I. Globalization and new technologies: challenges to drug law enforcement in the twenty-first century

1. Globalization and new communication technologies have brought innumerable benefits to our society. These benefits have been economic, educational and cultural and have bridged gaps that seemed insuperable only 10 years ago. Since the end of the cold war, restrictions on international commerce and finance have fallen away and deregulation and liberalization have boosted global trade, while the collapse of communism in the former East bloc has stimulated the growth of new, free-market economies and the intense cross-border movement of people, goods and capital. The number of Internet users around the world virtually doubles every six months and is expected to reach 700 million by the end of 2001. The information technology industry has become a global wealth generator in which developed and developing countries alike have a major stake.

2. The assimilation of national economies into a single global system, dominated by the performance of stock exchanges and capital markets, extends beyond economics to the roots of cultural and social identity. The fall of ideological barriers has been accompanied on the one hand by economic homogenization and on the other by political and social fragmentation. In many parts of the world, areas of economic prosperity coexist with pockets of worsening marginalization and poverty, while, especially in developing countries, traditional bonds of social cohesion have been weakened by the rapid pace of change. These disparities are exploited by drug dealers and traffickers in their attempts to develop new markets. Moreover, in the course of the last decade, the growth in trade and financial activity has provided criminals with greater possibilities for concealing the illicit transfer of goods such as internationally controlled drugs and precursor chemicals and for disguising the proceeds therefrom. Thus, technological change and the globalization of trade and finance have provided opportunities not only for social advancement, but also for new and traditional forms of drug-related crime.

3. The International Narcotics Control Board has decided to address the theme of globalization and new technologies in the present report not in a spirit of rejection, but because of the danger that the beneficial effects of these phenomena on society are being undermined by individuals and criminal groups for illicit gain. In particular, they pose new challenges to the mandates of the three international drug control treaties. The Board, as the guardian of the treaties, has a responsibility to alert Governments and the public at large to these challenges.

4. The Board has been concerned for some time over the misuse of new technologies in the field of internationally controlled drugs. In the report of the Board for 1997,[1] attention was drawn to the fact that, in violation of article 3 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988,[2] information disseminated through electronic and other media appeared to be offering invitations or inducements to take drugs. In its reports for 1997[3] and 1998,[4] the Board noted that the Internet was providing a forum for the exchange of information and advice on illicit drug use and manufacture. In its report for 2000,[5] the Board expressed concern over the unregulated growth of Internet pharmacies that promote and offer for sale controlled substances without prescription. Such practices violate article 10 of the Convention on Psychotropic Substances of 1971,[6] which requires parties to that convention, with due regard to their constitutional provisions, to prohibit the advertisement of psychotropic substances to the general public.

A. Impact of globalization and new technologies on drug-related crime and criminal organizations

Cyber crime: a definition

5. The term “cyber crime” covers many types of activities but essentially can be used to describe violations of law that are committed and/or facilitated through the use of electronic media.[7] In comparison with ordinary crime, cyber crime requires few resources relative to the damage that can be caused, it can be committed in a jurisdiction without the offender being physically present in it and, in many countries, offences are inadequately defined or not defined at all;

hence, personal risk and the likelihood of detection are low.

Impact on drug-related organized crime

6. Organized crime has its own operative code, which flouts the rule of law and depends upon violence for its enforcement. It has, however, adopted some of the business practices that characterize the legitimate economy. Organized criminality has become more transnational and has been restructured and decentralized; in other words, it too has globalized.

7. The pyramid-shaped structure of the single organized criminal group has tended to make way for fluid networks of cell-type structures in which national identity is subordinate to function or skill, although nationality itself can be a function if it opens the door to a new market or permits the penetration or corruption of a particular institution. Transnational criminals do not respect borders in that, in carrying out their activities, they trail their activities across several jurisdictions to minimize law enforcement risks and maximize profit; thus, no single State can presume that a particular criminal activity falls entirely under its jurisdiction.

8. The network is the organizational form that characterizes globalization in both the licit and illicit spheres. For a drug trafficking organization, the network structure has distinct advantages over the traditional hierarchy: it has a well-protected, dense core of organizations or people connected to a looser periphery by a multiplicity of links, which makes it more capable of evading law enforcement efforts.

9. Drug trafficking groups utilize new technologies in two distinct ways: to improve the efficiency of product delivery and distribution through the medium of secure, instant communications; and to protect themselves and their illicit operations from investigation by drug law enforcement agencies, sometimes using techniques of counter-attack. New technologies enable drug trafficking groups to commit traditional crimes with new methods—for example, to conceal information about the shipment of illicit drug consignments by means of encrypted messages or to launder drug-related funds by electronic transfer—and to commit new offences with new means, for example, by using information warfare or digital attack against intelligence activities of drug law enforcement agencies.

10. Drug traffickers use computers and electronic pocket organizers for storing information (such as bank account numbers, contact details of associates, databases of assets and financial activity, sales and other business records, grid coordinates of clandestine landing strips and recipes for synthetic drug manufacture) and for electronic mail (e-mail) and other correspondence.[8] Surrogates receive instructions by telephone, fax, pager or computer on where to deliver warehouse loads, whom to contact for transportation services and where to send the profits. Greater protection derives from the use of prepaid telephone cards, broadband radio frequencies, restricted-access Internet chat rooms, encryption, satellite telephony and "cloned" cellular telephones (so called when the identity codes assigned to legitimate customers are intercepted and programmed into cellular telephones used by criminals).[9] Members of drug trafficking organizations can program their computers to detect attempted intrusion and to use "back-hacking" techniques in order to damage the investigating source. Such techniques are of particular value to the organizers of drug trafficking activities, who rarely need to leave the protection of their home base in order to organize or supervise their operations.

11. Narcotics police in the Hong Kong Special Administrative Region of China report that detecting the laundering of drug-related funds has become more difficult with the advance of electronic commerce and Internet banking facilities. Drug traffickers communicate with each other mainly by using mobile telephones with prepaid cards that can be bought anonymously. China has also reported a case in which criminals tried to avoid detection by penetrating the customs database to alter the details and status of a commercial freight consignment, a case that undoubtedly has implications for drug trafficking.

12. In Australia, drug traffickers use a facility offered to all clients by worldwide courier services to track their shipments on the company's web site. A delay may indicate to the traffickers that a controlled delivery operation has been set in motion. Drug law enforcement authorities involved in such operations must therefore act within an extremely narrow time limit in order to avoid suspicion.

13. The Inter-American Drug Abuse Control Commission (CICAD) of the Organization of American States (OAS) noted in its *Hemispheric*

Report 1999-2000[10] that the Internet had become the most widely used medium for expanding the production of synthetic drugs in some countries and that globalization, instant communication and electronic fund transfers had been utilized by organized criminal groups to improve the efficiency of drug trafficking activities.

14. Drug law enforcement authorities in the Czech Republic report that nowadays illicit drug sales and purchases are agreed online at Internet cafes or through the use of cellular telephones. Because illicit drug deals are arranged instantaneously and over short distances, interception by drug law enforcement authorities is much more difficult.

15. Since 1996, companies based in the Netherlands have been using the Internet to sell cannabis seeds and derivatives. According to the International Criminal Police Organization (Interpol), at the beginning of the year 2000 authorities in the United Kingdom of Great Britain and Northern Ireland identified over 1,000 web sites worldwide offering to sell illicit drugs, mostly cannabis but also methylenedioxymethamphetamine (MDMA, commonly known as Ecstasy), cocaine and heroin, in direct violation of the international drug control treaties. The Netherlands and Switzerland had the highest number of such web sites.

16. Law enforcement agencies in the United States of America attribute the rapid increase in seizures of laboratories used for the illicit manufacture of methamphetamine to the evolution of technology and the increased use of the Internet. In the past, drug recipes were closely guarded secrets but, with modern computer technology and chemists' increasing willingness to share their knowledge, this information is now available to anyone with computer access. It does not require a college-educated chemist to produce amphetamine: less than 10 per cent of suspects arrested for illicitly manufacturing methamphetamine are trained chemists, a fact that explains the many fires, explosions and injuries in clandestine laboratories.[11]

17. A drug investigation carried out jointly by Colombian and United States authorities led to the arrest of 31 drug traffickers in October 1999. It was found that the traffickers had kept in touch with each other by using Internet chat rooms protected by firewalls to make them impenetrable. The details of each day's trafficking activities had been fed into a computer located on a ship off the coast of Mexico, ensuring that even if other computers had been penetrated it would have been impossible to bring down the whole network. The same group had used encryption that law enforcement authorities had been unable to break in time to act on the information. Those methods, in addition to "cloned" cellular telephones, had enabled the traffickers to move hundreds of tons of cocaine during a period of several years before being detected.[12]

18. Colombian and Mexican drug cartels have used sophisticated equipment for the surveillance of investigating officers and interception of their communications, collecting photographs of the officers and other personal information. This has also occurred in Europe. In 1995, a drug trafficking group in the Netherlands hired computer specialists to carry out hacking operations and to encrypt their communications. Encryption software installed on palmtop computers enabled the traffickers to create a secure database on unmarked police and intelligence vehicles. A laptop computer and disks belonging to the investigating authorities were stolen and the resultant information was used to intercept communications between police officers, who were subsequently observed and threatened.

Impact on drug abuse

19. The spiralling growth in the sale of prescription drugs over the Internet represents a serious challenge to drug safety regulators and law enforcement agencies. According to an oversight committee convened by the United States Congress, between 1998 and 1999 the number of pharmaceutical seizures made in the United States rose by 450 per cent—an increase of 7,586 seizures. That trend was attributed largely to Internet purchases. In the first five months of 2000, some 30 investigations into online pharmaceutical sales were opened.[13]

20. In the past, the Board has drawn attention to evidence that the Internet is being used as a vehicle for the exchange of messages and information favouring drug abuse, particularly among young people.[14] A simple surfing operation on the Internet lasting a matter of minutes may yield detailed instructions for manufacturing a wide range of synthetic drugs, reviews of books on how to obtain internationally controlled precursor chemicals and to operate illicit drug

laboratories, and invitations to buy a wide range of books containing drug recipes.

21. The likely consequences of these developments are, in the Board's view, alarming. One is the potential expansion of drug abuse as a result of the incitement to produce and consume drugs within a large "club" whose members encourage and assist one another. Another is the "amateurization" of drug-related crime: prospective drug chemists or consumers do not need to have special contacts or resources or to live in an area where drugs are available; a search engine enables the Internet user to contact like-minded individuals in different parts of the world and to locate supply sources of which the user would otherwise have been ignorant. Young people may be drawn into drug-related crime by misinformation, propaganda or brainwashing on the part of unseen individuals whose aim is to profit from a broader drug-consuming population. When the approach is "virtual", the warning signals that might deter or frighten a young person in the real world are minimized, and the filtering process by which an individual moves into physical contact with a criminal organization disappears. In psychological terms, "virtuality" could be described as a facilitating factor in the commission of crime.

Impact on money-laundering

22. The Board is aware that the deregulation of capital markets and the virtual elimination of exchange controls have led to lower costs and a greater range of choice for bank clients and, therefore, to significant advantages for large sectors of society; however, the Board is concerned that the increasing recourse to electronic means of financial transfer, together with a massive growth in the volume and speed of monetary flows, may lead to a reduced capability for detecting worldwide movements of illicit capital and therefore to increased drug-related money-laundering.

23. The Financial Action Task Force on Money Laundering has warned that there are three characteristics of Internet use that could aggravate certain "conventional" money-laundering risks: ease of access; the depersonalization of contact between customer and institution; and the rapidity of electronic transactions.[15] The globalization of financial markets could be considered an additional risk factor.

24. While cash may still be the most common form of currency for drug deals at the local level, the creation of new global markets in stocks, bonds, futures, currency and derivatives has enlarged the potential field of operations for moving large sums electronically around the world with speed, ease and secrecy—ideal attributes for launderers of illicit drug funds. The use of smart cards and online banking has reduced face-to-face contact between bank staff and clients and, as a result, the efficiency of mechanisms for verifying the legitimacy of financial activities.

25. Casinos have long been used as an outlet for laundering drug-related funds and other funds of illicit origin; thus, the extension of this activity through the Internet is a logical step. Whereas many onshore gaming establishments follow regulations against money-laundering, "virtual casinos" flourish in a completely unregulated environment. In March 2001, a gambling enthusiasts' site listed 12,000 web links, including 2,045 "virtual casinos".

26. In recent years, the financial services industry has become increasingly competitive, a trend that has discouraged many banks from pursuing due diligence enquiries lest their customers' funds be deposited with rival institutions. In an increasingly competitive market, financial institutions may see compliance with legislation against money-laundering as being antithetical to good business and assign low priority, few resources and low-calibre personnel to it. Furthermore, in most countries, almost all suspicious transaction disclosures relate to cash transactions. In increasingly "cashless" societies, this suggests that measures against money-laundering, even if followed, have not kept pace with technological change.

B. Impact of globalization and new technologies on government structures and capabilities designed to combat drug-related crime

27. Government structures, in particular judicial and law enforcement agencies set up to tackle drug-related crime, have long been faced with the problems of pursuing transnational crime within well-defined limits of territorial jurisdiction and sovereignty. Since the ratification of the 1988 Convention, many obstacles have been overcome by means of bilateral and multilateral agreements and mutual legal assistance treaties. However, the Board is concerned that the consolidation of international cooperation against

drug-related crime may be threatened by the adoption of techniques that enable organizations engaged in illicit drug trafficking and production to avoid identification and prosecution. There is no doubt that the rapidity with which criminals have taken advantage of new technologies has not been met by equal progress within the ranks of law enforcement.

28. The challenges to drug law enforcement may be divided into four types: structural and "mindset" challenges; legal challenges; technical and resource challenges; and issues involving privacy and freedom of expression.

Structural and "mindset" challenges

29. At the end of the cold war, law enforcement and intelligence organizations were obliged to undertake structural reforms and a review of priorities that have not yet been fully implemented. Today, combating drug-related crime at the transnational level requires another leap forward; it involves not only a structural approach, but also a "mindset" or overall approach. Law enforcement has traditionally taken the form of structured hierarchies with clear geographical demarcation lines. Transnational drug-related crime challenges this approach, partly because of its cross-jurisdictional operations and partly because of the low-profile network structure that now predominates.

30. The liberalization of the telecommunications sector has had unwanted repercussions for the investigation of crime, leaving Governments to deal with the challenge of trying to disrupt illicit usage without interfering with the now economically indispensable advantages of licit usage. Traditional police and investigative strategies are hampered by the absence of a conceptual and of a practical cooperative framework within which high-tech crime can be tackled. It is still a nebulous field in which crimes are ill-defined and perpetrators and their location are hard to identify.

31. To meet these challenges, drug law enforcement will have to develop new forms of cooperation, new strategies and new professional skills, all of which have significant resource implications. Drug law enforcement agencies must set up operational and functional networks at the global level if they are to succeed in disrupting drug trafficking organizations effectively. They will also have to develop intelligence and operational relations with other law enforcement agencies to avoid duplicating efforts and wasting resources. While a start has been made, the gap between criminal and investigative capacities is still all too evident.

Legal challenges

32. The most obvious legislative deficiency with which drug law enforcement has to deal is the absence of comprehensive legislation relating to offences committed in an electronic environment. Some countries have none at all, some have adopted measures that have been integrated awkwardly into existing legislation, but relatively few have adequately updated their penal codes. Even after legislation is introduced at the national level, many problems will remain unless Governments at the same time address the transnational nature of high-tech crime, which may originate in one country and have consequences in a second while the evidence may be spread through many more. At present there are no guidelines concerning which country's laws should prevail in pursuing an offence, how court decisions can be enforced if defendants reside abroad and which protocols govern cross-border investigations.[16]

33. Two surveys have exposed the fact that many countries are not prepared to meet the challenge of high-tech crime. A management consultancy company surveyed 52 countries throughout the world for legislation against high-tech crime and found that 33 had not updated their laws at all, 9 had enacted partial legislation, judged incomplete, and 10 had adopted legislation enabling the prosecution of the most serious forms of cyber crime.[17] Of those that had updated their laws, some, such as the Philippines, had only done so in the wake of a high-profile event, the "ILOVEYOU" virus, which infected 80 per cent of United States government computers and caused damage estimated at US$ 10 billion. The perpetrator had been tracked down to a suburb of Manila but, as no law in the Philippines prohibited his activities at the time, he could not be held responsible for the damage inflicted nor could he be extradited to face prosecution in the United States.[18]

34. In western Europe, replies to a questionnaire on drug-related crime committed via the Internet showed that Governments had generally failed to introduce legislation against such crime, while any cooperation between law enforcement and Internet service providers was on a voluntary and informal basis. In

most countries, Internet service providers operated outside a specific legal framework and were subject to little or no supervision. The Internet had been used principally as a means of communication and of exchanging information on the illicit production and sale of drugs. Hardly any countries had recorded drug-related cases in which traffickers had communicated with one another by using the Internet, but some lacked sufficient information to assess the phenomenon. All but two countries had recorded the use of encryption by criminals in other fields. Almost all countries had a contact point for sharing information on crimes committed via the Internet, although the location varied between police, customs, telecommunications authorities and computer crime research units.

35. The tracing and seizure of evidence, as well as standards of evidence for admissibility in court, are key issues. The process of requesting and obtaining authorization for search warrants in multiple jurisdictions and the time involved to implement them—already problematic—may not be achievable in real time, allowing perpetrators to destroy or remove incriminating evidence, for example, of drug transactions. Other problems arise because of the nature of electronic data. Standards of procedure for obtaining authorization to search stored data (carried out with the knowledge of a suspect) and authorization to intercept data (a covert operation) will vary, the latter being subject to more rigorous controls. Yet electronic data such as e-mail messages constitute both stored data and data in transmission.[19] A review of legal norms in this area appears to be indispensable.

36. The admissibility in court of evidence of crime perpetrated electronically is particularly difficult, since electronic data can be modified without leaving a trace. Law enforcement will have to develop transparent and secure procedures that enable authenticity to be proven when electronic data have been transcribed onto hard copy. If the process involves decryption, extra skill and care will be required to ensure that prosecuting authorities are not open to charges of evidence tampering. Moreover, establishing authenticity of content and source is difficult without revealing in public court (and therefore to criminals) the technologies and methods used to read the content.

Technical and resource challenges

37. The technical and resource challenges to law enforcement in tackling drug-related high-tech crime are formidable. Keeping up with technology implies constantly updating equipment and manpower, as well as maintaining a "24/7" contact network (operating 24 hours a day, 7 days a week) to ensure real-time investigation. For many developing countries, this may represent a major burden and may cause the gap between criminal and investigative capacities to widen. Some of these countries may become "data havens", where criminals locate their service providers and store their most sensitive data and where encrypted data are out of the reach of law enforcement agencies. Nations that do not equip their law enforcement agencies adequately or that have low standards of electronic security may be bypassed by electronic commerce companies, thus becoming economically disadvantaged, or they may run the risk of having their electronic messages blocked by the rest of the network.[20] Even developed countries suffer from a shortage of skilled investigators and prosecutors with the appropriate expertise, since salaries within the public sector are invariably lower than those offered by private industry.

Encryption

38. Encryption may be seen by law enforcement agencies as both a blessing and a bane. It facilitates electronic commerce under relatively secure conditions, ensures privacy and, together with the use of digital signature, helps to prevent unauthorized access to information systems; it also provides drug law enforcement agencies with a valuable tool for communications and for protecting sources and data. To many law enforcement agencies, however, it appears that the advantages that encryption offers to them are outweighed by the protection it offers to criminals.

39. Without the capacity to intercept and understand communications, drug law enforcement is severely handicapped in terms of prevention, detection and prosecution. As early as 1994, it was reported that every major investigation by the Federal Bureau of Investigation of organized crime in the United States had relied on electronic surveillance.[21] In the United Kingdom in 1996 and 1997, the interception of communications played a part—often a crucial part—in operations leading to 1,200 arrests, the seizure of

115 tons of drugs and the seizure of over 450 firearms.[22]

Issues involving privacy and freedom of expression

40. In all democracies, the requirement for law enforcement to investigate the private lives of suspects in order to prevent or detect crime must be balanced against respect for private property and communications. As legislation develops in the field of cyber crime, this reconciliation is proving to be elusive, all the more so since the views of a powerful industry must be heard alongside those of citizens' groups and of law enforcement. Finding a solution represents another major challenge for the fight against drug-related crime. Recent legislative developments concerning data storage have been in the direction of greater protection of individual privacy and of personal data, such that Internet service providers generally may not store customer information for longer than is necessary for billing purposes. To require them to keep client log records for criminal investigative purposes is a delicate matter—in terms of both privacy and cost implications—that is of concern to industry and civil liberty groups alike.

41. The use of the Internet for the exchange of drug "recipes" and for sending messages favouring illicit drug use poses law enforcement problems of a different kind: on the one hand, public incitement to produce or consume drugs violates article 3 of the 1988 Convention; on the other hand, many States consider freedom of expression to be an inalienable right and reject any censorship of communications. The unauthorized offering for sale of narcotic drugs, psychotropic substances or precursor chemicals should be a prosecutable offence in the jurisdiction of any State that is a party to the international drug control treaties. The offering of advice on how to obtain drugs or precursor chemicals for illicit purposes should also be considered inducement or incitement, in violation of article 3 of the 1988 Convention. However, a web site that, for example, discusses legalization of the non-medical use of narcotic drugs does not necessarily fall under this category, and to ban such sites might conflict with the principle of freedom of speech in many countries.

42. The one area of content-related crime via the Internet in which progress has been made is the fight against child pornography, but this has been achieved only because the activities concerned arouse universal condemnation and because mere possession of such images constitutes a crime in many countries. In such cases Internet service providers are legally liable if it can be shown that they were aware that they were providing access to web sites containing child pornography. Offences relating to child pornography are the only content-related criminal acts specified in the Council of Europe's Convention on Cybercrime[23] (see paragraph 65 below).

C. Future challenges

43. On the basis of the foregoing analysis and in the light of recent world events, the Board is of the view that the following developments may occur if action is not taken at the national and international levels:

(a) *Opportunities for all forms of crime may increase* as online communications, finance and commerce expand. The growth and interdependence of national economies will make it easier for criminal organizations to blend their operations into legitimate economic activity;

(b) *Transnational crime may increase* as networks make cross-border crimes easier to commit;

(c) *Organized crime may continue to exploit technological advances for offensive and defensive purposes*. The "IT warrior" will become an indispensable component of organized criminal groups;

(d) *Electronic money-laundering may increase* with the growth of online financial service companies, especially if measures against money-laundering remain a low priority and if offshore companies continue to offer anonymity and protection from investigation. Underground banking systems will also enjoy greater security through the use of information technology;

(e) *Drug-related crime may expand*; such crime will be committed by a larger number of people, many of whom will not be members of organized criminal groups, nor will they fit to any criminal profile;

(f) *Minors may increasingly commit crimes involving information technology* as new generations achieve computer literacy at an earlier age;

(g) *Criminal organizations may exploit scientific developments in order to invest more heavily in the production of synthetic drugs* for the illicit market;

(h) *Law enforcement may have less capacity to conduct interception and surveillance activities* as drug trafficking organizations increasingly adopt encryption and other means of concealment;

(i) *Jurisdictions without adequate laws against crime involving information technology may become sanctuaries*;

(j) *Traditional frameworks for extradition and mutual legal assistance may be stretched to their limits*.

D. How the challenges are being addressed

New approaches to high-technology crime within and between law enforcement structures

44. The national police forces of several countries, including Canada, the United Kingdom and the United States, have established dedicated cyber-crime units. The Hong Kong Special Administrative Region of China has enhanced its intelligence and enforcement capabilities at the international level and has set up a technology crime division comprising 76 officers specially trained to handle domestic crime.

45. The Australian Federal Police has developed an online investigation management system known as the Police Realtime Online Management Information System (PROMIS). Australian Federal Police liaison offices around the world use the system to exchange data, photographs and other information on investigations with colleagues in real time.

46. In Spain, the central investigation unit on information technology crimes and the department for high-technology crimes of the Ministry of the Interior are actively involved in preventing the use of the Internet for illicit advertising of controlled substances, including psychotropic substances. The national plan on drugs for the period 2004-2008 includes the establishment of an observation body on the use of new technologies by drug trafficking organizations, including the use of the Internet.

The use of advanced technologies to fight drug-related crime

47. Since 1997, when the Board first drew the attention of Governments to the fact that the electronic media was being used for sending messages favouring illicit drug use,[24] many health authorities have used the Internet as a quick and inexpensive means of disseminating factual information on drugs and their abuse.

48. In the United States, the Counterdrug Technology Assessment Center of the Office of National Drug Control Policy supports scientific and technological research and development for the benefit of drug law enforcement agencies. New procedures have been developed for analysing the effects of drugs on human beings and for detecting the presence of drugs concealed in or about the body, in containers, conveyances or other closed spaces. Non-intrusive inspection tools currently available to customs and cargo inspection authorities include improved X-ray and gamma-ray detector technology, the portable/transportable capability to detect drugs in vessels, compartments and containers of all sizes during inspections at sea and in ports and rapid and non-invasive screening of individuals and their luggage.

49. Specialized computer forensic programs permit the application of computer technology and techniques for handling seizures and evidence to retrieve information from computer systems for investigative or intelligence purposes. Software programs can screen data streams for key words or phrases, or "sniff" out portions of electronic communications that match a defined filter set programmed in conformity with a court order, such as messages transmitted to or from a particular account or user.[25] Integrity features upgrade the programs by imprinting the collection mode used on the evidence, demonstrating that no alteration has been made to the filter settings employed or to the information obtained. Such features strengthen proof of "chain of custody" authenticity and non-alteration.[26]

50. Other advances in the innovative use of existing technology include the creation of advanced computer models for the online identification of anomalies within financial transactions, software for high-speed computers that can verify the identity of drug traffickers through their fingerprints, and the setting up of networks that allow competent authorities to

cross-reference the registration of property ownership with other data such as income tax returns. In this way the apparent advantage that criminals have from the use of high-tech tools can be turned into an advantage for law enforcement.

Developments in the private sector

51. The private sector has begun to forge alliances with law enforcement to develop better response and protection facilities against high-tech crime. Internet service providers have set up international networks of cooperation with law enforcement through so-called hotline associations that cooperate to combat the use of child pornography through the Internet. If material considered child pornography is identified, the hotline identifies the location and, if based locally, notifies the police and/or the Internet service provider to remove the material using clearly defined notice and takedown procedures.[27] Many countries operate national systems on a similar basis.

52. In the United States, collaboration between the private sector and the public sector enables law enforcement to share information about cyber intrusions, exploited vulnerabilities and other threats with owners or operators of vital infrastructure such as power generation facilities.

Content regulation

53. Various means exist by which Internet access, and therefore content control, can be regulated. Web sites can be blocked altogether by means of censorship, as occurs in countries where the Government controls Internet access. Elsewhere, either Internet service providers or web site administrators can be held criminally liable if they knowingly distribute material that is considered illegal or harmful under any of the laws of the host country, including the drug laws. Internet service providers may regulate the content of the web sites that they host by introducing voluntary codes of practice, as in Italy or Japan, or by drawing up legally binding agreements between service provider and web site administrators that specify jurisdiction and venue for redress. A Canadian Internet service provider uses service contracts with users and web sites to establish online terms and conditions; Canadian laws are applied to web site content, and users are notified of this policy.

54. Individual users may exercise choice over Internet content by means of commercially available software programs that block or filter undesired content according to specified criteria. A wide range of such programs has been developed, some of which incorporate rating systems and complaint-registering processes. A software company in the United States filters Internet content according to a proprietary list of sites that is constantly updated: it has drawn up a blacklist of more than 60,000 sites deemed inappropriate for various reasons, including the encouragement of illicit drug use.

International and regional initiatives against high-technology crime

55. Drug-related high-tech crime is still a relatively new phenomenon, and few countries have any means of measuring its extent or impact—hence the lack of specific initiatives to counter it. However, international and regional organizations, such as the United Nations, the Group of Eight, Interpol and the Council of Europe, have begun serious efforts to address high-tech crime in general.[28] Those initiatives offer a working model from which efforts aimed at drug-related high-tech crime can be designed.

56. Since 1990, the Commission on Crime Prevention and Criminal Justice has been active in promoting international efforts to develop a comprehensive framework of guidelines and standards to assist States in dealing with computer-related crime. Those efforts include the publication in 1994 of a manual on the prevention and control of computer-related crime,[29] which contains proposals for the harmonization of both substantive and procedural law and urges international cooperation in that area. Expert group meetings were held under the auspices of the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders in preparation for the workshop on crimes related to the computer network that was held in Vienna on 15 April 2000 within the framework of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.[30]

57. Pursuant to Economic and Social Council resolution 1999/23, the Secretary-General conducted a study on effective measures to prevent and control high-technology and computer-related crime. In that report, several options were considered, such as the drafting of an international instrument against

computer-related crime and options for a shorter-term strategy including the establishment of a United Nations global programme against high-technology and computer-related crime.[31] In September 2001, the Commission on Crime Prevention and Criminal Justice adopted plans of action for the implementation of recommendations made by the Tenth Congress. The plan of action against high-technology and computer-related crime called for, inter alia, national actions: (a) to criminalize the misuse of information technologies; (b) to develop and implement rules and procedures to ensure that computer- and telecommunication-related crime could be detected and investigated; and (c) to ensure that law enforcement personnel were trained and equipped to respond to requests for assistance in the tracing of communications.

58. Interpol hosted an international conference of computer crime in 1995 and has produced manuals for investigators of information technology crime with the aim of setting technical investigation standards. A central unit and four working groups on high-tech crime have been set up, representing Africa, the Americas, Asia and Europe; their primary function is to provide regional training and cooperation. The Interpol Drugs Sub-Directorate operates a secure web site, accessible by national bureaux, that brings to the attention of police forces seizures of new drugs, drug trafficking alerts and other warnings that benefit from real-time communication. The security of recent projects targeting drug trafficking has benefited from the use of encrypted communication between team members. Interpol also cooperates with the private sector to secure business and industry against "cyber attack".

59. In Lyon, France, in June 1996, the heads of State or Government of the Political Group of Eight endorsed the 40 recommendations of the Senior Experts Group on Transnational Organized Crime. In recommendation 16, States were urged to review their legislation to ensure that abuses of modern technology deserving of criminal sanctions were criminalized and that the appropriate technical and resource implications of that capability were adequately addressed. In January 1997, the Lyon Group was created to address that recommendation. At the Meeting of Justice and Interior Ministers of the Eight held in Washington, D.C., in December 1997, the participants agreed on the Principles and Action Plan to Combat High-Tech Crime, in which States were urged to adopt legislation to investigate and prosecute high-tech crime and to strengthen international regimes for extradition and mutual legal assistance. The participants agreed on the need for a common approach to dealing with problem of high-tech crime. The Action Plan also called for the establishment of internationally recognized standard-making bodies to provide the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.[32]

60. By early 2001, the law enforcement agencies of the members of the Group of Eight and of nine other States were in daily contact and were sharing information through a "24/7" network (operating 24 hours a day, 7 days a week), which had been used successfully to investigate cases involving serious high-tech crime. The Lyon Group also hosted an international computer crime training conference for law enforcement investigators from the members of the Group of Eight in November 1998. It has developed standard procedures on transborder access to stored computer data and expedited mutual legal administrative assistance, and work is in progress to develop methods for determining the source and destination of communications.[33]

61. In all regions of the world, mechanisms are being developed for studying high-tech crime and the appropriate responses to it, although the drug component is marginal in most cases. In some regions, the focus has been more on combating fraud, child pornography and hacking activities; in others, concerns relate primarily to money-laundering and economic crime. In the light of recent world events, particular attention is now being paid to the use of new technologies by terrorist networks.

62. The Government of Japan, through the National Police Agency, is financing an Internet-based contact network of 21 countries in Asia for the exchange of information on high-tech crime. Eight countries are already participating in the first phase of the initiative.

63. Recommendation 5 of the 30 recommendations for tackling organized crime adopted by the European Council in July 1997 called for a study on high-tech crime, which was completed in January 1998. At a special meeting of the European Council held in Tampere, Finland, in October 1999, the heads of State or Government of European Union members concluded

that high-tech crime should be included in the efforts to agree on common definitions and sanctions. As part of the European Union Action Plan to Combat Drugs (2000-2004), in early 2001 the Council of Ministers' working group on drug trafficking carried out an assessment of the threat posed by the use of the Internet for illicit ends in relation to drugs, as well as a review of existing legal provisions in member States. The first stage of that analysis was the sending of a questionnaire by the European Police Office (Europol) to member States (see paragraph 34 above). The European Commission will be considering how to improve the effectiveness of efforts against the illicit drug trade on the Internet, the importance of which was recognized in the European Union drug strategy for the period 2000-2004.

64. In January 1999, the European Parliament and the European Council adopted a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.[34]

65. The Council of Europe's Convention on Cybercrime represents the most advanced international collaboration to date in the area of high-tech crime. The Council's 43 member States, together with Canada, Japan and the United States (which have observer status) and South Africa, were all involved in the drafting process and will be able to sign the Convention. The Convention covers issues of jurisdiction, extradition, the interception of communications and the production and preservation of data. It lists acts that must be criminalized under domestic law, including illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud and aiding or abetting the commission of these crimes. It creates detailed machinery to effect international cooperation and coordination in investigation and prosecution. Parties to the Convention will be obliged to empower their national authorities to carry out computer searches and seize computer data, require data subjects to produce data under their control, and preserve or obtain the expeditious preservation of vulnerable data. The Convention will be applicable in drug-related cases as a tool of mutual legal assistance, for example when authorities seeking electronic evidence of drug traffickers' activities, their customers or their assets in another State will be able to request that State to conduct a search of databases used by suspected traffickers or the interception of their electronic communications such as e-mail. The Convention was to be formally adopted on 8 November 2001 and to be opened for signature on 23 November 2001.

66. Private industry and citizens' groups, however, have objected to some clauses of the Convention on Cybercrime. A consortium of information technology industry associations has protested that the Convention could impose burdensome data preservation requirements on Internet service providers, make them liable for third-party action and restrict legitimate activities on the Internet. Civil liberty groups have also registered concern about measures called for in the Convention that they consider to be invasive of privacy. Nonetheless, the Board is of the view that this type of legal instrument can contribute to efforts against drug trafficking and abuse.

E. Conclusions and recommendations

Conclusions

67. Advanced telecommunication technologies constitute the motor of today's globalized economy and, as such, cannot be held back from expansion and technological evolution, nor is it desirable that they should. It must be recognized, however, that globalization and new technologies have facilitated certain drug-related criminal operations, thereby placing an additional burden on law enforcement agencies. although collaboration between industry and law enforcement is often good, inevitably, the public and private agenda do not always coincide, since companies have a duty to protect the privacy of their customers and the profits of their shareholders.

68. The Board has noted the wide range of efforts under way to tackle the threat of cyber crime in general. Although current initiatives regarding cyber crime focus primarily on child pornography and economic crimes such as fraud, hacking and theft of intellectual property, there are indications that new technologies are increasingly being used in drug trafficking and illicit drug manufacturing operations. For that reason, the absence of drug-related provisions in existing legislation against cyber crime is a matter of concern. If the challenges to drug law enforcement are to be met, there must be a programme of action at the national and international levels, within the context of

ongoing initiatives against cyber crime, that will have as its objective the prevention of drug-related high-tech crime. Many developing countries will instinctively look to the United Nations and to the Board for technical and legislative guidance in this area.

69. With regard to the drug-related content of sites on the Internet, technology tools, law enforcement and education are necessary, especially as regards parental involvement and user empowerment. Given the problems of identifying and investigating the innumerable drug advocacy web sites, filtering and blocking software can be of significant value in countering the use of the Internet for disseminating messages favouring drug abuse and may represent a more practical and realistic option than recourse to criminal law.

70. It is essential that law enforcement agencies and other national institutions responsible for fighting drug-related crime be given the technical and legislative means to develop an appropriate response capacity. But this alone is not sufficient. The Board is convinced that the challenges to drug law enforcement can only be met through cooperative partnerships involving Governments, the information technology industry and citizens, whose separate interests must be recognized and reconciled. The concerns raised by civil liberty groups over the invasion of privacy and the potential to limit freedom of expression are genuine and must be heeded.

71. Within the framework of cooperation between government and industry, the involvement of industry is required to identify vulnerabilities, to assist law enforcement authorities in threat assessment and to help to resolve cases when they arise. At the same time, industry must appreciate that self-regulation and informal channels of cooperation with law enforcement may not always be adequate to address the threat. Recent world events have already had major repercussions in terms of the investigation and prosecution of criminal acts, but only time will tell what the full impact of these will be. At present it can only be stated that the need for law enforcement structures to modernize and to adapt to changing circumstances and new challenges has become more acute. New technologies should be seen not as an enemy in the fight against drug-related crime, but as potential tools in the prevention of illicit drug use, production, manufacture and trafficking. The Board, as the guardian of three international drug control treaties whose goals are the health and well-being of society, proposes the concept of "shared guardianship" of the information society as a contribution to its future prosperity and security.

Recommendations

72. The most urgent task facing Governments is to ensure that appropriate procedural and substantive laws are introduced at the national level to deal with crimes committed in an electronic environment. Aggravating factors could be introduced when offences are committed with the aim of illicit drug trafficking or when the offence is committed by a participant in an organized criminal group (as defined in the United Nations Convention against Transnational Organized Crime).[35] Measures should be harmonized as far as possible to ensure that offences, sanctions and standards of proof are similar in countries throughout the world, in order to prevent the growth of data havens. Assistance should be provided to developing countries considered at risk from such exploitation.

73. Drug law enforcement agencies and judicial authorities should be given appropriate resources and equipment to investigate, identify, apprehend and prosecute offenders who use new technologies in drug trafficking activities.

74. Specialized inter-agency high-tech drug units should be introduced at the national level. The system of "24/7" networks should be expanded to include more countries on the principle that "it takes networks to fight networks". These units should maintain cooperative arrangements with other agencies against cyber crime.

75. Drug law enforcement agencies should be provided with critical infrastructure protection to protect their information and intelligence databases from "cyber attack".

76. Funding should be made available to provide equipment and training at appropriate levels in forensic techniques and in technological skills for policy makers and law enforcement and investigative personnel. Governments should find ways of attracting high-calibre technology specialists to work within drug law enforcement agencies.

77. Work should proceed to enable the Convention on Cybercrime to be ratified as soon as possible, and

support should be given to other initiatives in this field elsewhere in the world.

78. Governments should require online pharmacies to be licensed wherever they operate or deliver prescription drugs and should set up a system of oversight for such activities. The online sale of narcotic drugs and psychotropic drugs should be prohibited altogether, since it circumvents the existing national and international control system.

79. Governments should help to raise public awareness, especially among parents and teachers, of the fact that young people using the Internet may be exposed to messages favouring drug abuse and that the technological means to block or filter such messages are available.

80. Governments should support the establishment of web sites that provide attractively presented, unbiased information on illicit drug use—for example, explaining the laws governing illicit drug possession, use and trafficking for a given country and giving a description of drugs and their effects.

81. Consideration might be given to the development of a United Nations convention against cyber crime. Such a convention would provide a global classification and definition for high-tech and computer-related crime and a framework for legislative harmonization and international cooperation in the investigation and prosecution of cross-border crime committed or facilitated by electronic means. It could also include a section on drug-related crime, with a reminder to Governments that any form of advertisement for narcotic drugs or psychotropic substances must be prohibited. The convention would have to balance concerns of security and protection from crime with concerns for civil liberties, dignity and privacy.

82. Internet service providers should extend the practice of setting up hotlines to which the general public can report offensive or illegal content of sites on the Internet and should be aware that the drug-related content of some web sites may be in conflict with the international drug control treaties.

83. Financial institutions should review their measures against money-laundering in the light of technological developments.