For instance, there was a summit meeting in Beaune, France in 1994 attended by organized crime bosses from China, Russia, Colombia, Japan, Italy and the United States. This was followed by two further meetings on yachts in the Mediterranean .– Andrew Alderson and Carey Scott. 'Crime Kings meet to carve up Europe'. *The Sunday Times*, 29 March 1998; cit. James Morton. Gangland International. The Mafia and Other Mobs in the Twentieth Century. London, Warner Books, 1999,.856.
[4] Europol. Threat Assessment. Europol First Situation Report. The Hague, Europol, 1999, pp. 14-15.
[5] R.T. Naylor noted:" Mature criminality [in the symbiotic stage – see appendix I, AS] is compatible with the continued existence of the formal state and can even be employed to defend it; mature insurgency threatens the overthrow of that formal state and, by definition, cannot comfortably coexist with it. This distinction was neatly summed up in South Vietnam in the 1950s when the government ceded control of the Saigon-Cholon vice rackets to the Binh Xuyen gang of river pirates in exchange for their keeping the city free of Communist guerrilla activity". – R.T. Naylor. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002, p.55.
[6]The Serbian Interior Minister Dusan Mihajlovic in a TV program entitled "It is not Serbian to keep quiet"(BKTV, 11 Nov. 2002), commenting on arrests carried out in connection with the murder of former Belgrade police chief Bosko Buha, said:" The criminal heritage which I talk about can only be represented as a criminal pyramid at the top of which used to stand the highest tier of state and political officials that used to lead this country – then the chiefs [changes thought], individuals, not the institutions but individuals in the customs administration, state security service, this or that state institution – then those bosses who used to organize this business all the way down to the very bottom of the pyramid where we used to have drug dealers and hard currency dealers, murderers and racketeers in the street, all of which we are facing now. I repeat: this pyramid has two faces. One face is war crimes committed in our name and the other is organized crime". (BKTV, Belgrade, in Serbian 10:55, 11 Nov. 2002 BBC Monitoring European – Political, London.

and politicians".[1] This might be an 'educated guess' but is not based on hard data. Unfortunately, 'hard data' in this area are almost non-existent. They come only in small parcels.

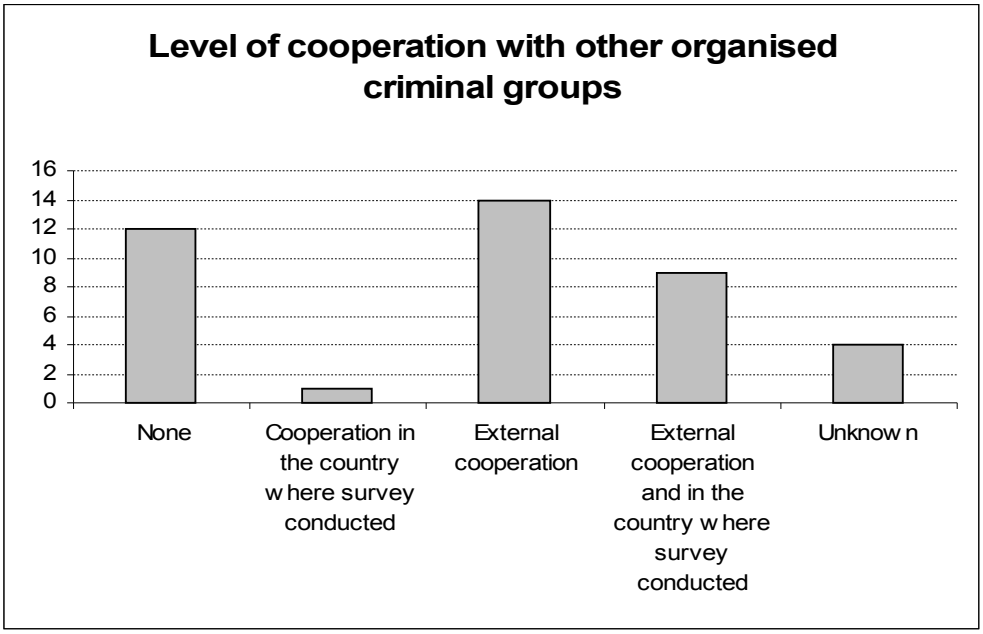


Table 10: Level of cooperation with other organized criminal groups

How frequent is cooperation between organized criminal groups at home and abroad? We have the findings of an UNODC pilot study surveying 40 groups in 16 countries. It was found that in 35 per cent of the cases there was some level of cooperation with transnational organized crime groups outside of the country where the survey of the criminal group itself was conducted. In 22 percent of all cases both external and internal cooperation was recorded.[2] Since the majority of organized crime groups are engaged in the smuggling of drugs which requires foreign partners, transnational cooperation is a necessary requirement. However, the data of the pilot study also indicate that in a rather high number of cases – 30 percent – there was no evidence of cooperation with other criminal groups. And, as mentioned before, only ten percent of the groups took the form of ´criminal

[1]Louise Shelley (Professor and Director, Center for Transnational Crime and Corruption, American University. Identifying, Counting and Categorizing Transnational Criminal Organizations. Unpubl. Paper, n. d., p.9.

[2] In 10 percent of the cases (four cases) it was not possible to establish a reliable response. – UNODC. Crime Trends: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, UNODC, 2002 , p.30.

networks´. [3] The reason for this might be security considerations. Trust is indeed a rare commodity in the underworld of crime.

Let us now look at some types of links of terrorist groups with others groups.

Table 11: 'Links' and 'Cross-overs' between Terrorist Groups - Organized Criminal Groups

1. One national organized criminal group with a national terrorist group (e.g. Colombian drug cartels and FARC);
2. One organized criminal group with foreign terrorist group abroad (Colombian drug traffickers with Sendero Luminoso in Peru)[1];
3. Foreign organized criminal group in host country linking up with local terrorist group; (e.g. Triades with protestant paramilitaries in Northern Ireland)[2];
4. Foreign terrorist sleepers engaging in organized crime in host country (e.g. GIA in France);
5. Foreign terrorist group training local guerrilla/terrorist group (e.g. Provisional IRA – FARC in Colombia).
6. Organized criminal group evolving into terrorist group – "felons turning fighters" (Zeljko Raznjatovic's group become Arkan Tigers in Yugoslavia)[3]
7. Declining/defeated terrorist group degenerating into pure organized criminality - "fighters turning felons", "guns to gold" (Abu Sayyaf in the Philippines).

So far, I have tried to show some empirically observed 'links' between terrorist groups, organized criminal groups and some of their allies. Let me now turn to the issue of motives for such forms of cooperation.

Incentives and Disincentives for Cooperation between Terrorist and Organized Criminal Groups

Why should terrorist groups and organized criminal groups seek each other's company? For the terrorist groups one answer is money. Since the end of the Cold War state

[3] The UNODC pilot study defined 'criminal networks' by the activities of key individuals who engage in illicit activity in often shifting alliances. Such individuals may not regard themselves as being members of a criminal group, and may not be regarded as being a criminal group by outsiders. Nevertheless the coalesce around a series of criminal projects.(…)Networks usually consist of relatively manageable numbers of individuals, although in many cases different components of the network may not work closely with (or even know each other) but be connected through another individual or individuals. Personal loyalties and ties are essential to the maintenance of the network and are key determinants of relationships. It should be noted however that various individuals within the network do not carry the same weight and the network is generally formed around a key series of individuals (or nodal points) through which most of the network connections run. Of the 40 groups on which data base been collected, only four of these constitute criminal networks. It should be conceded that while these constitute only a small component of this survey, it is likely that criminal networks are more common, and indeed are a growing phenomenon". – ODC. Towards a Monitoring System for Transnational Organized Crime Trends: Results of a Pilot Study of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, ADC, 2002, p.44.

[1] Phil Williams and Ernesto U. Savona. Introduction: Problems and Dangers Posed by Organized Crime in the Various Regions of the World. *Transnational Organized Crime*, Vol. 1, No. 3, Autumn 1995, p.25.

[2] An example would be the unholy alliance between a Chinese Triad gang in Northern Ireland and the protestant loyalist Ulster Volunteer Force. The leader of a 'Snakehead' gang, a wealthy businessman who owns a Chinese restaurant in Belfast, used five masked paramilitaries UVF men as his enforcers to force Chinese illegal immigrants to pay up money they owed for the transport. He had, in turn, smuggled arms for the UVF into the country. – John Cassidy. Republic of Ireland: UVF Link to Triad Gang. RUC probe attack on Chinese immigrants. *Sunday Mirror*, 2 July 2000, p. 39.

[3] F. Bovenkerk. Misdaadprofielen. Amsterdam, Meulenhoff, 2001, p. 82

–sponsorship has declined and new sources of funding had to be sought.[1] As Frank Cilluffo, an American expert on terrorism, put it simply: "Involvement in the drug business is almost a guarantee of financial independence from a state sponsor".[2] It is but one of a number of factors that make organized crime an interesting partner for terrorist groups.

Table 12: Factors encouraging 'links' from the point of view of terrorist organizations

- access to greater financial resources for terrorist attacks;
- independence from state sponsorship;
- possibility of building up economic power, compensating for lack of public support;
- access to specialist skills (e.g. forging travel documents);
- facilitation in cross-border movements (use of smuggling routes)[3]
- substitute activity during armistices or at end of hostilities;
- coming into contact with a wider range of potential recruits, who are already outlaws.
- access to expertise in illicit transfer and laundering of money for foreign operations.

However, there are also factors standing in the way of closer cooperation.

Table 13: Factors discouraging association/cooperation/links/cross-over from the point of view of terrorist organizations

- Danger of infiltration, treason;
- Danger of losing political credibility.

[1] However, while states might no longer support terrorist groups in order to use them as proxies, apparently some states paid terrorist groups 'protection money', to be free from attacks themselves. The line between voluntary support and extortion is often not clear for outside observers. – A US Senate Subcommittee Report entitled "The BCCI Affair" found that "terrorist organizations …received payment at BCCI-London and other branches directly from Gulf-state patrons, and then transferred those fund wherever they wished without apparent scrutiny". "http://www.ist.socrates.berkeley.edu/~pdscott/q4.html"

[2] Frank Cilluffo. The Threat Posed from the Convergence of Organized Crime, Drug Trafficking, and Terrorism. (Deputy Director, Global Organized Crime Program Director, Counterterrorism Task Force, Center for Strategic and International Studies, Washington D.C), before the U.S. House Committee on the Judiciary, Subcommittee on Crime, 13 December 2002.

[3] R.T. Naylor provides the following example: "in the border areas between Albania, Kosovo, and Serbia, the Kosovo Liberation Army (UCK) presides over a smugglers´ nest. It collects taxes in cash and in service – the smugglers assist by moving weapons. And individual members run their own rackets, trafficking in refugees, prostitutes bound for European brothels, drugs, and cigarettes". - R.T. Naylor. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002, p. 66.

Transnational organized criminal groups also differ in structure, membership and modus operandi. There might be a clash of cultures, a breach of security procedures that can jeopardize the survival of a group. One has to realize that cooperation is inherently risky because one side does not know whether the other side has been penetrated and whether therefore, cooperation will endanger one's own organization.

For that reason, cooperation between two or more terrorist groups is more the exception than the rule as the following table makes clear. One has, however, to distinguish between different forms of cooperation – logistical cooperation, financial cooperation and operational cooperation. It is the latter that is most rare and the observation from Martha Crenshaw from 1975 still holds, though probably less so than a quarter of a century ago:

> " Limited operational collaboration among terrorist organizations has taken place, but transnational relations among them are generally not active, formal, institutionalized or overt".[1]

Logistical cooperation – whether in the form of finances, training or supply of arms – however, is less risky and more frequent. It is but one of several forms of possible cooperation.

Table 14:Types of Cooperation among Terrorist Organizations

1. Financial support (e.g. sharing of ransom money);
2. Training (e.g. use of training camps, transfer of know-how on bomb-making);
3. Weapons;
3. Organizational (e.g. forged documents, communication and propaganda support)
4. Operational (proxy attacks, coordinated attacks and joint operations).

Source: Y. Alexander and Robert A. Kilmark International Network of Terrorist Movements. In: Y. Alexander and R.A. Kilmark (Eds.). Political Terrorism and Business: The Threat and Response. New York, Praeger, 1979, pp. 40-51; cit. K.L. Oots. A Political Organization Approach to Transnational Terrorism. Westport, Conn., Greenwood Press, 1986, p. 43.

How difficult cooperation is, has been empirically tested on the basis of a large dataset. Based on the ITERATE (International Terrorism: Attributes of Terrorist Events) dataset on international terrorism, Kent L. Oots tested a number of hypotheses and came to the following findings:

Table 15: Findings with regard to Terrorist Coalition Characteristics, 1968 – 1977

1. Participants are more likely to be wounded during coalitional acts than during single group acts;
2. The average numbers of deaths and injuries are higher for coalitions than for single groups;
3. Coalitions are more likely to engage in difficult acts of terrorism than are single groups;

[1] Martha Crenshaw Hutchinson. Transnational Terrorism and World Politics. *The Jerusalem Journal of International Relations*, Vol. 1, No.2, Winter 1975, p.111; cit. K. L. Oots, op. cit., p. 41. - Walter Reich. Understanding Terrorist Behavior. In: Isaac Cronin (Ed.) Confronting Fear. A History of Terrorism. New York, Thunder´s Mouth Press, 2002, p. 530.

4. Coalitions are relatively rare and account for only 5.6 percent of all terrorist acts;
5. Coalitions usually do not last very long. Nearly three-fourth of all coalitions disband after only one act.

Source K. L. Oots. A Political Organization Approach to Transnational; Terrorism. Westport, Conn., Greenwood Press, 1986, p. 106.

It must be added that these data are not recent. However, if cooperation has increased, it has increased from a very low level of only 5.6 percent among terrorist groups. If cooperation between like-minded terrorist groups is already difficult, how more difficult is cooperation between terrorist and organized criminal groups? Naylor has argued, and it is an argument that applies especially to the traditional anti-capitalist leftist groups, that:

> "…. whatever short-term alliances of convenience may occasionally emerge between well-entrenched criminals and anti-regime guerrillas, in the long run the two groups usually end up on opposite sides of the barricades, and inevitably so if the guerrilla groups' ideology is anticapitalist. For the guerrilla group, the underground economy and the treasures it yields are tools that will enable the group to carry out a political agenda; for the criminal organization, the riches of the black market are an end in themselves".[1]

However, this argument is less convincing for non-leftist groups or when there is some strong quid pro quo exchange opportunity that makes cooperation worthwhile for both sides.[2] Let us look at how the picture emerges from the less ideological and more pragmatic organized crime side:

Table 16: Factors Encouraging 'links'/cross-over/cooperation from the point of view of organized crime group

- Drug traffickers benefit from terrorists' military skills and obtain protection for illicit drug cultivation or trafficking in areas under guerrilla/terrorist control.
- Terrorist destabilization of political and economic structures may create favourable environment for organized crime activities.
- Law enforcement preoccupation with countering terrorism may divert attention from organized crime activities.
- Political-terrorist label provides extra degree of 'intimidation'.[3]

[1] R.T. Naylor. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002, p. 56.

[2] E.D. Mickolus, Combating International Terrorism: A Quantitative Analysis. New Haven, Yale University, PhD Thesis 1981, p.5.69-5.70; cit. K.L. Oots, op. cit., p. 49. - A reason why coalitions are the exception rather than the rule lies in the heterogeneity of terrorist groups. In this regard, Walter Reich notes:" Certainly, a number of themes and characteristics are shared by many of the terrorist groups and movements mentioned in this short history; the goals of achieving terror and publicity for the cause are shared by nearly all of them. But one searches with difficulty, and probably in vain, for psychological qualities that are shared by all or nearly all of the terrorists and terrorist groups mentioned here.(…) Moreover, the terrorist groups themselves shift in character. Some terrorist groups that were once on the right have ended up on the left, and vice versa; and most are, in fact, mixtures of types, such as leftist nationalists, rightist nationalists, religious nationalists, and so on. In terrorism, there are many mixed and borderline conditions. The lesson that the psychological researcher must draw from the long history of the terrorist enterprise, and especially from its variety and complexity, applies not only to the study of individual terrorists but also to the study of the terrorist groups themselves. Like individual terrorists, the groups to which they belong, and ultimately the communities from which those groups arise, are not necessarily alike in their psychological characteristics, even if they share certain goals or orientations". - Walter Reich. Understanding Terrorist Behaviour. In: Isaac Cronin (Ed.) Confronting Fear. A History of Terrorism. New York, Thunder´s Mouth Press, 2002, pp. 523-524.

[3] Naylor reports that Argentinean criminal kidnappers used to claim to be guerrillas because guerrilla groups, with better infrastructure, could hold victims longer and therefore could command a higher ransom. He also noted the use of the ´terrorist image in the case of criminals in Northern Ireland and the Philippines. - R.T. Naylor. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002´, p. 56.

Yet again, there are also a few, but decisive, arguments which speak against close links:

Table 17: Factors discouraging association/cooperation/links/cross-over from the point of view of organized crime group

- Terrorist group may extort drug-trafficking organizations;
- Terrorist group might take over 'business' from organized crime group.

Examples of this danger can be found in Colombia where the Revolutionary Armed forces of Colombia (FARC), 'stole' a good deal of business from organized crime.

How strong these pro- and contra- arguments weight in the minds of terrorist leaders and bosses of organized crime is hard to say. However, most of them are rational actors capable of cost-benefit analysis.

Conclusion

Let me summarize briefly what we found:

- To begin with, there is ample evidence that organized criminal groups cooperate with each other[1].
- Second, there is also, especially since the emergence of Al Qaeda, considerable evidence of cooperation between like-minded terrorist groups.
- Third, there is also some evidence of some terrorist groups making money from organized crime activities and
- Forth, there is evidence that some organized criminal groups also use tactics of terror.
- Finally, there is also evidence of a degree of cooperation between some organized criminal groups and some terrorist groups.

With regard to the last point, Marc Galeotti, Director of the Organised Russian and Eurasian Crime Research Unit at Keele University, recently said "Until now, fears of international alliances between terrorists and criminals have proved to be exaggerated".[2]

Perhaps he is right. The disquieting thing is that we do not know for sure. There is not enough empirical evidence to support or reject such a statement. The truth is that while there exists a considerable body of knowledge about terrorist groups and a somewhat smaller body of knowledge about organized criminal groups, we know too little about the logistical and operational 'links' between them to discover emerging patterns and trends.

What makes this conclusion even more depressing is that fifteen years ago, Grant Wardlaw, an outstanding Australian criminologist, when presenting a paper on "Linkages between the Illegal Drug Traffic and Terrorism", came to much the same conclusion. He wrote:

[1] An example would be the strategic alliance between the Sicilian Mafia and the Cali Cartel. The mafia helped the Cali cartel to break into the New York heroin market in return for franchise arrangements for cocaine in Europe. – Phil Williams and Ernesto Savona, op. cit., p. 31.

[2] Marc Galeotti. Crime Pays. *The World Today,* (London), August/September 2002.

> "what this analysis has shown is how little we know in detail about the linkages and what they mean. Clearly the drug-terrorism nexus is an important one, in some cases a critical determinant of the direction a terrorist movement will take.(…) Only with first-rate intelligence will we be able to approach the problems with the degree of sophistication which is required if we are to have any hope of making any impact at all….[1]

Those in government who often have first-rate intelligence on organized crime and terrorism often do not have the inclination to analyse it fully. Those in academia who would be willing and able to apply a scientific approach to reliable and up-to-date information on terrorism and organized crime, only rarely have full access to such data for their research.

Perhaps there is a role for ISPAC to serve as a forum to bring the two camps a bit closer together.

Bibliography

Arquilla, John and David F. Ronfeldt (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. St. Monica, Rand Corporation, 2001.

Adamoli, Sabrina, Andrea Di Nicola, Ernesto U. Savona, Paola Zoffi. Organized Crime Around the World. Helsinki, HEUNI, 1998.

Bovenkerk, F., Misdaadprofielen. Amsterdam, Meulenhoff, 2001

Cilluffo, Frank. The Threat Posed from the Convergence of Organized Crime, Drug Trafficking, and Terrorism. Statement before the U.S. House Committee on the Judiciary, Subcommittee on Crime, 13 December 2002.

Crenshaw Hutchinson, Martha. Transnational Terrorism and World Politics. *The Jerusalem Journal of International Relations*,Vol. 1, No.2, Winter 1975.

Cronin, Isaac (Ed.) Confronting Fear. A History of Terrorism. New York, Thunder's Mouth Press, 2002.

Europol. Threat Assessment. Europol First Situation Report. The Hague, Europol, 1999.

Geopolitical Drug Watch. Drug, Conflicts and Organized Crime, Paris, DGW, 1999.

Gunaratna, Rohan. Inside Al Qaeda. Global Network of Terror. London, Hurst & Company, 2002.

Henderson, Harry. Global Terrorism. The Complete Reference Guide. New York, Checkmark Books, 2001.

Krebs, Valdis E. Uncloaking Terrorist Networks. *First monday* (Peer-reviewed Journal on the Internet), Vol.7, No.4, April 2002.

[1] Grant Wardlaw. Linkages between the Illegal Drug Traffic and Terrorism. Paper prepared for the Conference on International Drugs: Threat and Response. Washington, D. C., Defense Intelligence College, 2-3 June 1987, p. 32.

Lupsha, Peter A., Transnational Organized Crime versus the Nation-State. *Transnational Organized Crime,* Vol. 2, Spring 1996.

Makarenko, Tamara. Transnational Crime and Its Evolving Links to Terrorism and Instability. *Jane's Intelligence Review*, 11/2001.

Martin, J. and Romano A. Multinational crime; terrorism, espionage, drugs and arms trafficking. London, Sage, 1992.

Mickolus, Edward. Combating International Terrorism: A Quantitative Analysis. Ph.D. Diss. New Haven, Yale University, 1981.

Millard, George. The Forgotten Victims of Narco-Trafficking in Latin America. In: Dilip K. Das and Peter C. Kratcoski. Meeting the Challenges of Global Terrorism: Prevention, Control, and Recovery. Lexington Books, 2002 (forthcoming).

Morton, James. Gangland International. The Mafia and Other Mobs in the Twentieth Century. London, Warner Books, 1999.

Naylor, T. Wages of Crime. Black Markets, Illegal Finance, and the Underworld Economy. Ithaca, Cornell University Press, 2002.

Oots, Kent Layne. A Political Organization Approach to Transnational Terrorism. Westport, Conn., Greenwood Press, 1986.

Prados, John (Ed.). America Confronts Terrorism. Understanding the Danger and How to Think About It. Chicago, Ivan R. Dee Publ., 2002.

Rapoport, David C. (Ed.). Inside Terrorist Organizations. London, Frank Cass, 2001.

Reich, Walter. Understanding Terrorist Behavior. In: Isaac Cronin (Ed.) Confronting Fear. A History of Terrorism. New York, Thunder´s Mouth Press, 2002.

Thamm, Berndt Georg and Konrad Freiberg. Mafia Global. Organisiertes Verbrechen auf dem Sprung in das 21. Jahrhundert. Hilden/Rhld., Verlag Deutsche Polizeiliteratur, 1998.

Thamm, Berndt Georg. Terrorism. Ein Handbuch über Täter und Opfer. Hilden/Rhld., Verlag Deutsche Polizeiliteratur, 2002.

Schmid, Alex P. The Links between Transnational Organized Crime and Terrorist Crimes. *Transnational Organized Crime,* Vol. 2, No. 4, Winter 1996, p.40-82.

Shelley, Louise (Professor and Director, Center for Transnational Crime and Corruption, American University). Identifying, Counting and Categorizing Transnational Criminal Organizations. Conference. paper, n. d..

United Nations. Office on Drugs and Crime. Towards a Monitoring System for Transnational Organized Crime Trends: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. Vienna, ODC, 2002 (forthcoming).

U.S. Department of State. The Nexus Between Drug Trafficking and Terrorism. Fact Sheet. Washington, D.C., Bureau for International Narcotics and Law Enforcement Affairs, 10 April 2002.

U.S. Government Interagency Working Group. International Crime Threat Assessment. Washington, D.C., Whitehouse, 2001.

Villamarin Pulido, Luis Alberto. El Cartel de las FARC. Bogota, Edictiones El Faraon, 1996.

Wardlaw, Grant. Linkages between the Illegal Drug Traffic and Terrorism. Paper prepared for the Conference on International Drugs: Threat and Response. Washington, D. C., Defense Intelligence College, 2-3 June 1987.

Williams, Phil. Organizing Transnational Crime: Networks, Markets and Hierarchies. In: Phil Williams and Dimitri Vlassis (Eds.). Combating Transnational Crime. Concept, Activities and Responses. London, Frank Cass, 2001, pp. 57- 87.

Williams, Phil and Savona, Ernesto. Introduction: Problems and Dangers Posed by Organized Crime in the Various Regions of the World. *Transnational Organized Crime*, Vol. 1, No. 3, Autumn 1995.

Williams, Phil. Transnational Criminal Networks. In: John Arquilla and David F. Ronfeldt (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. St. Monica, Rand Corporation, 2001.

Zanini, Michele and Edwards, Sean J.A., The Networking of Terror in the Information Age. In: John Arquilla and David Ronfeldt (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. St. Monica, Rand Corporation, 2001.

APPENDIX I: Stages of Organized Crime

One can categorize organized crime's relationship with the wider economic and political context in which it operates. A phase or stage model to this effect has been proposed by Peter A. Lupsha, explaining the rise of organized crime in the United States since the mid-19th century. This evolutionary model is probably also applicable to many other countries. The model involves predatory, parasitical, and symbiotic stages described below:

Table: Stages of Organize Crime (P. Lupsha)

1. ***Predatory Stage:*** criminal group is basically a street gang or group rooted in a particular area, neighbourhood or territory. In this phase, its criminal violence is most frequently defensive, to maintain dominance over territory, to eliminate enemies, and to create a monopoly over the illicit use of force. Once neighbourhood, territorial or ethnic enclave dominance is established, the predatory gang gains recognition among legitimate power brokers, local political notables and economic influential who can use the gangs' organization and skills at impersonal violence for their own ends, such as debt collection, turning out the vote, or eliminating political rivals or economic competitors.

2. ***Parasitical Stage:*** There needs to be a 'window of opportunity' such as war, conflict to create large-scale black market opportunities with the help of legitimate power sectors. Political corruption provides the essential glue binding together the legitimate sectors of the community and the underworld criminal organization. Increasingly, organize crime extends its influence over entire cities and regions and becomes an equal of, rather than servant to, the state.

3. ***The Symbiotic Stage:*** the separate but equal parasitical bond between organized crime and the political system becomes one of mutuality. The host, the legitimate political system, now becomes dependent upon the parasite, the monopolies and networks of organized crime to sustain itself. The traditional tools of the state to enforce law will no longer work, for organized crime has become part of the state; a state within the state.

Source: Peter A. Lupsha. Transnational Organized Crime versus the Nation-State. Transnational Organized Crime, Vol. 2, Spring 1996, pp. 31-32.

APPENDIX II: Links between terrorist groups and illicit narcotic drugs

Terrorist groups involved in drugs in	Heroine	Cocaine	Cannabis/ Marijuana/ Kat	Ecstasy and Amphetamines
Afghanistan (Talib., Al Qaeda)	X			
Albania/Kosovo/ Macedonia	X			
Burma/Myanmar (United Wa State Army)	X			X
Colombia (FARC, AUC)		X		
Lebanon (Hizbollah)			X	
Nepal (Maoists)			X	
Philippines (Abu Sayyaf)			X	
Somalia (Warlords)			X	
Sri Lanka (LTTE)	X			
Turkey (PKK)	X			
Uzbekistan (IMU)	X			

Other countries: Peru, Mexico, India, Azerbaijan/Armenia, Russia/Chechnya, Georgia/Adjaria, Abkhazia, North Ireland, Algeria, Egypt, Sudan, Senegal/Casamanche, Guinea Bissau, Nigeria, Sierra Leone, Democratic Republic of Congo, Congo Brazzaville, Chad, Uganda, Rwanda, Angola, Comoros/Anjouan.

Source: Geopolitical Drug Watch. Drug, Conflicts and Organized Crime, Paris, DGW, 1999; Berndt Georg Thamm. Terrorismus. Ein Handbuch ueber Taeter und Opfer. Hilden/Rhld, Verlag Deutsch Polizeiliteratur, 2002.

APPENDIX III: UN Definition of Terrorism (UN Ad Hoc Committee on Terrorism: Informal Texts of Art. 2 and 2 bis of the draft Comprehensive Convention, prepared by the Coordinator[1]).

Article 2

1. Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, causes:

(a) Death or serious bodily injury to any person; or
(b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment; or
(c) Damage to property, places, facilities, or systems referred to in paragraph 1 (b) of this article, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act.

2. Any person also commits an offence if that person makes a credible and serious threat to commit an offence as set forth in paragraph 1 of this article.

3. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of this article.

4. Any person also commits an offence if that person:

(a) Participates as an accomplice in an offence as set forth in paragraph 1,2 or 3 of this article;
(b) Organizes or directs others to commit an offence as set forth in paragraph 1,2, or 3 of this article; or
(c) Contributes to the commission of one or more offences as set forth in paragraph 1, 2, or 3 of this article by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either:

(i) Be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of an offence as set forth in paragraph 1 of this article; or
(ii) Be made in the knowledge of the intention of the group to commit an offence as set forth in paragraph 1 of this article.

[1] Reproduced from document A/C.6/56/L.9, annex I.B. These texts represent the stage of consideration reached at the 2001 session of the Working Group of the Sixth Committee. It is understood that further consideration will be given to these texts in future discussions, including on outstanding issues. – A/57/37 Annex II.

APPENDIX IV: UN Definition of "Organized criminal group"

United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, Annex I) Article 2, Use of terms:

For the purposes of this Convention:

(a) "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

(b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

(c) "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

Illicit Trafficking in Nuclear and Other Radioactive Materials

with a focus on nuclear and radiological terrorism

FRIEDRICH STEINHÄUSLER and LYUDMILA ZAITSEVA
Center for International Security and Cooperation (CISAC)
Stanford University, CA, USA

Introduction

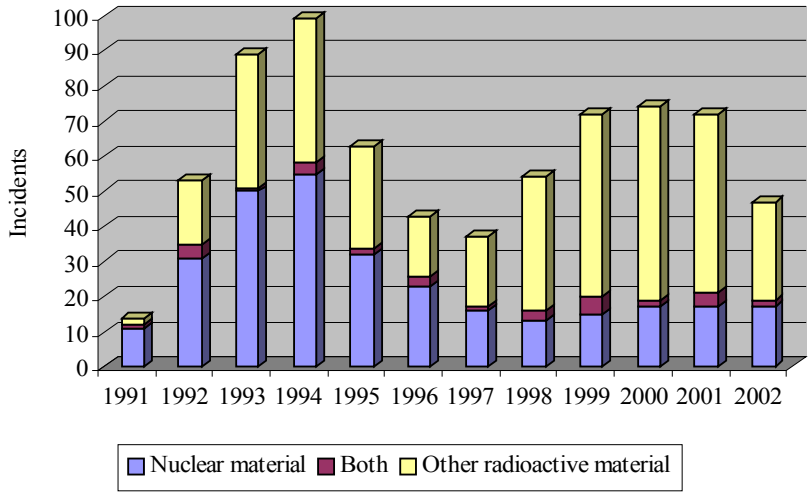
The problem of nuclear smuggling appeared shortly after the collapse of the former Soviet Union in 1991, when a weakened country with a plummeting economy, open borders, growing crime and corruption, and hundreds of tons of poorly protected nuclear material started to 'leak' abroad. The issue has been of great concern ever since and has prompted extensive research among security specialists. In order to get a comprehensive view on nuclear smuggling, the authors developed at Stanford University the *Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources* (DSTO). The DSTO contains over 950 cases of illicit trafficking of nuclear and other radioactive material[1], as well as incidents involving radiation sources out of regulatory control, the so called 'orphan' sources. The database combines government-confirmed information on illicit trafficking with open source reports and categorizes the incidents with an elaborate weighting scheme, which includes such parameters as reliability of the information source, technical feasibility and nuclear proliferation significance of an incident. DSTO collects incidents that happened worldwide, not just in the Former Soviet Union. In this paper, the DSTO will be used as the basis for the analysis of illicit trafficking on a global scale and the potential threat of nuclear and radiological terrorism.

Temporal and Regional Trends in Illicit Trafficking

Analysis of the DSTO illicit trafficking incidents on a global scale indicates that after a sharp peak in 1993 and 1994 there was a decline from 1995 to 1997, followed by another increase in 1998–2001 (Figure 1). Most incidents in the initial peak account for the detected smuggling in Western and Eastern Europe and in the Russian Federation.

[1] For the purpose of the DSTD, nuclear material is defined as uranium, plutonium, thorium or a compound containing any of these elements, and irradiated nuclear reactor fuel. Although nuclear material is radioactive, the term 'other radioactive' refers primarily to ionising radiation sources (e.g., americium, caesium, cobalt, strontium, radium, etc.).

Figure 1. Illicit Trafficking Incidents Worldwide: 1991-2002[2]



In the early 1990s, Europe observed a sharp increase in nuclear smuggling incidents (Figure 2). Soviet nuclear material, such as various forms of uranium and plutonium, as well as other radioactive material, unsuitable for building a nuclear weapon, was brought through the Eastern European countries into Western Europe in the hope of finding a market. However, the market either never existed there or was successfully disrupted by the European law enforcement authorities, especially those in Germany. German undercover agents conducted multiple sting operations in what they believed was an effort to recover "loose nukes" before a real buyer could be found. However, some argued that such efforts were in fact artificially creating a demand for the stolen material. When in August 1994 one of such undercover operations instigated an illegal transport of over 300 grams of plutonium on an ordinary Lufthansa flight from Moscow, the German public condemned the security services and parliamentary investigations of the intelligence activities were launched. As a result, the number of sting operations significantly diminished in 1995 causing a decrease in the number of detected illicit trafficking cases. In 1996, such operations were banned in Germany altogether and the smuggling cases in Western Europe subsequently decreased to a small fraction of the 1994 level (Figure 3).

[2] Friedrich Steinhausler & Lyudmila Zaitseva, Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources (DSTO), Center for International Security and Cooperation, Institute of International Studies, Stanford University, December 2002 (restricted access). Both state-confirmed and unconfirmed incidents with different degrees of reliability (high, medium and low) are included in the graphics. Data on illicit trafficking cases significantly varies in quality. Open press reports tend to sensationalize seizures on the one hand and omit important details on the other. Follow-up reports on investigations and trials are very rare. Therefore, information can often be distorted, inaccurate, and conflicting. (For a detailed discussion of data reliability problems, see William C. Potter and Elena Sokova, "Illicit Nuclear Trafficking: What's New? What's True?" *Nonproliferation Review* 9 (Summer 2002), p.119. A special parameter – reliability factor – was devised for the Stanford DSTO to define of reliability of information presented in each particular case: high, medium or low. *High* denotes high credibility of data (confirmed by IAEA and/or confirmed by competent national authorities), *medium* denotes reasonable credibility of data (not confirmed by the IAEA, but confirmed by local authorities directly involved in the incident investigations, as referenced in mass media reports) and *low* denotes less credible or conflicting data. It should be noted that over 80% of the incidents recorded in the DSTO are in the reliability categories *high or medium.*

Figure 2. Illicit Trafficking Incidents in the Western and Eastern Europe: 1991-2002[1]

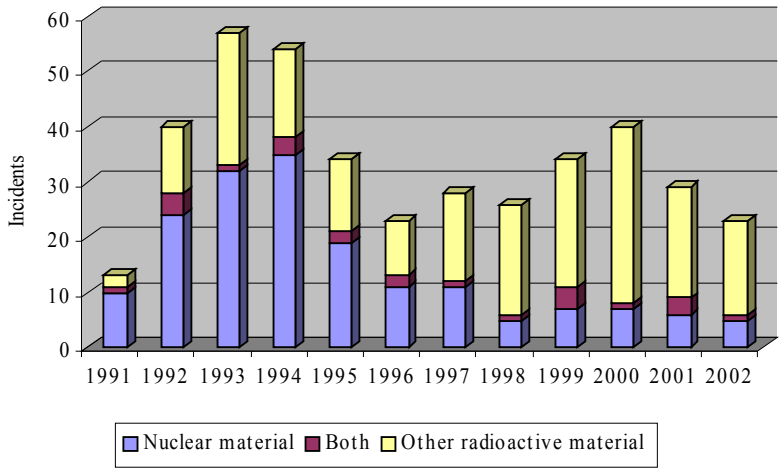
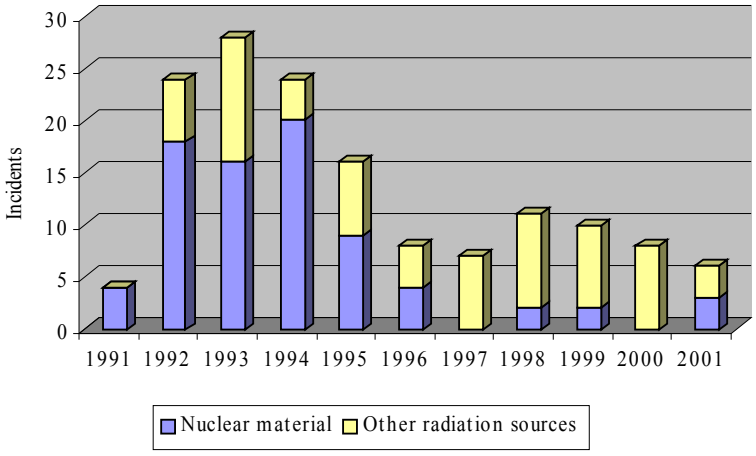


Figure 3. Illicit Trafficking Incidents in Western Europe (Austria, Germany, France, Switzerland, UK): 1991-2001[2]



Other factors have probably also contributed to the decline in nuclear trafficking in Europe in the mid-1990s. First, for the first time in years, the Russian Government acknowledged the leakage of the material from its territory and started major cooperative efforts to strengthen security at the Russian nuclear facilities and improve border control.[3] Second, some traffickers might have been discouraged from travelling to Europe either because they were convinced by the press that there was no market there or because they feared arrest by undercover agents. Finally, the improved border controls and policing for radioactive materials in Eastern Europe may have served as a barrier for nuclear trafficking from the former Soviet Union, allowing less material to reach Western Europe. By comparison, the decline recorded in the mid-1990s in Eastern Europe was less pronounced than in Western Europe and the number of incidents, involving mainly radiation sources, increased again significantly in 1999 and 2000. Seizures of nuclear material in Europe in 1995 accounted for only about half of such cases in 1994 and decreased even further in the

[1] Ibid
[2] Ibid
[3] Vladimir Orlov, Roland Timebaev, and Anton Khlopkov, *Nuclear Nonproliferation in U.S.-Russian Relations: Challenges and Opportunities* (PIR Center 2002), pp. 38-39.

following years. Since 1996, Western Europe has mainly observed trafficking in radiation sources. According to the preliminary data, no smuggling cases were recorded in Western Europe in 2002.

The situation in Russia from 1992 to 1997 appears similar to that in Western Europe – the smuggling incidents reached their peak in 1993–1994 and started to decline in 1995. Russia, however, observed a new, although less significant, peak in 1998–2001, with most incidents involving radiation sources. Before 1997, half of the detected cases involved nuclear material. The data for 2002 show a decrease in the overall number of incidents.

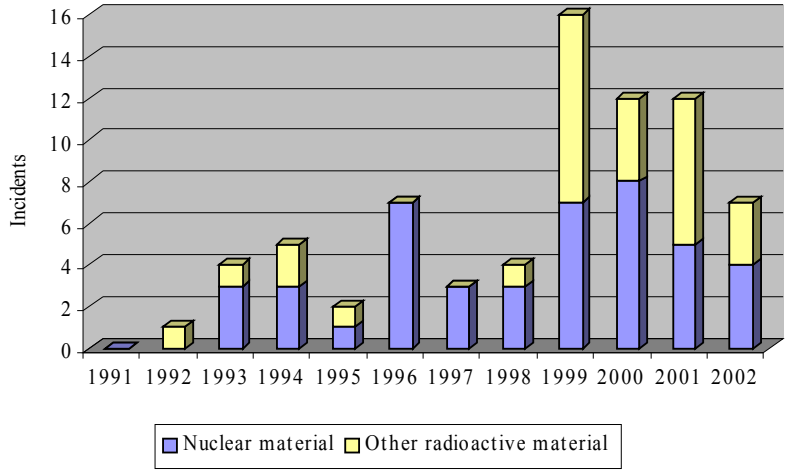
The DSTO data recorded for the period 1999-2001 show an increase in nuclear smuggling incidents in the Southern republics of the former Soviet Union (Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrghyzstan, Tajikistan, Turkmenistan, and Uzbekistan), the so-called Southern Tier, and Turkey from 4 cases in 1998 to 16 in 1999 (Figure 4).[1] This increase is in large part due to seizures of radioactive material using the new detection equipment supplied to the republics by donor countries. However, the number of seizures of nuclear material has grown as well. Although the total number of trafficking incidents recorded in the Caucasus, Turkey and Central Asia over the period January 1999 to December 2001 was lower than in Europe, enriched uranium or plutonium was seized more frequently on the Southern routes.[2] This finding suggests that nuclear trafficking from the former Soviet Union may now be flowing southward and that the reduction in smuggling incidents observed in Europe is, at least in part, due to this shift southward rather than to the improvement of the situation overall. However, the situation is not the same in all the regions. If Georgia and Turkey detect nuclear material smuggled from other countries, there is no reported activity to suggest that other republics are used as transit corridors as well. All of the nuclear material seized in Central Asia so far, had been stolen from the region's own nuclear facilities located in Kazakhstan and Tajikistan. The possibility that Russian nuclear material has been smuggled across the porous Central Asian borders, or Armenia and Azerbaijan, however, should not be excluded. Close proximity of these countries to potential end-users of nuclear material (e.g., Iraq, Iran, and terrorist networks in Afghanistan and possibly Middle Eastern countries) and inadequate border controls make them very attractive to smugglers. Since the collapse of the former Soviet Union, the region has developed into a major trafficking route for drugs and weapons.

Figure 4. Illicit Trafficking Incidents in the Southern Tier and Turkey: 1991-2002[3]

[1] For the purposes of this paper, the Caucasus region also includes the southern Russian autonomous republics of Northern Ossetiya and Dagestan

[2] For a more detailed description of the situation in the Southern Tier, see Lyudmila Zaitseva, "Illicit Trafficking in the Southern Tier and Turkey Since 1999: A Shift from Europe?" Nonproliferation Review 9, (Fall/Winter 2002)(in print).

[3] DSTO



Nuclear Material

In recent years, the number of incidents involving thefts and seizures of nuclear material is considerably lower than in the early 1990s. From 1991 to 1996, nuclear material was seized or stolen more frequently than other radioactive material (Figure 1), but this trend was reversed in 1997 and since then, there have been fewer cases involving nuclear material than incidents involving radiation sources. Over the period 1998–2001, the incidents involving nuclear material worldwide have accounted for less than one-third of the total number of illicit trafficking cases.

All seized weapons-usable material recorded in the IAEA Illicit Trafficking Database of state-confirmed smuggling cases totals about 9 kilograms (Table 1). However, there are at least 5 other highly credible proliferation significant cases that for various reasons have not been reported to the IAEA (Table 2). Together with the state-confirmed data, these incidents amount to 39 kg of HEU and plutonium. All of this material is believed to be of Russian origin. Of the 39 kg, 18.5 kg were intercepted during the attempted diversion in the Chelyabinsk region in 1998, 16.5 kg were stolen undetected and seized later during attempts to sell the material in Russia, and 4 kg were seized outside Russia – in Germany, Czech Republic, Georgia, Lithuania, Bulgaria, and France.

Table 1. Government-Confirmed Cases of Proliferation Significance[1]

Date of Seizure	Location of Seizure	Type and Amount of Material
May 1993	Vilnyus, Lithuania	100 g of 50% HEU
May 1994	Tengen, Germany	6.2 g of Pu-239 (99.75%)
June 1994	St. Petersburg, Russia	2.972 kg of 90% HEU
June 1994	Landshut, Germany	795 mg of ***87.7%*** HEU
July 1994	Munich, Germany	240 mg of Pu-239
Aug. 1994	Munich, Germany	363 g of Pu-239
Dec. 1994	Prague, Czech Rep	2.73 kg of ***87.7%*** HEU
June 1995	Prague, Czech Rep.	415 mg of ***87.7%*** HEU
June 1995	Electrostal, Russia	1.7 kg of 21% HEU
June 1995	Ceske Budejovice, Czech Rep.	17 g of ***87.7%*** HEU

[1] International Atomic Energy Agency (IAEA) Illicit Trafficking Database. See "Comprehensive List of Incidents Involving Illicit Trafficking in Nuclear Materials and Other Radioactive Sources: Confirmed by States," available form the IAEA Office of Physical Protection and Material Security.

May 1999	Dounav Most, Bulgaria	10 g of 73% HEU
Oct. 1999	Kara-Balta, Kyrghyzstan	1.49 g of Pu
Apr. 2000	Batumi, Georgia	920 g of 30 (±3)% HEU
Jan. 2001	Liepaja sea port, Latvia	6 g of Pu in Pu/Be sources
Jan. 2001	Tsessaloniki, Greece	3 g of Pu-239 in anti-static devices
July 2001	Paris, France	5 g of 72% HEU

Table 2. Other Highly-Credible Cases of Proliferation Significance[1]

Date of Seizure	Location of Incident	Type and Amount of Material
Oct. 1992	Podolsk, Russia	1.5 kg of 90% HEU
July 1993	Andreeva Guba, Russia	1.8 kg of 36% HEU
Nov. 1993	Sevmorput, Russia	4.5 kg of 20% HEU
1998	Chelyabinsk region, Russia	18.5 kg of HEU
2000	Electrostal, Russia	3.7 kg of 21% HEU

Thefts of weapons-usable nuclear material in Russia have been discovered at nuclear research facilities, fuel fabrication facilities, closed nuclear cities, and naval fuel depots. However, only one such theft (Sevmorput Shipyard, Murmansk region, Russia, November 1993) was noticed and reported to law enforcement officials, before the material was actually seized and traced back to the facility. All but one (Dounav Most, Bulgaria, May 1999) seizures of Russian weapons-usable material outside the country were a result of police and intelligence operations rather than effective border control. This allows us to put strengthening border control by equipping guards with radiation detectors into perspective. It is undoubtedly necessary to equip *all* border crossings with radiation detectors and train customs and border enforcement personnel in using this equipment as a minimum deterrence. Nevertheless, there is the continuing need for intelligence operations in order to identify illicit trafficking activities already taking place at the national level. Professional traffickers will test border crossings for the installation of radiation detectors and subsequently avoid those equipped. Instead, long, sparsely controlled borders will be used instead – as is done with smuggling of migrants and drug trafficking. Mobile and concealed radiation detectors should be considered as possible countermeasures.

In many cases the material was confiscated in the milligram or gram quantities. However, this should not be necessarily interpreted as the only amounts available on the black market. Similar to drug trafficking, trafficking in nuclear material is likely to start with offering only small amounts as a sample to a potential buyer, to be followed up with significantly larger amounts once a deal has been struck. This scheme was apparently used in the attempted sale of HEU in the Czech Republic and Germany in 1994, where almost three kilogram of 87.7 percent uranium was seized together with three samples of the same material. Gram amounts of uranium seized in Bulgaria in 1999 and in France in 2001 also appear to be of almost the same enrichment level. Besides, both samples were packaged in a very similar fashion, which strengthens the allegation that they may have originated from the same facility.

However, there have also been incidents involving kilogram amounts. The largest amount seized to date is 18.5 kg of HEU. It was intercepted at one of the nuclear facilities in the Chelyabinsk region of Russia during an attempted diversion by the facility employees. Should this attempt have been successful, the material could probably be enough to build one nuclear weapon.[2] Two other significant seizures involved almost 3 kg of 90 percent enriched uranium stolen from the Electrostal Machine-Building Plant near Moscow and

[1] DSTO

seized in St. Petersburg in June 1994 and 2.7 kg of 87 percent HEU believed to have come from the Obninsk nuclear research center in Russia and intercepted in the Czech Republic in December 1994.

If one were to compare nuclear smuggling with drug trafficking in the United States, where the intercepted drugs represent only 10 to 40 percent of the total amount smuggled into the country, it would be possible to imagine that there was a lot more nuclear material stolen and smuggled without detection than the estimated 39 kg.[1] Since the border control and law enforcement in Russia and its former satellites are clearly not better than in the US, it is safe to assume that the success rate of these countries' customs officials in detecting illegal immigrants and products is at best of the same order of magnitude, but most likely lower.

Radiation Sources

Whilst ionising radiation sources are unsuitable for building a crude nuclear device, some of them could be used for a terror attack deploying a radiological dispersal device (RDD) such as caesium-137, americium-241, radium-226, strontium-90, cobalt-60, californium-252, and irridium-192. Countries generally exercise stringent regulatory control over the radioactive material located in their territory. However, the degree of control varies widely, ranging from the lack of even a central national register of radioactive sources, to reportedly implementing a "cradle-to-grave" concept all through the life cycle of the material[2]. However, even in the latter case, for example the US Nuclear Regulatory Commission receives on average about 200 reports of lost or stolen ('orphan') radioactive material each year[3]. According to some estimates, the US has lost control over approximately 30,000 radioactive sources nationwide[4]. A European Union (EU) study estimated that every year up to about 70 sources are lost from regulatory control in the EU[5]. A recent European Commission report estimated that about 30,000 disused sources in the EU that are held in local storage at the users' premises are at risk of being lost from regulatory control. However, the report also noted that the majority of these sources would not pose a significant radiological risk if used in a dirty bomb[6].

Analysis of the DSTO shows that Cs-137, the isotope best suited for an RDD if used in a water-soluble form, is also most frequently trafficked. Since 1991, Cs-137 has been interdicted in approximately 50 percent of all DSTO smuggling cases involving ionising radiation sources (Figure 5). It is also the most frequently occurring "orphan" radiation source detected in half of such incidents recorded by the DSTO, in which the isotope was identified. In both categories, it is followed by Co-60 and Sr-90.

---

[2] Matthew Bunn, "The next wave: Urgently needed new steps to control warheads and fissile material," a joint publication of Harvard University's Project on Managing the Atom and the Non-Proliferation Project of the Carnegie Endowment for International Peace, April 2000.

[1] At best, law enforcement officials seize only 10-40% of the illegal drugs smuggling into the USA each year. See Phil Williams & Paul N. Woessner, "Nuclear material trafficking: An interim assessment", *Ridgeway Viewpoints*, 95-3, 1995, p.9.

[2] InternationalHAZAMAT Working Group (Eds.: F. Steinhausler and A. Sands), "White Paper: Reducing the Threat from Loss of Control of Hazardous and Potential Hazardous Materials," European Forum , Institute of International Studies, Stanford University, May 2002.

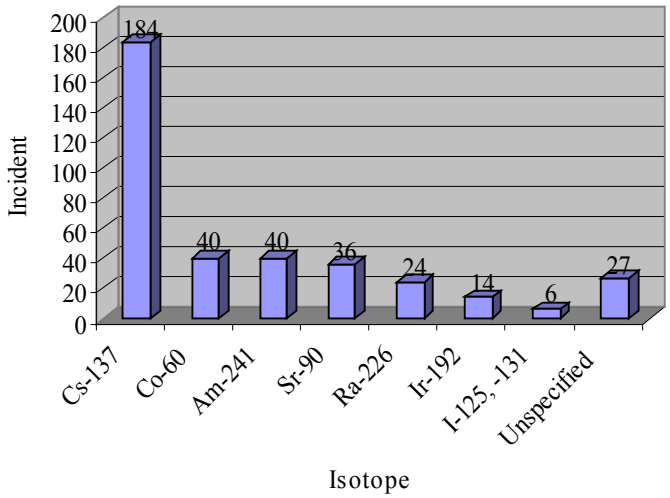
[3] These are not small sources, such as a smoke-detector, but radioactive material licensed under the Atomic Energy Act (1954). See Great Joy Dicus, "USA perspectives: safety and security of radioactive sources," IAEA Bulletin, vol.41, no.3 (1999), p.22.

[4] See Environmental Protection Agency, *Orphan Sources Initiative,* available at URL *http://www.epa.gov/radiation/cleanmetals/orphan.html*.

[5] IAEA Press Release "Inadequate Control of World's Radioactive Sources," September 2002; available at URL *http://www.iaea.or.at/worldatom/Press/P_release/2002/prn0209.html*

[6] Ibid

Figure 5. Illicit Trafficking Incidents Involving Radiation Sources: 1991-2002[1]



Potential for Nuclear and Radiological Terrorism

Although traditional terrorist groups have shown little interest in weapons of mass destruction, the new terrorism, such as seen on September 11, 2001, in the United States, presents a real threat. In a 1998 interview, Osama bin Laden said: "If I seek to acquire such weapons, this is a religious duty."[2] In January 2002, the Associated Press reported that U.S. military officials had found crude diagrams of nuclear devices in an al Qaeda safehouse in Kabul, Afghanistan[3]. The diagrams described components essential to nuclear weapons and led nuclear specialists to believe that if al Qaeda had enough weapons-usable nuclear material, it would be capable of building a crude nuclear device[4]. The material needed to build a crude nuclear device is either uranium highly enriched in the isotope U-235 (HEU), or weapon-usable plutonium-239. Whether or not terrorists succeeded in the acquisition of such material is unknown, but there is significant evidence that they have actively sought it. For example, in February 2001, Jamal Ahmad al-Fadl, a Sudanese national and al Qaeda defector, testified that he had negotiated a $1.5 million deal to obtain an unknown quantity of enriched uranium in Khartoum, Sudan, at the end of 1993 or the beginning of 1994[5]. He was allegedly shown a cylinder two to three feet tall with the words "South Africa" engraved on it, but he could not tell if there was indeed enriched uranium inside. In September 1998, another associate of bin Laden, Mamdouh Mahmud Salim, was arrested in Munich, Germany, and charged with trying to obtain highly enriched uranium in the mid-1990s on behalf of bin Laden.

At least one other organization besides al Qaeda, the Japanese doomsday cult Aum Shinrikyo, had sought a nuclear weapons capability. The cult tried to obtain the necessary material and expertise in Russia, by recruiting scientists involved in nuclear weapons research. Thus, a top scientist at the Kurchatov Institute, Russia's advanced nuclear research

[1] DSTO
[2] Transcript of interview with Osama bin Laden. *ABC News*. December 24, 1998. Retrieved on July 30, 2002 form *http://more.abcnews.go.com/sections/world/diarynews/binladen_wnt981224.html*
[3] Joan J. Lumpkin, "Al-Qaida had crude nuclear diagrams," Associated Press, January 31, 2002.
[4] David Albright, Kathryn Buehler and Holly Higgins, "Bin Laden and the Bomb," Bulletin of Atomic Scientists, January/February 2002.
[5] Kimberly McCloud and Matthew Osborne, "WMD Terrorism and Osama bin Laden,"CNS Report, Center for Nonproliferation Studies, Moneterey Institue of International Studies. Retrieved April 22, 2002 from *Http://cns.miis.edu/pubs/reports/binladen.html.*

facility housing large amounts of weapons-usable material, was found to be member of the Japanese cult.

There is also evidence that terrorists are interested in other, non-nuclear radioactive material that could be used for building an RDD. An RDD consists of a suitable radiation source combined with conventional explosives, a so-called "dirty bomb". Such a device would not necessarily cause more deaths than a conventional bomb, but would complicate the search and rescue operation after a terrorist attack, and increase the costs for the subsequent clean-up operations.[1] Jose Padilla, a US national arrested in Chicago's O'Hare airport after his flight from Pakistan in May 2002, had allegedly plotted such an attack in the United States.[2] According to media reports, Padilla had originally planned to build a nuclear weapon, but a senior al Qaeda operative advised him to think smaller and go for a dirty bomb instead. He was arrested before he could make any progress with his plan. Chechen rebels in Russia repeatedly threatened the use of radioactive material. In 1995, Shamil Basayev, a Chechen field commander, ordered the burial of radioactive waste in Izmailovsky Park in Moscow and informed a Russian TV station about its location. Although the radioactivity level of the found material was not very high, the incident nevertheless caused great concern about the possibility of more serious radiological terrorist attacks in the future. Special radiation search teams were set up in Moscow and some other large Russian cities in order to detect, secure and dispose of dangerous radiation sources. Another radioactive container attached to an explosive was found near a railway line in Chechnya in 1998. The incident was considered a foiled act of sabotage by Chechen militants.[3]

It should be noted that radiological terrorism is not limited to the use of radioactive material in an RDD only. For example, a strong gamma radiation source can be used for covert irradiation, resulting possibly in the death of the victim. In March 2002, Belarus police arrested members of a criminal gang who planned to plant radiation sources in Internal Affairs Ministry offices in two towns in Gomel Oblast. Four containers with radioactive material were seized from the gang members, together with firearms, a grenade, and explosives.[4] DSTO lists a total of 20 malevolent acts using radioactive material. Strong sources can also be used for the covert generation of radioactive aerosols to be inhaled by the unsuspecting users of a metropolitan subway system or an enclosed shopping mall.

In the recent past, organized criminal groups have reportedly also taken on the issue of nuclear smuggling. Thus, members of Italian organized crime were arrested in 1998 in possession of a nuclear fuel rod, enriched just below the 20 percent level to be considered weapons-usable.[5] The rod had been stolen from the Kinshasa research reactor in the Democratic Republic of Congo and was reportedly intended for sale to one of the terrorist organizations in the Middle East. In the beginning of 1990's, the Italian mafia reportedly shipped counterfeit merchandise (e.g., clothes, watches) to Russia and was paid for it with highly sophisticated military equipment, heavy and light weapons, and uranium[6]. Indeed, several incidents involving nuclear material of Russian origin were reported in Italy in the

[1] Friedrich Steinhausler, "What it takes to become a nuclear terrorist," *American Behavioural Scientist*, Vol.46, No.6, p. 782-795, February 2003.
[2] Amanda Ripley, "The Case of the Dirty Bomber," *Time Magazine*, June 16, 2002, Online version retrieved on July 30, 2002 from *http://www.time.com/time/nation/article/0,8599,262917,00.html.*
[3] "Container with radioactive substances found in Chechnya, "*ITAR – TASS*, December 29, 1998. Retrieved from NIS Nuclear Trafficking Database.
[4] "Belarusian police seize weapons, radioactive materials from crime ring," *Belapan*, March 6, 2002 (FBIS Document CEP20020306000194). Retrieved from NIS Nuclear Trafficking Database.
[5] Michaela Wrong, "More wreck than reactor, "*Financial Times*, 21 August 1999, p.8.
[6] Phil Williams & Paul N. Woessner, "Nuclear material trafficking: An interim assessment," *Ridgeway Viewpoints*, 95-3, 1995, p.9.

early 1990's. The trafficked material was allegedly headed for Middle Eastern countries and former Soviet intelligence officials were implicated in some of the incidents. Members of the Russian mafia have apparently cooperated with members of the Japanese Yakuza as well. According to some reports, they met in Vladivostok to discuss the feasibility of stealing nuclear material and nuclear weapons in the Pacific Region. Members of different organized criminal groups in Russia (e.g., Dmitry Naumov, Semyon Mogilevich, Grigory Louchansky) have considered forming alliances in getting involved in illicit trafficking of radioactive material.[1] Thus, according to reports by the European intelligence community, Semyon Mogilevich, an Israeli businessman of Ukrainian origin who had allegedly been involved with al Qaeda through drug trafficking, was approached by bin Laden's associates with a request to provide them with Russian fissile material[2].

Organized crime has the financial capacity to engage in the kind of transactions necessary to consider the acquisition of nuclear weapons from corrupt members of the military. According to the Russian Interior Ministry, the annual black market revenues of these groups now amount to US$ 18 billion. By comparison, the "Grozny deal" (an exchange of 2 tons of heroin and cash for nuclear weapons), believed to have taken place between al Qaeda and the Chechen organized crime in Russia, reportedly involved only US$ 20 million[3]. Organized criminal groups have well-established transcontinental trafficking routes for drugs, weapons, stolen art, and people. These "goods" are, in comparison to radioactive material, bulky, require large storage volumes, and can be detected using human sensors – none of which apply to the nuclear material needed for a crude nuclear device (less than 10 kg of Pu or 25 kg of 90 percent HEU) or an RDD (a few hundred gram of Cs-137). The logistical requirements to add trafficking of radioactive material to their existing trafficking activities are therefore minimal.

What should be done next?

Terrorist networks may be actively seeking HEU and plutonium to build a nuclear device or other radioactive material suitable for an RDD to deploy in a terror attack. Both types of material are subject to illicit trafficking today. Stealing the essential components to build a crude nuclear device, diverting other non-nuclear radioactive material to manufacture an RDD, or killing with a strong radiation source are no longer a hypothetical concerns, but goals actively pursued by disciples of catastrophic terrorism or members of organized crime as shown in several cases contained in the DSTO.

The large stockpiles of nuclear weapon-usable material worldwide and inadequate physical protection practices in some countries are reason for concern. According to 2001 estimates, eight countries (Belgium, France, Germany, India, Japan, Russia, the United Kingdom and the United States) possess among them 210,000kg of separated civilian plutonium[4]. These civilian stocks are growing and, given the current rate of increase, they will surpass the estimated 250,000 kg of plutonium in weapons or weapon reserves in a few years[5]. Highly-enriched uranium is even more widely spread around the world than plutonium and frequently less guarded, especially at some research reactors located in

[1] Jeffrey Robinson, *The Merger: The Conglomeration of International Organized Crime* The Overlook Press (New York, 2000).
[2] Fro details, see, "Osama bin Laden sotrudnichaet s russkoi mafiey" ["Osama bin Laden cooperates with Russian Mafia"], *Russian Information Agency (RIA) Novosti*, September 24, 2001.
[3] Kimberly McCoud and Matthew Osborne, "WMD Terrorism and Osama bin Laden."
[4] Arjun Makhijiani, "A Global Truth Commission on Health and Environmental Damage from Nuclear Weapons Production," *Science for Democratic Action* (Institute for Energy and Environmental Research Newsletter), 9 February 2001.
[5] David Albright and Lauren Barbour, "Separated Inventories of Civil Plutonium Continue to Grow," *ISIS* Plutonium Watch (Washington: Institute for Science and International Security, 1999), pp.2-3.

developing countries. Several thousand radiation sources currently in use in industry, medicine, research and agriculture around the world are potentially suitable for use in an RDD – and much easier for terrorists to obtain than nuclear material.

Since the threat of nuclear and radiological terrorism has a global dimension, an internationally coordinated response is required. In view of the devastating effects of a nuclear explosion or the extensive economic disruption and mass panic caused by the detonation of a dirty bomb, it is recommended to strengthen two lines of defence. First, physical protection of nuclear material should be elevated to the same level of focused worldwide attention as given to international safeguards against diversion of nuclear material from a reactor by the reactor operator[1]. Second, in case the physical protection system fails to stop the adversary actions, or illicit nuclear or other radioactive material is smuggled across borders, the policing inside the countries and the detection capabilities on the borders need to be strengthened. Details on the legal, logistical and technical requirements to meet these challenges have been outlined by a panel of international experts on the occasion of the European Union High-level Scientific Conference NUMAT, resulting in the *NUMAT Strategic Action Plan*[2].

[1] George Bunn, "Raising International Standards for Protecting Nuclear Material form Theft and sabotage," *Nonproliferation Review* 7 (Summer 2000). See also Matthew Bunn & George Bunn, "Nuclear Theft and Sabotage: Priorities for Reducing the Threat," *IAEA Bulletin* 43, No.4, 2001.

[2] Friedrich Steinhausler (Ed.), Proceedings, Int. Conference on Physical Protection "Strengthening Global Practice for Protecting Nuclear Material," Salzburg, Austria, 8-13 September 2002 (in press). Copies of the NUMAT Strategic Action Plan are available from the NUMAT Secretariat, Hellbrunnerstr. 34, A-5020 Salzburg, Austria; email: *physic@sbg.act.at* .

The Funding of Terror: Al-Qaida's Financial Links

MICHAEL E. G. CHANDLER
Chairman, Monitoring Group of the Security Council, United Nations

First of all it is important to put in perspective Al-Qaida and their financing and what has and is being done about it. Secondly, it is quite important to have a good understanding of what the United Nations itself is doing in a very positive way about such an unpleasant matter with which we now have to deal internationally, namely Al-Qaida and the Al-Qaida network.

Back in 1999, Osama bin Laden had to be brought to justice and because the people who were harbouring him at the time in Afghanistan, namely the Taliban, were not prepared to assist in this matter, the United Nations Security Council decided to impose sanctions on them. In December 1999 the Security Council approved resolution 1267. Even though it has been superseded both by events (in Afghanistan) and subsequent resolutions, Resolution 1267 remains important in the present-day context because it established three key points:

- Firstly the "1267 Sanctions Committee" (referred to hereinafter as the "Committee") which still operates and through which the monitoring group reports to the Security Council.

- Secondly, the resolution established a list of designated individuals and entities against whom the sanctions are targeted, subsequently titled the United Nations Consolidated List and to which I will return in a moment and,

- Thirdly, resolution1267 decided that Member States shall impose a travel ban on the Taliban and a freeze on their assets.

Since the Taliban did not respond at the end of year 2000 the United Nations Security Council re-enforced resolution 1267 (1999) with a new one, Resolution 1333, which added a ban on civil aviation movements in and out of Afghanistan and an arms embargo against the Taliban. Resolution 1333 (2000) also requested the Secretary-General to set up a panel of experts, which was given a period of 60 days, in which to recommend how the measures that had to be taken by States, under these two resolutions, could actually be monitored.

I had just finished setting up the new State Border Service in Bosnia in October 2000, when I got a call from the (UK's) Foreign and Commonwealth Office in London saying there was a job I might be interested in and that had to do with Afghanistan. My immediate reaction was negative. However, when I eventually spoke to the person at the other end of the telephone and heard the details, it turned out that I would not have to spend much time Afghanistan. This panel, on which they wanted me to be the UK representative, was going to work out of New York, only travelling to the immediate area and then back, in order to make recommendations to the Security Council, on how best to monitor the arms embargo and the travel ban.

So, for me, that's how it all began. We did the job in the spring of 2001, made our recommendations to the Council in June, which resulted in another Security Council

resolution by the end of July (2001), namely resolution 1363. Resolution 1363 (2001) actually established the monitoring mechanism, which was originally intended to monitor and assist the States bordering Afghanistan in their efforts to implement these smart sanctions (as indicated earlier).

However, for a number of unforeseen reasons, the actual formation of the group took a little bit longer than had been anticipated and it was actually the 23rd of September when I arrived in New York to help set-up the Monitoring Group. Over the next couple of weeks, the other four experts, destined to constitute the Group, joined me in New York. Needless to say, at the same time that we started looking into the task, the coalition forces commenced their assault on Afghanistan and its environs and the situation, particularly with regard to the Taliban changed very quickly. So, when in January 2002, the previous resolutions (namely 1267 and 1333) came up for review, the Council decided that the way they had been looking at the Taliban and those sanctions was now very different. The major interest, especially in the wake of September 11 was Osama bin Laden, Al-Qaida, what was left of the Taliban, and now clearly all their associates, or as they are referred to, "associated entities". January 2002 heralded in a new resolution, Resolution 1390, and my Group was re-assigned to monitor the implementation, by States, of the measures the Council has decided they shall take.

The three measures are a freezing of financial and economic assets, a travel ban and an arms embargo, targeted against those people and entities designated in the United Nations Consolidated List (the List). I said earlier that I would come again to the List, because it is one of the key elements, to assist States in their implementation of this resolution. Of the three measures, the one that is seen as the most important, is the freezing of financial and economic assets.

How do we (the Group) do our work? In keeping with our mandate, our usual way of operating is to visit member states, talk to their governments and ask them to explain to us the measures they have put in place, with respect to the resolution, and how they are actually implementing them. We discuss how they monitor the measures they have taken, the legislation, the rules and procedures. This involves the Group talking to the Ministries of Finance, the Interior, the Treasury, and/or Central Bank, Customs, Immigration and, depending on how each country administers controls of weapons, etc., the ministries or departments responsible for trade, economics and sometimes defence.

This aspect of the work is, in itself, very interesting. It is also very interesting what we find out as we go along. The Group is required to submit a written report to the Committee three times a year[1]. To date we have reported twice and (at the time of the Conference in Courmayeur) we were working on the third report.

I am very fortunate in having a tremendous team working on this project. We are five, appointed by the Secretary-General: myself, a retired UK diplomat (the first UK Ambassador to FYR of Macedonia and the UK lead on sanctions against Milošević and, later, the Bosnian Serbs); a retired major general from the Royal Jordanian Air Force (who is a wonderful asset because he brings the Islamic and the Arabic flavour into our considerations and deliberations), a French officer, who is seconded from the French Ministry of Defence (who has a wonderful nose for people who are trafficking and selling

[1] This reporting requirement has changed, under the new mandate (Security Council resolution 1455), to only twice a year for written reports, but in addition, the Chairman of the Group has to support the Chairman of the 1267 Committee, when he briefs the Security Council every 90 days.

weapons) and finally a very bright young police superintendent from the Royal Nepalese Constabulary, who is our leader on counter terrorism and our data base. The wonderful thing about these people is that they are all totally committed to the eradication of Bin Laden and al-Qaida. Even though we are not physically able to do a lot about it, because that is primarily for the law enforcement and security services of Member States, we are very interested in trying to make sure that Governments are able to do everything possible within the terms of the resolution. In addition we are expected to report to the Security Council accurately and to tell the Security Council what it needs to hear, and not necessarily, what some people would like it to hear. We are operationally independent and it is this operational autonomy that is one of our strengths.

Our second report was unfortunately leaked before it had been presented to the Committee, and it caused a certain amount of interest in a number of quarters. It has been very good to see the tremendous effort that is going on as we go around the world, to combat al-Qaida, and we have travelled a lot. There has been a noticeable increase in the amount of cooperation and exchange of information between intelligence, police and security agencies: nonetheless, much more still needs to be done – there is no room for complacency.

So much for the background of who we are and how we work. In our last report, issued in August 2002, we made a number of points. Two of these were of particular note: first of all, that we considered at that time, that the al-Qaida network was "fit and well" - I think those were the words we used – and secondly; we said that, based on everything that we had learnt and people have said to us, it (al-Qaida) was able "…to strike wherever it wanted, how it wanted and when it wanted." Tragically we have seen the very unpleasant bombing in Bali, and, more recently, we have seen other events; the French tanker "Limburg" off Yemen, the bombing of the tourist hotel at Kimbala (Kenya) and the attempt to down the Israeli airliner, with shoulder-fired (SA-7 type) missiles, as it took off from Mombassa (Kenya).

So, as we can see, there is no room for complacency, as far as Al-Qaida is concerned, notwithstanding the tremendous effort that has already been taking place over the last eight to ten months. It is still the assessment of the Group that al-Qaida remains capable of being quite a nuisance. If you combine all the other things we have heard over the last two and a half days (at this conference), that means continued vigilance is essential. Tremendous political will still be required from every Government to put all the resources and efforts necessary into continuing to disrupt Al-Qaida. Also efforts are required to make sure that Member States continue to improve the timely and effective exchange of information.

The reason I say this is because it is the general feeling of the Group that al-Qaida is now a network that is loose, has a flat hierarchy – and that is one of its strengths –, is still flexible enough to pop up and do something very unpleasant somewhere. Such events will probably not be on the scale of September 11, but it does not need to be that big to continue with a campaign of terror – and that is al-Qaida's aim. Unfortunately it is having its effect. It is having its impact on many economic aspects throughout the world – tourism, the airline industry, the aircraft manufacturing industry and reduced investment in many areas, to name but a few.

Now, within the context of this loose flat network, al-Qaida is believed to exist in between 45 and 60 countries. There is tremendous sympathy for the "cause" as expounded by Osama bin Laden in many countries. The way al-Qaida operates is almost like a franchise, we look upon it as "terrorism without borders" – "*terrorisme sans frontieres"*. As things are, al-Qaida seems to be one or two steps ahead of the international community; they can operate easily across borders and communicate within their groups and are able to go wherever they please. Well, if we get over some of the "hang- ups" between intelligence and investigatory bodies, to actually just share that extra bit of information quickly enough sometimes, then maybe the international community will start to get on top of the situation.

Now, to be more specific on the funding and financing of al-Qaida: There is a lot of talk about how much money Osama Bin Laden (or "OBL" as I will refer to him from now on) actually inherited. The figure that is often discussed is around US$300 million, but that was a long time ago and lot of water has flowed between here and Afghanistan and other places since he received that money. And we have to look at what has happened since. He was, as we heard earlier, in Sudan for a while. He invested a lot of money while he was in Sudan setting up businesses. He built a high way to the port and then when he had to leave Sudan and went back to Afghanistan he needed money there to undertake the many enterprises with which he got involved. There are also plenty of reports that be paid his "cohorts" quite well, both in Sudan and later, although there are instances of people asking for money and not getting it, and then there has always been the problem of who really is sympathetic to OBL and the al-Qaida network. It is from this sympathy, and we must not underestimate the extent of the sympathy that exists for al-Qaida and what some people see that it stands for, that produces money.

In my own country it has been a problem, just how much money goes into collection boxes at the mosque on Fridays - and that's not confined to UK, it happens elsewhere in Europe and many other parts of the World. And there are plenty of stories of how people cheered, very regrettably, when they saw what happened on September 11th. So there is a lot of sympathy for these people around the World.

The little guy whom they call Mamosie, although his name is Mamosa, who is the first man they caught in connection with the Bali bombing is totally unrepentant. He did what he believed was right to do, to kill 200 people, but he didn't do it with nothing! So clearly, al-Qaida still needs money. A lot of the money that keeps these cells going comes from petty crime, street crime, selling drugs on the streets, credit card fraud and things like that. There are indications that the Bali bomb needed only a relatively small amount of money. One figure quoted recently, was US$ 3,000. That was just for ammonia nitrate, the fertilizers, for the actual bomb and to buy the Mitsubishi van. So you see al-Qaida or its associates need money! – but not large sums.

Al-Qaida also needs money to move around the world. Whereas you have these regional groups, these regional cells who do the donkey work, very often one of the "high-up guys", who was trained in the camps in Afghanistan when they were at the height of their operation, has to come in and do the actual work, get things set up, make sure the people, the "foot soldiers", know how to put the bombs together and everything else. He may be around the day the bomb goes off, he may have gone two days before - but he comes and he goes! ... usually by commercial airline... So much for the travel ban, if he is one of the people on the UN List!

Then, let's really look and see where the money came from... or is still coming from, to be more exact. There were clear indications in all the investigative work after September 11, that clearly indicated that al-Qaida had been able to move its money around. The money they had for all aspects of this major operation is, I believe, normally quoted at around half a million dollars and that money was definitely moved through the formal banking system. Since September 11 there has been a tremendous amount of effort using anti-money-laundering procedures and techniques to clamp down on such transactions. This clamp down has worked so well that it is now quite difficult to trace the money and where they were moving it, but at least it is disrupting their way of operating in doing things probably "big time" again, at least in the near future.

However, there are recent indications that, maybe, money was moved to support the Bali bombing. Also, when another operative, Mashira, was picked up in the Middle East two or three weeks ago, there were suggestions of a figure, in the order of US$ 127,000 moving around through some Middle East banks to the Yemen, to support other attacks that were being planned at that time.

Hence, there are still indications of sums of money being moved through the formal banking system. Many people have been trying to work out how they move their money. If all concerned get really good at spotting suspicious transaction reports, being sent to financial investigation units [FIUs] or their national equivalents, with no results, then al-Qaida must be using other methods to move funds around. So the thinking is that al-Qaida is using informal transfer mechanisms (or alternative remittance systems) such as *Hawala*. *Hawala,* came into existence hundreds of years ago as a means of making sure that, when you were travelling as a trader along the *Silk Road* in Central Asia, you didn't get robbed because you had no money to be stolen from you. When you were transporting your goods, such as carpets, silks and spices, and sold them at the coast for onward transport to Europe or wherever they were going, you would get the value of what you were due when you got back home, to what is now Tajikistan or Kazakhstan or wherever.

Hawala then took on a new meaning with the Gulf oil boom. It came into its own then as the way most of the expatriate workers who were working in the Gulf states – and still are – sent their money home to Pakistan, India, Sri Lanka, Bangladesh and the Philippines. It is a fantastic system. It is fast; you can use it to get small sums transferred between say Dubai and some tiny village outside of Peshawar within less than three hours. It is cheap, you pay only three or four dollars for the service – just a small overhead for the *Hawaladar,* sitting on his cushions in some small shop in the *suk,* and finally it is secure. It works. The people trust it and it beats the banks everyday!

In order to get a better understanding of *Hawala*, there was a big conference in May 2002 in Abu Dhabi, hosted by the United Arab Emirates Central Bank. It was attended by around 300 people (mostly from that area and from one or two other areas which are well connected with this whole business of *Hawala*). The conference discussed what is, and what could be done to reduce the opportunities for *hawala* to be exploited by terrorists. Out of the conference came a declaration. This has, apparently, been followed by progress being made in establishing controls and regulatory means in some of the countries in the Middle East, South and Southeast Asia. For example, the UAE recently introduced a regulatory system to improve the control of *Hawala*. *Hawaladars or Hawala* operators have to "know their customers" and to report large sums of money transferred, etc.. Similarly, the Group was in

Pakistan, three or four weeks ago, and we heard of similar arrangements now coming into play within the financial regulatory structures of that country.

So progress is being made in this area, but it is still very easy to move sums of money around - or has been - so we cannot overlook the fact that this is a method which Al-Qaida is likely to go on using.

And we come now to the rather sensitive subject of charities. I do not intend to go into detail on the subject of those connected with Saudi Arabia. Currently, there is enough going on and I think it is best left to see how this all turns out. People are looking at it. It is being investigated; it is being discussed and I think that is the best way to leave it for the time being. But, the facts are there. On the United Nations Consolidated List (the List) there are a number of charities that have been put on during 2002. They have been put on the List because evidence has been found that in certain cases it is believed that, unwittingly, money donated and provided at the top end by generous people, for a genuine humanitarian cause, whether it's for refugees, schools, mosques or education has found its way downstream to al-Qaida. The way it works is that Al-Qaida operatives have infiltrated the entities actually doing the downstream project work, for example in Bosnia or Somalia. These are the people then divert funds from some local project. That's why you now have such charities as Al Haramain and the Benevolent International Foundation on the List. I am sure before long we may see more on the United Nations List, plus some of the people who have been involved in actually running those charities.

There are even connections in Southeast Asia, where one of the people running the Islamic International Relief Organization (the IIRO), in the Philippines and in other places was Bin Laden's brother-in-law, Mohammed Jamal Kalifa. He even had a Philippino wife as well.

So, the connections are there. The way the money has been moved around must have been there and it is not confined to the money that has come from the philanthropic side. There are indications of wealthy people in other Gulf states being equally generous.

I think that probably sums it up at the moment. These are the key areas that are being looked at now. As I said, Al-Qaida will continue to need money and find ways of moving it, as it (al-Qaida) is far from eradicated. It is likely to be around and alive for a long time. In analysing the situation, within our little group, we use the analogy of an infantry battle of the 1800's and the "red lines" advancing. As they go forward gaps are made in the lines as the troops are hit by shot and shell. But the gaps are refilled and new cells and new ranks form. And I think we must be aware that for some time to come this is likely to happen with Al-Qaida. As these cells get wrapped-up, due to the concerted efforts of the various law enforcement agencies, others come to light. It was very interesting to hear of the successes mentioned in this Conference, but also of the different connections, between cells in different countries. We are going to see more cells in the future.

There are too many sympathizers out there and too many people have been indoctrinated. There are still too many people who were trained in Afghanistan when the camps were still running who are at large somewhere around in the world - and those are the ones perhaps that we, in my little group anyway, are more worried about than the people we actually know about. It is important that every effort is made to take out the top people in the network. Our Group considers that Doctor Zawahiri, OBL's second-in-command, is much more dangerous, than OBL. But even the latter has said that even if you take out OBL, there are ten Osamas waiting to take over.

So, in summary, there must be a much more open and greater effort in the exchange of intelligence and that sort of information. All the efforts that are going on in the banking world to bring more regulatory action and investigative and knowledge of what is going on in the system must be reinforced. Those measures have to be kept going and reinforced and we just have to stay on top of this problem as it faces us.

9. Combating Trafficking

Combating Trafficking: The Role of Governments

PHIL WILLIAMS
University of Pittsburgh

Introduction

Ten years ago assertions that the rise of transnational organized crime, the trafficking of illicit goods, the provision of illegal services, and the expansion of illegal markets represented the dark side of globalization and interdependence were often dismissed as hyperbole. Today the skepticism has been replaced by a recognition that these phenomena have damaging consequences for governance at the national, regional, and global levels, have pernicious effects on national economies, undermine social cohesion and stability, and threaten human security, as well as national and international security. In response, governments and international agencies and organizations have increased the resources devoted to combating various forms of trafficking, organized crime, money laundering and corruption. Yet, as Moises Naim has pointed out, governments may be still losing the "five wars of globalization" – the wars against drugs, arms, and people trafficking, against intellectual property theft, and money laundering. Naim identifies various reasons for the lack of success, claiming that "the world's governments are fighting a qualitatively new phenomenon with obsolete tools, inadequate laws, inefficient bureaucratic arrangements, and ineffective strategies". He also contends that "the collective thinking that guides government strategies in the five wars is rooted in wrong ideas, false assumptions, and obsolete institutions".

It is against this background that the United Nations is making significant efforts to combat trafficking in arms, drugs and persons. If these activities are to be successful, however, then it is crucial to start from a solid baseline that is rooted in a clear understanding of the trafficking problem. Consequently, this paper starts with an effort to identify and elaborate some of the "wrong ideas" and "false assumptions" that underpin current efforts to combat trafficking. The analysis also suggests that there are several stark, unpalatable, and underlying realities that need to be understood before it is possible to think sensibly about, let alone devise, effective strategies. Failure to understand these realities is sure to affect efforts to reduce women trafficking to the Balkans and Western Europe, drug trafficking from Afghanistan and Colombia, and arms trafficking that fuels civil wars and ethnic conflicts. Accordingly, the first part of this paper elucidates some key characteristics of the trafficking issue, highlighting both several myths and several very compelling realities. After this has been done, the paper seeks to answer four major questions: (1) how can anti-trafficking policies and their implementation be made more effective? (2) do anti-trafficking measures provide sufficient solutions to combat overlapping issues in the economic sphere (e.g. anti-money laundering, anti-corruption measures etc.)? (3) to what extent can policies to combat organized crime be supplemented with specific anti-trafficking measures? (4) how can governments assist the business community in reducing the harmful effects of trafficking? In effect, the first question subsumes all the others. In considering the response to this fundamental question, it is helpful to identify three complementary approaches: incremental, unorthodox, and strategic. The incremental approach seeks to devise improvements and ensure that what is currently being done, is done better. The unorthodox approach is based on the inadequacy of existing responses, the potential inadequacy of more of the same, and the need for "out of the box" solutions. It seeks alternative strategies that could have significant impact in reducing the harm that is

done to societies, economies, and to individuals as a result of trafficking in arms, drugs, and persons, but that differ significantly from existing responses. The strategic approach aims to develop a comprehensive or holistic design that integrates existing and additional measures, including some that are not part of the orthodoxy, into an overall strategy. Such a design is the main focus of attention here and it incorporates related issues such as corruption and money laundering, the relationship between trafficking and organized crime, and ways in which the business community can be protected from the harmful effects of trafficking. Prior to looking at the policy prescriptions, however, it is necessary to provide an accurate diagnosis of the problem and to strip away some of the myths that have developed about trafficking.

Trafficking in persons, drugs and arms: myths and realities

If international community is to be successful in facilitating the development of successful strategies to combat trafficking, it needs to recognize several realities that, although compelling, have often been obscured by rhetoric, moral simplicity, and a failure to recognize the complexity of the issues involved. At least five myths about trafficking need to be dispelled and five realities need to be far better understood than is currently the case.

Myth 1: We understand the dimensions of the problem

Data on trafficking is still grossly inadequate, thereby helping to fuel unchallenged assumptions and assertions. While some trafficking organizations engage in multiple commodity trafficking, many others specialize in particular activities, developing skills, mechanisms, routes, and corrupt linkages, peculiar to the product they are focusing on. In some cases, often in response to changing market opportunities, some groups will move from one product to another. With the cessation of hostilities in the Balkans, for example, some of those groups which were deeply involved in arms trafficking began to focus more on trafficking in women. There are also some cases in which outlets for commercial sex are also outlets for illegal drugs. In yet other instances, there is barter trade involving the exchange of drugs for arms. To acknowledge these very specific forms of linkage and overlap, however, is not to conclude that there are invariably consistent connections between trafficking in arms, trafficking in drugs, and trafficking in persons. While they are sometimes parallel activities, the degree of overlap remains uncertain.

Much the same is true in terms of the relationship between organized crime and terrorism. In recent years, many commentators have emphasized the emerging nexus between criminal and trafficking organizations on the one side and terrorist networks on the other. Yet, a close examination reveals a more complex reality in which there are limited, albeit occasionally significant, cooperative links between insurgency groups and drug traffickers, but in which the most dominant and novel feature is the manner in which insurgents and terrorists have appropriated organized crime methods to fund themselves. This leads to both cooperation and competition between terrorist and criminal organizations and it is not surprising that, in some situations, terrorist groups and trafficking or criminal organizations are hostile towards one another. Once again, however, this is an area where anecdote too easily becomes a substitute for analysis and much solid research still needs to be done before governments have an accurate assessment of the main contours of the problem.

Myth 2. There is nothing new or different about contemporary forms of trafficking

It is very easy to conclude that there is nothing new or different about the kind of trafficking in arms, persons and drugs that is so pervasive in the early years of the twenty first century. After all, trafficking is one of the world's oldest endeavours, with a long if inglorious history. And even though the methods and routes change, there are also remarkable threads of continuity. In the late nineteenth century, for example, women were being trafficked from Ukraine (which happens to be one of the main sources of trafficked women today) to North and South America and the Middle East. Moreover, the traffickers were able to use the latest developments in transportation and technology – the steamship, the railways, and the telegraph – to facilitate their activities. Acknowledging the antecedents of contemporary trafficking is one thing; failure to recognize the extent of the current problem, the ease and speed with which trafficking can be carried out, and the political and economic power wielded by contemporary traffickers (along with other criminal organizations) is quite another. Indeed, in some parts of the world, such as the Balkans or Central Asia, trafficking is an economic activity to be reckoned with and the black market economy proportionately outweighs the legitimate economy. Moreover, trafficking has grown along with global business (sometimes in a parasitic relationship and sometimes as a parallel activity) to become a truly global phenomenon. Nigerian women trafficked to Italy for prostitution, arms from the Former Soviet Union supplied to African civil wars by a Tajik arms dealer based in the United Arab Emirates, and drugs from Colombia and Afghanistan on the streets of Scandinavian and Spanish cities are merely a few examples of the illicit forms of connectivity that characterize the global economy.

Myth 3. Trafficking is an unmitigated social ill with few beneficiaries

Most discussions of trafficking in drugs, arms, and persons fail to recognize that these phenomena benefit a large number of people. Most obviously, those directly involved in organizing trafficking activities find them very lucrative. There are also multiplier effects from the influx of illegal profits into national economies. In some developing countries as well as countries with economy in transition, drug cultivation and production provide a means of subsistence for peasants that is rarely matched let alone surpassed by alternative crops. Although governments have placed considerable emphasis on crop substitution and alternative development to try to wean growers from opium and coca, success has been limited. This is perhaps most evident in the resurgence of opium cultivation in Afghanistan in 2002 after the removal of the Taliban. Growing opium and coca is easier and more lucrative than growing alternative crops. There are also fewer uncertainties about market conditions. Emphasizing the fact that the peasants make only a very small percentage of the profits of the drug trade - as little as 1 per cent according to recent estimates - misses the crucial point that they can still make more than with most available alternatives. This also explains why there is a constant balloon effect, when repression in one locale simply leads to expansion in another. And for those who are involved not in cultivation, but in trafficking the rewards are even greater.

None of this is meant to condone trafficking in drugs, let alone trafficking in arms or persons. Indeed, it is hard to disagree with the International Narcotics Control Board in its statement that the gains are for the few and the losses for the many. Made specifically about trafficking in drugs, this comment could be applied equally well to trafficking in arms and persons. At the same time it has to be recognized that trafficking obeys the laws of the market, brings profits to those who organize the supply, and has some positive secondary

effects. In other words, even though trafficking activities are highly pernicious, and even though the costs to society enormously outweigh the benefits to the relatively small number of individuals who benefit, excluding the benefits from the equation risks over-simplifying the problem and making it appear more malleable than it really is. Recognition of this is rare, and even when it occurs, is usually accompanied by the caveat that although the benefits are short-term, the long-term consequences are invariably negative. Yet, as Keynes noted, in the long-term we are all dead: for peasants concerned about avoiding starvation, short-term benefits of drug cultivation are much more compelling than long-term negative effects. Similarly, even though trafficking in women completely undercuts arguments that organized crime tends to be victimless, for some women there are so few economic alternatives that going to another country and becoming involved in prostitution looks the least unattractive of an appalling set of choices – and their choice is conscious and deliberate even if ill-informed about how bad it will be.

The emphasis on the limited scope of the benefits of trafficking also ignores the fact that one of the methods that traffickers use to stay in business is to extend the benefits – either to local populations rendered sympathetic to the traffickers because of patronage, or to government and law enforcement officials who are neutralized through bribery and corruption. Indeed, the complicity of government officials in trafficking activities greatly facilitates the process.

Myth 4. Governments give high priority to combating trafficking

Although transnational organized crime and various forms of trafficking have been given much more attention since the end of the Cold War, it is arguable that policies to combat trafficking are (1) a low priority for governments (2) subordinated to broader geopolitical concerns.

The general impression of low priority for governments stems from the comparative paucity of resources devoted by most governments to criminal justice in general and to combating trafficking in particular. The subordination of anti-trafficking considerations to broader geopolitics has been evident in several relatively recent conflicts. NATO support for the KLA, for example, was rooted not only in principle (in order to stop ethnic cleansing) but also in the expediency of a temporary alliance against Milosevic that ignored indications of KLA involvement in criminal activities. Although it is possible to argue that the organization as such was not involved, there are indications that many KLA units and members were deeply implicated in drug trafficking. Indeed, one facet of the conflict over Kosovo was a struggle between the major cigarette smugglers (the Milosevic family) and the major heroin traffickers in Europe. Perhaps even more blatantly, if certainly understandably, the United States allied with the Northern Alliance to overthrow the Taliban even though many of the allied warlords were deeply involved in the opium trade. In the aftermath of the overthrow of the Taliban, the international community faces another dilemma: efforts to clamp down on opium cultivation and trafficking would intensify opposition, foment instability, and render it almost impossible for the new government to develop legitimacy and authority.

In other cases, the low priority is a result not of acute policy dilemmas created by geopolitical considerations but simply of the constant and often unavoidable tradeoffs of energy and resources that are inherent in government. Many governments, for example, have failed to give efforts to combat trafficking in persons the resources or attention they deserve. Penalties for trafficking in persons have remained largely inadequate, law

enforcement agencies have not been trained and equipped either to investigate adequately or to provide victim support, and only NGOs and international organizations have managed to keep the issue on the public agenda. Similarly, with arms trafficking, few governments have adequate regulation. All this is not to suggest that combating trafficking is simply a matter of will and commitment. Even when the will and commitment, and significant resources, are present, anti-trafficking policies encounter many problems.

Myth 5. There is a clear distinction between the legitimate and the criminal worlds

The divide between the underworld of trafficking and organized crime and the upper or legitimate world of business and government is not nearly as sharp as it first appears. Perhaps nowhere is this more obvious than in the area of arms trafficking. The most important factor differentiating arms trafficking from what governments often refer to as arms transfers is usually only the destination of the weapons. When governments cease business as usual, because arms are being used to fuel civil war or ethnic conflict and place an embargo on arms supplies to particular countries or regions, other less scrupulous suppliers simply step in to fill the vacuum. Put another way, when the operation of the legal or gray market is interrupted, the black market becomes dominant. This alone suggests that distinctions between legal policies and illegal activities are rarely as fixed and immutable as governments would like.

Distinctions between the criminal and legitimate worlds are also blurred by the connections that sometimes exist between them. In some cases, the connections are created through coercion, when traffickers and organized crime groups compel collusion, and use intimidation to take over or exploit legitimate businesses. In other instances, however, the connections between the two worlds are facilitated by bankers, lawyers, and accountants who act as what some law enforcement agencies in Australia describe as "gatekeepers". Moreover, it is often financial institutions themselves that are to blame and not simply rogue or corrupted individuals. Poor oversight is often used as an excuse for activities which are, in fact, calculated and deliberate. Lack of oversight is both facilitator and in-built excuse for reckless and unwise policies that, if discovered, are blamed on individual aberrations. Even putting aside the scandals that have highlighted the paucity of corporate governance, in recent years banks and bankers in several countries and jurisdictions have been involved in facilitating dubious financial transactions for political parties, criminal and drug trafficking organizations, and corrupt dictators. More generally, banks have been reluctant to impose anti-money laundering regulations: their business is about attracting money and from their perspective the origin of the money is largely irrelevant. Similarly, businesses often connive in trafficking activities. Antique dealers and auction houses rarely demand proof of provenance of antiquities that have been stolen and illegally exported; firms in the transportation industry welcome orders and are not overly concerned about what they are shipping so long as the documents appear to be in good order, and for the travel business a customer is a customer, irrespective of whether he or she is a legitimate businessman or businesswoman or a person being trafficked.

In sum, it is important to recognize the limits of knowledge about trafficking as well as the extent to which contemporary forms of trafficking transcend anything previously experienced, the benefits of trafficking especially in the short term, the limited resources that are devoted by governments to combating trafficking, and the lack of a sharp distinction between the legitimate world and the underworld. As well as dispelling these myths, however, it is necessary to emphasize key facets of the trafficking problem.

Reality 1. Traffickers have many advantages over governments

Governments have become so accustomed to dealing with each other that they have really been unprepared for the diversity of actors that now play major roles in global political and economic life. As a result, it has been hard for them to recognize that non-state or, what James Rosenau termed, "sovereignty-free" actors have certain qualities that make them very formidable adversaries. This is certainly true of terrorist networks, as became dramatically and tragically evident on September 11, 2001. It is equally true of criminal and trafficking organizations. Indeed, traffickers have many advantages in carrying out their activities including:

(1) the capacity to embed illicit products in the huge volume of legal trade facilitated by globalization and, at the practical level, by the development of inter-modal containers;
(2) the initiative in terms of method, time, and route;
(3) the choice of circumvention, concealment or deception (or indeed some mix of the three) to ensure that the illicit products reach their destinations;
(4) the capacity to neutralize or overcome the control mechanisms and regulatory measures imposed by governments through corruption and co-option;
(5) the capacity to accept significant losses as a result of interdiction and still make considerable profit;
(6) the capacity to use multiple jurisdictions and thereby ensure that the activity is distributed in ways that make it very difficult to counter. As one commentator on the illicit arms trade noted: arms traffickers are "stateless" threats in that they typically use one jurisdiction as a hub, a second as a banking center, a third to buy arms, a fourth as a weapons depot.
(7) the lack of a clear target for governments, partly because of the agility of trafficking networks and partly because of the fact that although traffickers routinely and inherently violate national sovereignty, they can still use national sovereignty for defensive purposes, retreating to safe havens when international pressure is on them.
(8) The use of network organizational forms that are, in so many respects superior to the hierarchical structures through which governments typically operate. When the bureaucratic nature of government is added to the equation, the advantage swings even further in favor of the traffickers.

Reality 2: Weak states are part of the problem rather than the solution

Many developing states and countries with economy in transition share certain characteristics: there is a low level of state legitimacy; border controls are weak; rules are ineffective; the institutions and people who represent the state put other goals above the public interest; there is little economic or social provision for the citizenry; business is not legally regulated or protected; social control through a fair and efficient criminal justice system is lacking; and other typical state functions are not carried out with either efficiency or effectiveness. Not surprisingly, these weakness provide a green-house effect for trafficking organizations.

Weak states suffer from capacity gaps, and capacity gaps lead to functional holes, (i.e. a failure of the state to fulfil certain basic functions that are normally associated with states and that are expected by the citizenry). Capacity gaps and functional holes are exploited by criminal organizations in one of two ways – either by filling them and, in

effect, substituting or compensating for the state or by exploiting the room for manoeuvre that they provide. Domestic criminal organizations providing private protection for business (protection that overlaps significantly with extortion) are generally substituting for the state; trafficking organizations that use weak states as a safe haven and typically smuggle drugs, arms and people across borders are exploiting the room for manoeuvre provided by functional holes such as inadequate law enforcement and border control. Both domestic criminal organizations and trafficking organizations have a vested interest either in perpetuating the weakness of states and governments or ensuring that even if they become stronger, they remain acquiescent.

Reality 3. Corruption is the lubricant of trafficking

It is hardly surprising, therefore, that even when the legal framework is present and enforcement capabilities are adequate, implementation of anti-trafficking measures remains uneven because of a lack of desire. Strengthening the state is one thing; minimizing corruption in government is another. And when critical members of the government, law enforcement, and customs agencies are beneficiaries of trafficking activities through corruption payments, they are loathe to push any activities liable to damage the flow of additional income. Unfortunately, the debates over corruption and over trafficking rarely intersect. The anti-corruption debate treats corruption solely as a condition of poor governance. Yet, from a trafficking and organized crime perspective, corruption is best understood as instrumental and specifically targeted rather than as a general or pervasive factor in political, social and economic life. There are, of course, connections between corruption as condition and corruption as instrument: the more pervasive the existing corruption, the easier it is for trafficking and other criminal organizations to identify appropriate targets who will facilitate their activities. Nevertheless, it is important to recognize the critical importance of targeted corruption by criminal and trafficking organizations.

For traffickers the targets of corruption vary according to where in the trafficking process they are. In the home base of the trafficking organization, corruption will typically be directed at government, the judiciary, and law enforcement agencies to ensure that the organization can act with impunity. In these circumstances, corruption often becomes systemic or institutional In transshipment and destination states the main targets will typically be customs personnel and border guards or immigration officials. The same is largely true in destination or market countries where the trafficked commodities end up.

Targeted corruption of this kind is highly damaging irrespective of its location. Corruption linked to organized crime and trafficking is the most pernicious form of corruption: it seeks to neutralize and circumvent the powers of the state, to co-opt the servants of the state, to eliminate social and territorial controls, and to neutralize the criminal justice system. In this sense, trafficking and organized crime related corruption can be understood as the HIV of the modern state: it breaks down the defenses of the body politic. In some cases, the process goes even further, leading to the emergence of what Roy Godson termed "the political-criminal nexus". In effect, trafficking and other criminal organizations develop corrupt and collusive relations with political elites, bureaucrats, and law enforcement and customs officials. Members of these elites become major beneficiaries of the trafficking process and other criminal activities. In some cases, they play a key role in organizing these activities; in others they simply provide a degree of protection that enables trafficking to continue with little or no interference. Whatever the exact role of

corrupt political elites, however, it is clear that they seriously exacerbate the trafficking problem.

Reality 4: Trafficking is a symptom of fundamental trends and problems.

Trafficking activities are, in large part, a symptom of underlying problems, rather than independent and autonomous activities. The most obvious of these underlying problems include: conflicts which generates the demand for arms; the co-location of insurgency and drug cultivation (e.g. Afghanistan or Colombia) which often leads to barter trade of drugs for arms; and the lack of employment opportunities in the licit economy that compels people to migrate to other countries, to migrate to the illegal economy, or to do both. Yet, trafficking also reflects the structural conditions of global politics in the twenty-first century.

Trafficking is related in complex ways to globalization. The increased speed and ease of global trade, finance, communications, transportation, and mobility, significantly augment the capacity of traffickers to operate effectively. Transaction costs have been reduced for traffickers just as they have for legitimate businesses. At the same time, some of the losers of globalization in the legitimate world have become major players in the underside of globalization. Both Afghanistan and Myanmar, for example, have been among those states that are most isolated and least integrated into the licit global economy. Yet both have become major players in the global drug trade. In this sense, trafficking can be understood as compensating mechanism that brings outliers back into the mainstream, albeit in a parallel underground economy. This is equally true in relation to many members of diaspora communities who often respond to marginalization and alienation in their host countries by providing trafficking outposts that link back to the home country. So long as globalization continues to have grossly disparate consequences, such balancing or offsetting mechanisms will continue to operate.

As suggested above, the growth of trafficking and organized crime more generally, is also related to the weakness of state institutions. The Westphalian system of state dominance is in decline, with a shrinking domain of state authority that is eroded from above by globalization and from below by a crisis of authority and legitimacy that was most obviously manifest in the communist world but that is certainly not restricted to it. What is perhaps most significant is the growth in the number of weak states, a growth that has led to the emergence of lawless regions and no-go zones where the state is simply not present. The implication of all this is clear: attacking the symptoms without also doing something about the underlying problems is a recipe for failure if not futility. And because the problems are structural rather than transient in nature, adequate responses will be more difficult to formulate and implement.

Reality 5: Transnational and multilateral responses are necessary but not sufficient to combat trafficking

Because trafficking is an inherently transnational activity only collective, multilateral or transnational responses will succeed in having a major impact. Criminal organizations in general, and traffickers in particular, engage in jurisdictional arbitrage, exploiting both jurisdictional asymmetries (highly divergent laws and penalties) and jurisdictional voids (countries in which there are no effective laws and regulations or no effective implementation of the laws and regulations against trafficking and its profits). Indeed, one of the problems is that trafficking networks often operate from jurisdictional

voids which, in effect, provide them with sanctuaries or safe havens. Consequently, no government, no matter how powerful, can adequately respond to trafficking in isolation. In effect, it is a distributed problem that requires a distributed solution.

In part, of course, there is a reluctance to opt for distributed responses, because of continued concerns about ceding or relinquishing national sovereignty, particularly in the areas of law enforcement and national security. As one commentator has noted, "governments need to recognize that restricting the scope of multilateral action for the sake of protecting their sovereignty is often a moot point. Their sovereignty is compromised daily, not by nation-states but by stateless networks that break laws and cross borders in pursuit of trade… Without new forms of codifying and "managing" sovereignty, governments will continue to face a large disadvantage" in their efforts to combat trafficking.

However, multilateral approaches to trafficking need to be accompanied by both capacity building and measures designed to ensure high levels of compliance with multilateral regimes. In some cases, these regimes have not been fully articulated and developed; in others the problem is not one of standards but of implementation.

Dispelling the myths about trafficking and emphasizing some compelling but oft-neglected realities is essential to the development of effective measures to combat trafficking in arms, persons, and drugs. The next section of this paper seeks to articulate some of the ways in which governments can respond more effectively.

Policy Reponses: What Governments Can Do

The United Nations, along with other international organizations and agencies, is in a good position to encourage and facilitate the process of responding more effectively to trafficking in persons, drugs, and arms. In devising these responses, there are three broad alternatives: incremental, unorthodox and strategic approaches.

1. Incremental approaches to strengthening anti-trafficking policies and their implementation.

Incremental approaches to strengthening anti-trafficking policies generally focus on law enforcement and seek to identify ways in which it can be made more effective. Some of the improvements cross all three areas of trafficking; others are particularly relevant to one trafficking activity rather than all three. Nevertheless, several requirements for enhanced effectiveness stand out, the most important of which is the need to introduce more risk into the trafficking process. This can be done in several ways, perhaps the most important of which is the introduction of more specific laws against trafficking and the vigorous and effective implementation of these laws. In some countries weak or nonexistent laws make trafficking a low-risk activity.

This is less true for drug trafficking than trafficking in arms or persons. The Vienna Convention on drugs and psychotropic substances has achieved almost universal adherence and laws against drug trafficking are by now commonplace. Moreover considerable efforts are directed against drug trafficking through interdiction, controlled deliveries, electronic surveillance, and the like. An increasing number of countries have also introduced asset seizure and forfeiture laws for drug trafficking and associated laundering of the profits. Yet

implementation remains a challenge. In responding to trafficking in arms and persons, the situation is even more urgent as many countries continue to have inadequate laws, enforcement is often both problematic and misguided (for example, treating women who have been trafficked for commercial sex as criminals rather than victims), and on those relatively few occasions when penalties are enforced they are often low. Moreover, although many governments are making progress, jurisdictional asymmetries and corruption continue to provide safe havens for traffickers and trafficking, thereby reducing the effectiveness of what are already rather modest efforts at international law enforcement cooperation. Even Operation Girasole which provided a good example of multi-national law enforcement cooperation against women trafficking, and had Europol playing important analytical and coordinating roles, was stymied by a limited investigation into the Russian and Ukrainian parts of the trafficking network.

2. Alternative approaches to the trafficking problem

Incremental approaches to trafficking in arms, persons, and drugs are dominant in the current repertoire of responses at both the national and international levels. The limitations on what has been achieved through such approaches has led many critics to demand more radical alternatives. Nowhere has this been more evident than in the area of drug policy, where interdiction is widely regarded as a failure. This has led to demands for de-criminalization or legalization of drug use and even drug supply. The rationale is that the major harm to society is not the result of drug use as such but of prohibition policies and the criminal activities they generate. De-criminalization, it is argued, would lower costs of the drugs and take the profits out of the business. The problem with this approach is that it ignores the social harms caused by drug use and abuse, harms that are independent of whether or not supply is criminalized. Moreover, it is not an approach that can be applied to trafficking in persons – which resembles a contemporary form of slavery rather than a victimless crime. Nor is it something that can be applied to arms trafficking where continued supply – and often the exchange of drugs or diamonds for arms – perpetuates violent conflicts.

Are there then any other unorthodox approaches to the trafficking problem that might be adopted by governments? Demand side reduction is often held up as a less orthodox solution than the supply side approaches, currently in vogue. Certainly demand reduction, whether through preventive diplomacy (for arms) or education campaigns (for drugs and use of prostitutes), is an important and all too often neglected approach. Arguably more resources could be devoted to these programs. Yet, there is almost certainly a point at which the law of diminishing returns becomes very apparent. Moreover, demand reduction is unlikely to work without some continued efforts at supply reduction. Rather than being a radical alternative that can stand on its own, therefore, demand reduction is better seen as a critical component of an overall strategic approach of the kind discussed more fully below.

Another approach is to put the emphasis less on law enforcement and much more on harm reduction. Treating trafficked women as victims is a key factor in this, and programs to rescue these women from the traffickers and to rehabilitate them in society certainly deserve a higher priority than they currently receive. Yet, unless there is a law enforcement component, women who are taken out of the commercial sex trade will simply be replaced by new victims. The implication once again is that although responses such as victim assistance and support that have been developed largely by the NGO community are particularly important, they need to be combined with the best of the current law

enforcement efforts (and some significant enhancements). In some cases, there are tensions between the two approaches. The extent to which trafficked persons can be used as witnesses against the traffickers as opposed to simply being protected and reintegrated into society is a natural bone of contention between law enforcement and the NGO community. It is one that requires both a degree of pragmatism and the development of far more effective witness protection programs than currently exist.

Transparency is another quality that is often emphasized by those who contend that existing responses are inadequate. There is something to this. In the world of arms supplies, for example, greater transparency and accountability would make it more difficult for black market arms suppliers to operate. Yet the whole point about trafficking is that it is covert. Transparency is not something that is easily achieved when those involved in the activities want to remain in the shadows. Consequently, transparency often requires thorough and careful investigation. Nevertheless, it is once again something that needs to be incorporated into a comprehensive response to the trafficking problem.

In terms of unorthodox solutions in the intelligence and law enforcement arena, some have argued that one approach might be to take initiatives that create greater competition and even overt conflict in the criminal world. Measures to reduce trust between traffickers and their immediate customers might make it harder for criminal organizations to develop and maintain strategic alliances. Creating such difficulties, provoking wars between rival traffickers, and creating distrust in the networks, increases transaction costs and thereby makes the business less profitable. The difficulty is that although this might help to prevent the concentration of criminal power, it would simply make it easier for the lower profile traffickers to develop greater market share. In some cases, provoking criminal conflicts could also backfire and lead to the concentration of power in the criminal world, as one group emerges dominant.

In short, although unorthodox solutions to trafficking might appear superficially attractive, they also encounter enormous difficulties in practice. Moreover, they generally deal with only one facet of the problem, leaving others untouched. Finally, they can also have unpredictable consequences that could ultimately exacerbate rather than alleviate the problem. The other shortcoming is that these approaches do not take sufficient account of the corruption that typically facilitates trafficking or the laundering and enjoyment of profits that is the ultimate outcome of a successful trafficking process. A comprehensive strategic approach, in contrast, can take account of these broader issues. Indeed, it is to the key components of such an approach that attention must be given.

3. A strategic approach to strengthening anti-trafficking policies and their implementation.

This section identifies the major components of a strategic approach to combating trafficking in arms, drugs and persons. It is designed to take into account the myths and realities discussed above as well as the shortcomings of both incremental and less orthodox approaches. It is also based on a recognition that some of the alternatives to current policies – while not compelling as single solutions – can usefully be integrated into a more far-reaching strategy. With these considerations in mind, a strategic approach to combating trafficking needs to answer questions such as: who develops the strategy? what are its major objectives? what kind of principles need to be embodied in the strategy? what are the major components of the strategy? and what are the major targets of the strategy? The following analysis elucidates a 10 point strategy that seeks to answer these questions. Although these

are presented as separate components of the strategy, however, it bears emphasis that these components are often closely interlocking and mutually reinforcing.

(i) Acceptance of a variable geometry institutional framework

While it would be ideal if there were a single global agency with the responsibility for formulating and implementing an anti-trafficking strategy, this is not the case now, nor is it likely to be the case in the foreseeable future. Consequently, different international institutions and national agencies can play different but complementary roles, depending on their particular capabilities and resources, their mandates, and the particular facets of the trafficking problem for which they have a responsibility. The United Nations is critical in the area of norm creation, particularly through the Palermo Convention on Transnational Organized Crime, and has also been important in training and assistance as well as analysis. Interpol and Europol are both critical in information sharing activities. The OSCE can assist in coordination and training in its areas of competence. So long as critical functions are identified and implemented appropriately, the issue of who does what is secondary. One important initiative, however, would be for some kind of high-level meeting among representatives of the major institutions, agencies, and organizations involved in efforts to combat various forms of trafficking, organized crime, and corruption. At the very least, this should include representatives from the United Nations Office on Drugs and Crime, the OSCE, the World Customs Organization, the G-8 Secretariat dealing with Transnational Crime, the European Union and the Council of Europe, the Financial Action Task Force, the Egmont Group of Financial Intelligence Units, Interpol and Europol. As well as these obvious agencies, the process could be extended to NATO, the South-East European Co-operation Initiative (SECI) Regional Center to Combat Transborder Crime, the Task Force on Organized Crime in the Baltic Sea region, as well as to CIS coordinating bodies in the fight against trafficking and organized crime. The purpose would be to work out at least a broad division of labour, to ensure that particular problem issues or countries did not fall through the gaps, to coordinate rather than duplicate efforts so that scarce resources are utilized most effectively, and to identify more systematically than is currently done where these organizations can most effectively work together. Such an effort could not be simply a one-time affair. It requires both annual meetings and the creation of an ad hoc coordinating group that would meet much more regularly in an attempt to ensure meaningful cooperation and coordination and bring a degree of coherence and purpose to what are currently largely ad hoc and uncoordinated initiatives.

(ii) Achieve enhanced understanding of trafficking

A strategic approach to the trafficking problem needs to go well beyond law enforcement and incorporate intelligence assessments that are based on an understanding of the trafficking process, the underlying market dynamics, the nature of the participants in the trafficking business, the methods and modalities of trafficking, the profits that accrue and how and where they are distributed, re-invested, and laundered. These assessments require a creation of a knowledge base that (1) involves pooling of data-bases (2) is network-based (3) crosses national borders and is shared by intelligence and enforcement agencies in multiple jurisdictions (4) makes full use of the knowledge provided by the NGO community, which often has detailed information about particular transactions and local conditions relating to trafficking in drugs, arms, and persons, (5) makes use of information from the private sector, and (6) considers potential ways in which trafficking networks might successfully adapt to, and circumvent, law enforcement efforts. A knowledge-base of this kind is essential in each of the three trafficking areas under consideration (as well as in

other areas such as trafficking in art and antiquities or endangered species), but provision also needs to be made for cross-referencing the data in ways that reveal otherwise hidden connections between the three trafficking areas such as personal overlap, (the same people active in each product niche), personal linkages (such as the cooperation between individuals in different product niches) use of the same routes or methods, use of the same institutions (institutional linkages) or similarities in the way profits are laundered.

(iii) Develop realistic and explicit objectives and measures of effectiveness

The elimination of trafficking in arms, drugs, or persons is impossible. Approaches designed to reduce the size of the markets, to reduce the amount or number of drugs, arms and persons trafficked, to make these areas less profitable and more risky, and to reduce harm to societies and to individuals, however, are subject to the criticism that they do not go nearly far enough. Yet such approaches recognize the persistent nature of the trafficking business as well as the difficulty of interventions designed to change market choices. In some ways the strategy advocated here mirrors that of the Cold War when grand designs for disarmament gave way to more realistic efforts to limit arms in ways that enhanced strategic stability. Strategy, as much as politics, is about the art of the possible. A realistic strategy requires realistic goals that in turn yield tangible measures of success. Such measures need to be both quantitative and qualitative, encompassing obvious indicators such as number of arrests, indictments, and convictions for trafficking offences, or the amount of drugs or illegal arms that are seized, as well as less obvious and less tangible assessments. Assessments of the impact of deterrence strategies as well as other preventive measures, of education campaigns, and of harm reduction schemes are less easily quantified but are nonetheless significant.

(iv) Attack the basis of the illicit markets

Another component of a comprehensive strategic approach is attacking the market. This can be done in several ways, but invariably needs to deal with the dynamics of both supply and demand. Education is often a key component of this, but can differ in its target and impact. In trying to counter the drug market, for example, education is important on the demand side, where it is a key component of restricting the market and reducing the profits. Unfortunately, the market impact of education is all too often ignored. In some countries debate on drug policy, in particular, demand reduction and supply reduction are seen in terms of a dichotomy rather than as complementary efforts to make the market less profitable and, therefore, less attractive. Indeed, education and rehabilitation are not soft options, but are options designed to reduce the market. With trafficking in persons, in contrast, education is, initially at least, more important on the supply side. The supply of people from transitional and developing countries to the more developed countries has been greatly facilitated by the fact that many people are virtually oblivious to the slave-like conditions that they will find themselves in if they become victims of trafficking. Consequently, educational efforts are particularly important in countries where the attraction of emigration often combines with wishful thinking to encourage a complete disregard of the associated dangers. Education is also important at the demand level, where male customers of women trafficked for the commercial sex trade need to be made aware of the degradation and despair that they are tacitly condoning with their actions and actively encouraging with their money. In relation to the arms trade, education is less relevant. Indeed, attacking the demand for arms is particularly difficult given the endemic nature of regional conflict and civil war. Yet it is not impossible: the equivalent to drug demand reduction in terms of attacking demand for small arms and light weapons is to devote more

resources to early warning and preventive diplomacy. This approach can be augmented by efforts to encourage voluntary arms restrictions on the potential belligerents rather than war-time embargoes which are inherently self-defeating because of the prohibition-price dynamic.

(v) Attack the trafficking networks

Another critical component of a comprehensive strategy is to attack the transnational networks that connect the demand and supply sides of the market. This has both legal and operational dimensions. In order to strengthen the legal framework, it is necessary to develop specific anti-trafficking laws and regulations. Many countries have laws explicitly directed against organized crime. They include in their criminal codes penalties for criminal association, for criminal conspiracy or for patterns of racketeering activities. Moreover, many have also introduced measures to conform with the Palermo Convention against Transnational Organized Crime and its Protocols. In terms of trafficking, most have also developed specific measures against the use, cultivation, transportation and sale of drugs. The development of measures against illicit arms trafficking has lagged somewhat behind, largely because of the existence of the white and gray markets in arms and the fact that often it is not the weapons themselves that are problematic but their destination. Similarly, measures specifically designed to combat trafficking in women for commercial sex have often been lacking. And even when they have been introduced, penalties have been too low to create a sufficient level of risk to deter traffickers.

The need for specific measures against trafficking is an important complement to measures against organized crime for several reasons. First, not all traffickers are members of criminal organizations. Some are crooked businessmen who engage in both licit and illicit activities; others, particularly in the area of trafficking in persons, but also in the drug area, are essentially opportunistic amateurs who act alone and do not meet the requirements for the UN definition of organized criminal group. Second, it is sometimes easier to prove involvement in trafficking activities than the more nebulous notions of criminal conspiracy. Third, a focus on the crimes of trafficking is particularly useful in cases where the networks involved are fluid and amorphous collections rather than the tightly-knit criminal families that are the more traditional targets of anti-organized crime legislation. Fourth, laws on trafficking should also include support for victims of trafficking, support that should supercede issues of whether or not the people who have been trafficked are in the country legally or illegally. While this is consistent with the Palermo Convention's emphasis on victim assistance, it is something that needs to be as explicit as possible in national laws if it is to succeed in changing the attitudes of many policemen who still treat women involved in prostitution, even if they have been trafficked, as criminals rather than victims.

Such measures help to increase the risks faced by traffickers. As Ernesto Savona has so persuasively argued, however, the risks and costs of criminal activities such as trafficking must not only be increased but also distributed more widely and more evenly. Only if this is done, does it become difficult for the traffickers to find safe havens and sanctuaries from which they can operate with impunity. Crucial to achieving this is greater inter-operability of legal systems, a goal that is more realistic and acceptable than notions of complete harmonization. Indeed, a degree of inter-operability that allows for dual criminality combined with the extension of mutual legal assistance and extradition agreements, arrangements or legislation to encompass major kinds of trafficking activities, could significantly increase the degree of risk faced by traffickers, irrespective of where they were operating. One way of looking at such arrangements is that they allow the

international community to compensate for the inadequacies and shortcomings in the criminal justice systems of weak states.

Attacking trafficking networks through more comprehensive and distributed laws needs to be accompanied by operational attacks on these networks. Initially, this requires identifying critical nodes and connections in the networks. Once these have been identified, it is then necessary (1) to engage in the systematic removal of the network organizers, (2) to eliminate those figures who are pivotal in maintaining communication in the network, (3) to attack the connections between the criminal world and the upper-world, connections that involve corrupt linkages that protect both the criminals and their activities.

The kind and number of critical nodes will vary from one trafficked commodity to another. In the case of small arms and light weapons trafficking, arms brokers certainly constitute some of the more important nodes. There are several reasons for this ranging from accumulated expertise to lacunae in national legislation. Moreover, a relatively small number of key figures have the resources to acquire, transport, and sell arms. Yet there is also a second category of brokers who do not do it all themselves but are able to put together various parts of the transaction chain for the illicit supply of arms. According to one report, a retired U.S. intelligence officer with experience of brokering arms transfers out of Eastern Europe described the ease and speed with which it was possible to arrange an illicit deal. In his view, obtaining price quotes from European-based brokers with good contacts in the East, officials at various Ministries of Defense, higher-ups at a few scattered weapons factories would take no more than 48 hours. Bogus end-user certificates could be acquired from a known dealer who traditionally kept a stack in his safe. According to the same report, the whole process could be completed in a month. In effect, these second-tier brokers put together the supply of small arms and light weapons. As such, they represent critical nodes whose elimination would seriously degrade arms trafficking networks.

As well as attacking the critical nodes, it is also necessary to target the critical linkages and the mechanisms used for these linkages. In the case of the illegal trade in small arms and light weapons, one of the most important of these links in the supply chain is cargo planes and the pilots who fly them. This requires stricter control of aircraft and of pilots.

In the case of drug trafficking, the networks are both more extensive and more fragmented. Yet a similar focus that seeks to identify and target key nodes (whether particular people such as chemists or key processes such as those involving precursor chemicals or transportation) in the production and supply networks could also yield very significant results.

In other cases, of course, it is necessary to target not simply the critical nodes in the criminal network, but the points of connection between the criminal network and the legitimate world. In some cases, this requires the identification and arrest of officials linked to the criminals; in others it requires going after the businesses that provide fronts for the criminal activities. It also requires efforts to remove the members of the criminal network from those legitimate institutions in which they have embedded themselves in order to facilitate their illegal activities. In addition, to these direct attacks, it is also possible to introduce distrust and disinformation into the network, attacking the basis of trust on which it operates.

Underlying all this and helping to make it possible is the increased capacity for network analysis using increasingly sophisticated software tools. These tools are extensively used in law enforcement for investigations at the tactical level; they can be used even more effectively for strategic mapping of trafficking networks and identifying points of vulnerability for attack.

(vi) Target the profits

As part of a comprehensive anti-trafficking strategy it is essential to make it more difficult for the traffickers to profit financially from their activities. In part, this requires that any governments that have not already made trafficking in arms, drugs and persons predicate offences for money laundering do so as soon as possible. It also requires that governments introduce anti-money laundering measures that at least meet and preferably exceed the requirements of the UN Convention against Transnational Organized Crime. Measures such as cash transaction reports and suspicious activity reports, along with requirements for due diligence and "know-your-customer", at least make it more complicated for traffickers to launder the proceeds of their criminal activities. Measures for asset seizure and asset forfeiture can be used to attack directly the proceeds of crime, while the assets seized can be used for victim assistance programs, especially in the area of trafficking in persons.

If it has become easier to identify and investigate suspicious transactions, in too many cases investigations fail to result in indictments let alone convictions – which are perhaps the most important indicators of success in making money laundering a high-risk rather than low-risk activity.

As financial systems have become more regulated and more transparent, however, traffickers and other criminal organizations have adapted by using alternative laundering methods, such as the movement of bulk cash, the use of front companies, and the use of underground banking or alternative remittance systems such as hawala. One area that is almost certainly a favourite of traffickers (who, after all are involved in the export business, if illegally) is trade-based money-laundering, which is a natural alternative when direct placement of criminal proceeds in the financial system is more difficult. This can be done through the use of "legitimate" front companies that engage in legal business as well as providing a cover for illegal transactions. Import-export companies, travel agencies, and transportation firms are not only important to the trafficking process but are natural conduits for financial transactions and lend themselves easily to the kinds of over-invoicing and under-invoicing that are crucial to the laundering process. Operation Girasole identified the key role that travel agents and some hotels played in the women trafficking process. It is likely that some of these firms were also involved in laundering the proceeds of the trafficking operations, thereby playing a dual function. The point is, however, that anti-money laundering measures need to focus on these companies. Additional options for attacking the proceeds of trafficking include more vigorous use of taxation departments for investigations, more stringent registration and reporting requirements for companies, and more widespread use of asset seizure and asset forfeiture laws.

(vii) Attack corrupt support structures and networks and pressure corrupt governments

As suggested above, trafficking does not exist in isolation. It is greatly facilitated by corruption. Responding adequately to this aspect of the problem, however, is hindered by the fact that the anti-corruption debate on the one side and the anti-trafficking and anti-

organized crime debate on the other are all too rarely connected. As suggested above, the implication is that generalized concerns (and the corresponding policy responses) about corruption as a condition need to be replaced by a recognition that the most pernicious forms of corruption are related to trafficking and the power of organized traffickers to use corruption as an instrument to co-opt people and to neutralize criminal justice and law enforcement institutions. One simple measure consistent with such a recognition is for governments to adopt particularly severe penalties for corruption that is linked to trafficking or organized crime. The irony is that the states and societies that most need to formulate and vigorously implement such anti-corruption laws are the ones least likely to do so. Even if anti-corruption laws are on the books, they are usually little more than symbolic measures with no real teeth.

One of the best ways to deal with all this is through greater transparency. At the international level, efforts to come up with survey data and indices provide a useful reference for highlighting the most egregious cases of pervasive corruption but do little to highlight corruption that is specifically linked to trafficking or organized crime. This gap is filled in liberal democracies by investigative reporting. Yet in some countries, journalism remains an extremely high risk activity. Investigative journalists who unearth information on organized crime, trafficking or crime-corruption linkages risk their lives – and many have been intimidated, beaten, or killed either during their investigations or immediately after their revelations were published. A sustained and long-term effort and investment is required by the international community and the United Nations to deal with this problem. The new UN Convention against Corruption provide an excellent basis and framework for such efforts.

(viii) Enhance national and international cooperation

Another key component of this strategy is coordination and cooperation (1) at the national level among different government agencies in the intelligence and law enforcement communities (2) among multiple governments affected, in one way or another, by trafficking, (3) among international organizations and agencies that have some responsibility either for combating one or more forms of trafficking or for mitigating the consequences of trafficking (4) between governments, international organizations, and the relevant NGOs which not only provide major contributions to understanding the dimensions of trafficking but also focus attention on the problem, thereby helping to create awareness and set the political agenda; (5) and between governments and the private sector to ensure that wittingly or unwittingly businesses do not provide assistance to the trafficking process. Cooperation is required at all levels from government sharing of information about potential infiltration of particular industries to efforts, especially by firms in industries that are particularly important or useful to the trafficking process, to police themselves in some way. Another way of seeing this is in terms of the creation of anti-trafficking networks, a development that meets the principle enunciated by John Arquilla and David Ronfeldt that it takes a network to defeat a network. In some cases, these networks of trust among law enforcement and intelligence personnel in different countries, usefully extended to corporate security officers and experts from the NGO world, will be maintained for the long haul; in others they will be created for specific missions against specific targets. The temporary network of the multi-national task force is extremely valuable and can yield excellent short term results in specific investigations or against specific targets. The longer term transnational network of officials from various countries who have developed mutual trust and respect and can operate together informally is even more valuable, especially where it extends beyond two or three countries and beyond governments to the private and non-

profit sectors. However large or small, formal or informal, restricted or open, these networks are essential to combating trafficking networks and activities.

(ix) Assist the business community in reducing the harmful effects of trafficking

In considering the issue of government assistance to the business community, it is important to acknowledge at the outset that not all businesses want to be assisted. As suggested in the discussion of the myths that exist in this domain, trafficking is not invariably nor uniformly harmful. For some businesses, trafficking activities might be beneficial in terms of request for services, generation of entrepreneurial opportunities, and flow of profits. The issue for these particular companies is not assistance to protect them, but enforcement either to put them out of business or to ensure compliance with the laws.

For companies that are not overtly criminal, there are several ways in which they might be harmed by trafficking: direct but inadvertent involvement in trafficking activities (such as the diversion of a legitimate arms shipment to a prohibited country), the takeover or co-option of the company by criminals (in which case the legitimate owners are either forced out or compelled to connive in criminal activities); the inadvertent employment of criminals in the company (sometimes leading to takeover); the use of the company for specific criminal undertakings such as money laundering (putting the company at risk in terms of both reputation and financial stability); and deals with other companies that are criminal in nature but appear to be legitimate (again making the legitimate companies vulnerable to criminal pressure or law enforcement action). In all cases, their lack of knowledge can put companies in harm's way.

In order to protect the business community from the harmful effects of trafficking, governments need to think not in terms of enforcement so much as prevention. Preventive measures can be understood largely in terms of target hardening – making it more difficult for organized crime to infiltrate the industry or particular firms within it. This might require careful regulations that allow competitive bidding but also prescribe certain standards that must be met. In this connection, some business associations have already developed voluntary codes of conduct or industry standards that they expect their members to respect and meet. Yet it might be useful to formalize this process, incorporating penalties for non-compliance.

Perhaps the most valuable way in which governments and law enforcement agencies can assist firms or even industries is by sharing knowledge of suspicious individuals, organizations or companies. Advisories about the dangers of doing business with such companies could become routine, just as in the United States the Financial Crimes Enforcement Network and the Federal Reserve Bank provide warnings about dubious banks and financial jurisdictions. There is a useful precedent here from the oil industry where, during the 1990s, the major companies established an information-sharing mechanism designed to assist due diligence about potential partners and an early warning system of individuals and companies they should keep out of the industry. In this process, they worked closely with law enforcement agencies which helped identify potential threats.

Such public-private partnerships to combat trafficking require that governments and law enforcement agencies share information that has typically been seen as confidential or sensitive. If the emphasis is on preventive strategies, rather than simply reacting after crimes have been committed, however, such reservations need to be overcome. Information about potential problems is one of the biggest resources that governments can provide. The

difficulty is ensuring that the information remains confidential and does not get leaked to the criminals (something that is often the result of organized crime related corruption whether in government or the private sector). Nevertheless, in many cases this will be a risk worth taking as it allows firms to protect themselves more effectively against infiltration or potential takeover.

A variant of this approach – but one that can be valuable for law enforcement investigations and enforcement – is where the industry provides information to government. This occurs predominantly in the financial sector where banks and increasingly non-bank financial institutions have been compelled to man the first line of defense against money laundering. Similarly, the British Customs Service and others have developed memoranda of understanding with the freight forwarding industry in which Customs helps to expedite inspection and delivery in return for information from the industry about any suspicious activities or people. In effect, this too can be seen as a preventive measure as it allows law enforcement to respond quickly to developments that could endanger the industry. It also highlights the principle of reciprocity as the basis for partnership.

(x) Move from reaction to anticipation

The final component of the anti-trafficking strategy being enunciated here encapsulates this requirement for what might be termed agile law enforcement - measures that are forward looking and pro-active combined with the maintenance of a capacity for adaptability and flexibility. In effect, law enforcement and traffickers are in an adversarial relationship that, like other adversarial relationships, is in large part a battle of wits. In these circumstances, it is essential for governments to develop a capacity for strategic anticipation that not only allows them to pre-empt certain trafficking activities, but also to respond rapidly to adjustments or innovations made by the traffickers after they have encountered setbacks. In effect, any anti-trafficking strategy must incorporate possible responses by traffickers to successful law enforcement. From the law enforcement perspective, the process is one of displacement; from the trafficking perspective, it is one of adaptability. Whichever way the process is characterized, however, some degree of planning is required to ensure that the traffickers remain on the defensive and are not always one step ahead.

Conclusions

As suggested above, a comprehensive anti-trafficking strategy needs to go beyond the trafficking process itself and encompass measures that deal with the corruption that facilitates trafficking and the laundering of the proceeds of trafficking. This will not be easy but a focus on sectors of business such as import-export companies that are linked to trafficking could prove highly beneficial in terms of going after money laundering, while particular attention also needs to be paid to police, border guards, and customs agencies whose connivance can greatly facilitate the trafficking in drugs, arms, or persons. At the same time, it is necessary to deal with some of the underlying problems that fuel trafficking. These include conflicts that generate a demand for arms that are paid for with diamonds and other natural resources, poor economic performance that limits opportunities available to people in their home countries, and a demand for drugs that can result from surplus income for recreation on the one side and the desire to escape conditions of poverty and despair on the other. There are no easy and simple solutions to these problems or to the trafficking in arms, persons and drugs. The comprehensive strategy outlined here is no exception. It is

presented with a clear recognition that it needs considerable modification and refinement, but that it could be a stimulus for discussion and provide a broad framework for an action plan. Even if a comprehensive strategy of this kind is adopted, however, it is certainly no guarantee of success. The only certainty would be that without such a strategy continued failure in combating trafficking may be inevitable.

References

Arquilla, John, and David Ronfeldt, (eds.) *Networks and Netwars* (Santa Monica: RAND, 2001)

Bristow, Edward J., *Prostitution and Prejudice: The Jewish Fight against White Slavery 1870-1939* (New York: Schocken Books, 1983)

Godson, Roy, "The Political-Criminal Nexus and Global Security." *The Asia Times*, 19 June 2002.

Holloway, Robert, "Air Transport a Little-Known Key to Arms Smuggling" *Agence France Presse* 27 March 2001

Naim, Moises, "The Five Wars of Globalization" *Foreign Policy*

Rosenau, James N., *Turbulence in World Politics* (Princeton N.J.: Princeton University Press, 1989)

Savona, Ernesto, (and Phil Williams) (eds) The United Nations and Transnational Crime (London: Cass, 1996)

Silverstein, Ken, "Comrades in arms: meet the former Soviet mobsters who sell terrorists their guns" *Washington Monthly*, Jan-Feb 2002 p19 (7)

The Economist "Small Arms Big Damage" 13 July 2001

Wolosky, Lee quoted in "The Merchant of Death" *Africa News Service*, 21 November 2002

Williams, Phil "Transnational Criminal Networks in John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001)

Winer, Jonathan, "How to Clean Up Dirty Money" *Financial Times,* 22 March 2002.

Printed by
WELTKOPIE S.a.S. - Milan - Italy
on behalf of
Centro nazionale di prevenzione e difesa sociale / CNPDS
Piazza Castello, 3 – 20121 Milano
April 2004