CONTENTS

PREFACE

OPENING SESSION

Welcome Address
by Guido ROSSI

Keynote Address
by Antonio M. COSTA

1. THE IMPACT OF TECHNOLOGY ON CRIME

Introduction
by Ernesto U. SAVONA

Cyber-crime: typologies and likely future trends*:*
by Chris PAINTER

2. NEW CHALLENGES FOR LAW AND REGULATION

Introduction:
by Fausto POCAR

Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation
by Lucie ANGERS

Trade-offs between security and human rights
by Giuseppe BUSIA

3. NEW CHALLENGES FOR LAW ENFORCEMENT

Introduction
by Gloria LAYCOCK

Technology and Intelligence Collection
by Neil BAILEY

4. NEW CHALLENGES FOR RESEARCH AND NEW PATHS FOR DEVELOPING CURRICULA

Introduction:
by Ronald V. CLARKE

Research on crime and technology
by Cindy J. SMITH

The contribution of research to the development of more effective policies against crime
by Sandeep CHAWLA

Defining new curricula to train new professional figures
by Jerry H. RATCLIFFE

OPENING SESSION

Welcome Address

Guido ROSSI
Chairman of ISPAC

As Chairman, I want to thank the Authorities particularly Mr. Antonio Costa, the Speakers and you all participating to this Conference.

This could be the end of my intervention if I would not feel uneasy not considering one of the problems I believe to be pivotal in the relationship between crime and technology. I shall also consider that the same relationship exists between terror and globalization, while globalization is stemming from technology and terror from crime. Transnational terrorism is today made possible by the vast array of communication tools. But the paradox is that if globalization facilitates terrorist violence, the fight against this war without borders is potentially disastrous for both economic development and globalization. Antiterrorist measures restrict mobility and financial flows, while new terrorist attacks could lead the way for an antiglobalist reaction.

But the global society has yet to agree on a common definition of terrorism or on a common policy against it.

The ordinary traditional criminal law is still depending on the sovereignty of national States while international criminal justice is only a spotty and contested last resort. The fragmented and weak international institutions and underdeveloped civil societies have no power to enforce criminal justice against terrorism. In the same time the States that are its targets have no interest in applying the laws of war (the Geneva conventions) to their fight against terrorists. Wars are supposed to begin and to end and to be declared and fought against a State. But terrorism had no precise beginning and nobody knows when the bitter end will occur. Furthermore there is no such a State called Terror where terrorists abide, while Al-Qaeda is almost a nation. The States have every interest in treating terrorist as outlaws and pariahs, and when prisoners they are described, in the voice for example of the President of the U.S., as killers. The prisoners at Guantanamo Bay are beyond the rule of law and in the works of Lord Johan Steyn, in a very important article of the yesterday Herald Tribune, “a monstrous failure of Justice”. The problem of the Guantanamo Bay jurisdiction is now standing for judgment before the Supreme Court of the U.S.

We can analyze the present, but we cannot predict the future.

The present is that not having the possibility to enforce against terrorism internal criminal laws of the States, with all the procedural guaranties for a fair trial, neither the war international conventions, the terrorist in prisoned are deprived of their human rights.

The future is the challenge to find a new legal order to fight terrorism. We have to discuss and try to find the way out, asking politicians, civil society, historians, philosophers, sociologists, lawyers, scientists, academic organizations to look for general accepted rules of human morality, whose principles cannot be subject to any trade-off not even to fight terrorism. Those principles shall be the basis for new international Conventions to be submitted to the U.N.

This is the challenge which I humbly launch to the Speakers of this international conference and I believe this is the challenge of the agenda of ISPAC for the next future.

This challenge is a dilemma facing democracies, and to conclude I want to quote Aharon Barak, President of the Supreme Court of Israel (mentioned also in Johan Steyn article). In a case in which the Court held that violent interrogation of a suspected terrorist is not lawful even if doing so may save human life by preventing impending terrorist acts, he said: “Sometimes, a democracy must fight with one hand tied behind its back. Nonetheless, it has the upper hand. Preserving the rule of law and recognition of individual liberties constitute an important component of its

understanding of security. As the end of the day, they strengthen its spirit and strength and allow it to overcome its difficulties".

That is my challenge for real democratic values and also my humble suggestion for the Preparation for the Eleventh United Nations Congress of Crime Prevention and Criminal Justice.

Keynote Address

Antonio M. COSTA

Executive Director,
United Nations Office on Drugs and Crime

Mr. Chairman,
Your Excellencies,
Ladies and Gentlemen,

Let me begin by thanking you for participating in this annual conference of the International Scientific and Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC).

ISPAC works hard every year to organize a conference that brings together leading thinkers and practitioners to debate some of the most pressing criminal justice issues of our age. Two years ago, the focus was on international terrorism, last year on the rapid growth in illicit forms of trafficking, and this year on the critical issue of the relationship between crime, its control, and advances in technology.

The issue of technology and its misuse by criminals increasingly runs like a golden thread through all discussions of the new security threats that face the contemporary world.

What is perhaps so remarkable, and a critical element in why it is so difficult to understand the implications of these trends, is the speed at which these developments have occurred. The World Summit on the Information Society to be held shortly in Geneva will confront a range of critical issues in this regard, including the thorny question of the governance of the internet itself.

In the space of only about ten years significant advances in the field of technology have transformed global information flows and the way in which business is conducted.

To take just one indicator, albeit an important one for the purposes of this conference: the growth of the internet – a key symbol of globalisation and the domain for the spread of information and the conducting of legitimate business transactions, but equally, providing significant new opportunities for cybercrimes such as fraud, the spread of pornographic material, the misuse of personal data and sabotage.

In 1991 there were only a handful of internet hosts or websites, but by the beginning of this year, there were reported to be a minimum of 180 million. That is truly a phenomenal level of growth. What is perhaps more startling is that over half of that growth has taken place over the last three years with an estimated 100 million hosts being added in that short period.[1]

[1] Data collected by the Internet Software Consortium, see www.isc.org.

The benefits that such advances bring are significant – both for legitimate business activity, but also for those who engage in unlawful acts.

While terrorist organizations may still use bombs and bullets to kill and intimidate in order to promote their cause, technology has greatly facilitated these activities. Instructions for making explosive devices can be downloaded from the internet, and communication between secret cells takes place through the use of encrypted e-mails. Traffickers now not only transport tangible goods such as drugs or weapons, again using advances in technology to facilitate their underground trade, but they also traffic in 'intangible commodities' – such as child pornography – that can be shifted at the touch of a button.

As we try to anticipate the effects of technology's accelerated expansion, there are two important dimensions to consider.

Firstly, that the use of technology has broadened from wealthy and sophisticated users to the wider population. There can be few businesses, organizations and households in the developed world which do not have access to the internet and do not use it for the conduct of their activities.

Secondly, even in the developing world the benefits brought by technological advances are not insignificant. Perhaps the best example of this is that in many poor and even war torn states, where official systems of governance have all but collapsed, the mobile phone and hotmail are ubiquitous symbols of technological penetration.

This dual shift of the use of technology – both downwards and outwards – provides a critical space for the development of criminal opportunities that national frontiers can do little to contain. Take just one example that many of us have experienced – proposals for advanced fee fraud or '419 scams', the speciality of West African criminal groups, which generally involve the request for an upfront payment on the promise of a greater financial reward that never, of course, materializes. Originally such letters were faxed to a few hundred possible victims, now the internet has been used as a resource to identify likely targets, with electronic mail providing an ability to make contact with thousands of possible victims simultaneously.

There can be little doubt too that the spread of electronic banking and the rapid growth of the internet have resulted in new opportunities for economic and financial crimes. The global interdependence of the international financial system also accentuates the knock-on effects of unlawful activity. In prominent cases of substantial fraud in the banking system in the last decade, for example, such as that of BCCI, the implications were truly global, involving investors across the world and damaging the banking systems of a number of developing countries.

In a number of cases advances in technology have brought burgeoning new criminal industries.
Fraud using credit or debit cards is now acknowledged to be a serious international problem, generating higher levels of illicit profits than the counterfeiting of currency. While the growing use of plastic cards during the late 1970s and early 1980s saw various attempts at their fraudulent use, by the late 1990s this has become a truly globalised business with sophisticated organised crime groups making use of advanced counterfeiting technologies.

The anti-fraud manager of a major credit card company recently reported that it is now common – and making use of technologies that can often be purchased off the shelf – for data from genuine credit cards to be compromised in one country in the morning, counterfeit cards produced using the stolen data in the afternoon in a second country, then purchases made that evening in a third country. These countries may not even be on the same continent. In 2000 global losses for fraud committed using plastic cards was estimated to be in excess of US$ 2 billion.[2]

Quite apart from the opportunities that technology provides for crimes aimed at profit, our reliance (you may perhaps even say over-reliance) on technology brings with it significant new dangers. Bluntly put, our dependence on technology means that it causes much greater harm when it fails or comes under threat.

Technology then may itself be the subject of attack for purposes of ideology or profit.

The reliance of the global financial system on high-tech communications systems makes it vulnerable to attack by those who may wish to disrupt it. And, because globalisation places such a high premium on the provision of information, this process too is subject to the age-old crime of extortion.

The last two months have seen a wave of cyber attacks on online web retailers, internet payment systems and online gambling sites. Payments from the companies involved were then extorted under the threat that the attacks would resume.

Law enforcement officials suggest that these attacks are not the work of mischievous hackers but of sophisticated criminal operations, which were traced back to Eastern Europe.[3] A recent and successful cyber attack on a major bank was traced back to Ukraine.[4] The notorious love bug virus that caused such significant international damage just two years ago, originated in the Philippines.

The impact of technology on crime crosses borders, and while we often debate the issue as one which impacts only upon the developed world (indeed, as indicated by where the vast majority of speakers for this conference come from) there are critical implications for developing countries.

[2] Steve Vanhinsbergh, 'The evolution of plastic card fraud', *ICPR*, 491/2001.
[3] *Financial Times*, 11 November 2003.
[4] *Financial Times*, 6 November 2003.

If law enforcement agencies in the developed world struggle to retain skills and keep up with new technologies, how can similar agencies in countries in transition and in the developing world hope to compete.

This question becomes all the more urgent when it is taken into account that in many high-technology crimes the physical presence of the offender is not a defining factor. Crimes can therefore be committed from jurisdictions that have the weakest legal framework and law enforcement infrastructure to counter them. This highlights the degree to which there is a global community of interests in ensuring effective law enforcement capacity in the developing world, combined with effective systems for states to exchange information and intelligence and provide mutual legal assistance.

The United Nations has a key role to play in this regard. The UN Convention against Transnational Organized Crime, which entered into force in September of this year, provides a global response to the problems of criminal organizations and provides mechanisms for more effective cross-border cooperation. Nevertheless, this Convention only covers high-technology crimes perpetrated by organized criminal groups. Indeed, it has already been suggested that a specific international instrument to deal with the issue of high-tech criminality is now a prerequisite for building an effective global response. This issue deserves to be debated at a conference such as this.

Advances in technology in themselves provide critical mechanisms to facilitate greater global cooperation. It seems likely that over time law enforcement agencies from all parts of the globe will be in much greater electronic communication with each other. They will be able to access sophisticated global databases and track criminals more effectively across borders. The foundations for such a system are already in place through INTERPOL.

As always, however, it must be emphasised that any database or communication technology is only as good as the number of countries that would participate in such a system, as well as the quality of the information that is provided. Technology can enhance the work of law enforcement but cannot completely substitute for traditional policing or intelligence gathering methods.

Such wider access to information, the ease with which it can be collected, and its exchange among multiple agencies across the globe raise significant issues in respect of human rights. The threat of terrorism and the global reach of organized crime places renewed pressures on governments to ensure the safety of their citizens, and new demands by law enforcement and security personnel for more intrusive means to collect information to achieve this. The balance between the rights of states to access information, and the rights of citizens to their privacy, is surely one of the most important debates of the global information society. I am pleased to see that this conference will also consider this issue in some detail both from the perspective of law enforcement officials as well as those responsible for data protection.

This debate between privacy and accessibility to information demonstrates only too clearly that while technology brings many opportunities it also carries with it great challenges. For the most part, I suspect these are seldom different for law enforcement agencies than they are for any other business or government institution.

Key questions that managers have to ask themselves are, in the context of limited resources, which technologies are the most appropriate for their organization – the answers to this may not always be as obvious as they seem. A recent review of the technological requirements of local police departments in the United States based on a survey sent to many agencies came to a surprising conclusion: The technologies that police managers emphasised that needed upgrading were not necessarily the fancy law enforcement gadgets that the general public would have considered to be on the list, but rather better systems for administration and accounting.[5]

Introducing technology into any workplace also requires a series of trade offs. Because of the labour intensity of most policing activities, technology acquisition almost always has to compete with a number of other priorities, from placing more patrol officers on the street to improving levels of service. And, because of the variety of ways in which law enforcement agencies can allocate their funds, it is trade offs amongst different technologies themselves that are likely to be important.

Rapid advances in technology pose an additional and important challenge – while providing technologies to a police agency today may introduce immediate benefits, the return of the investment will gradually decrease as the systems become obsolete, and are overtaken by other newer technologies. It is possible that other programmes, whose returns increase with time rather than decrease, might be better policy targets. Here the importance of training, an issue to be considered at this conference, must receive some attention. Correctly conducted, training has the possibility to improve not only how officials use current technologies, but also building capacity in order to improve their use of the technologies of the future, and, at the same time, building a better understanding of the implications of technology use on human rights.

None of the challenges or trade offs I have spoken of should be interpreted as a belief that technology is not bringing a revolution to law enforcement. If we are realistic, however, that revolution brings with it a series of questions about the most adequate application of technology, not only to enhance ordinary policing, but also more specialized law enforcement interventions. As I believe speakers at the conference will indicate, the use of DNA technology, advances in forensic science and improved capacities for intelligence collection will mean that police agencies, particularly in highly specialized fields, will continue to undergo rapid advances.

[5] RAND, *Challenges and Choices for Crime Fighting Technology*, 2001.

In the context of this debate it must be highlighted too that technology can play a critical role not only in improving the prospects for effective law enforcement, but also for improving the transparency and accountability of agencies responsible for bringing justice. More sophisticated information systems also mean that the monitoring of police performance is enhanced. These factors have resulted in greater scrutiny of the police, more public awareness about both their successes and failures, and greater pressures than ever on police managers to orientate their agencies towards more clearly stated goals and objectives.

Greater access to information in the longer term will also by implication improve the transparency of governments, a key prerequisite for fighting corruption.

Let me conclude by saying that I look forward with great anticipation to the discussions and outcomes of your deliberations. The role of the United Nations is to provide assistance to developing countries and countries in transition. We need to continue to study the lessons learnt in the field of technological interventions to combat crime, enriching the input and advice we provide in the field of law enforcement and crime prevention.

It should also be said that many of the issues that I have raised in relation to both the advantages and challenges that technology brings apply also to the United Nations. Never before has there been such opportunity for the UN to convey its message and its work to the peoples of the world. With the information available – and just a short visit to the UN's various websites will aptly demonstrate this – the detailed work of the organization is open to public scrutiny in a way that is unprecedented.

There can be little doubt that advances in technology have both brought new opportunities for the conducting of criminal activity as well as new opportunities and challenges for law enforcement. It is perhaps not yet possible to fully understand the implications of these developments – hence the importance of maintaining a healthy debate that brings together not only government officials, but members of the scientific and academic communities as well as representatives of civil society, debating not only the specific details of the technologies themselves, but their broader implications for our communities.

I wish you every success as you explore these critical issues.

Thank you.

1. THE IMPACT OF TECHNOLOGY ON CRIME

Introduction

Ernesto U. SAVONA
Professor of Criminology,
Milan Catholic University
Director,TRANSCRIME
President, European Society of Criminology

Cyber-crime: typologies and likely future trends*:*

Chris PAINTER
Deputy Chief, Computer Crime
and Intellectual Property Session
Chair, G8 High Tech Crime Subgroup

2. NEW CHALLENGES FOR LAW AND REGULATION

Introduction

New Challenges for International Rules against Cyber-crime*

Fausto POCAR
Professor, Milan University
Vice President, International Criminal Tribunal
for the former Yugoslavia, The Hague

This paper is aimed at identifying, in light of current approaches of international institutions dealing with cyber-crime and existing legal instruments in this area, the main issues which require further consideration for the purposes of combating this criminal phenomenon. Such issues include the definition of crimes and of sanctions, an enhanced international cooperation between domestic authorities, and harmonized criteria for establishing jurisdiction over cyber-crimes.

1. The need for international instruments

It is almost a banal remark to state that crime follows human technological progress: as cyberspace was established as a new medium of communication, criminal activity followed in parallel. In addition, this kind of criminal activity takes advantage of and expands as a result of all the opportunities offered by the Internet, i.e. the evolution of e-commerce, the growth of multinational companies, the ease and speed at which information can be passed around the world, the security and anonymity provided by this technology, and, above all, the territorial dimension of traditional legal approaches. Finally, for organized crime «[t]he spoils (…) are significant and the risk must appear very low» (National Hi-Tech Crime Unit, 2002)[6] and this situation leads to great vulnerability for any member of the international community.

A recent *Proposal of the Commission of the European Union for a Council Framework Decision on Attacks against Information Systems*[7] organizes in these terms the phenomenon: «Computer-related crimes are committed across cyberspace and do not stop at the conventional, political State-borders. They can, in principle, be perpetrated from anywhere and against any computer user in the world. (…) Given the worldwide dimension of the Internet, safety and confidence in cyber-space is an activity which calls for a collective response on a global scale. (…)».[8] The dichotomy is, indeed, between the globalization of crime and the territoriality of domestic law, generally confined to a specific territory.

Thus, «solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments», including, in particular, «binding international instruments, that can ensure the necessary efficiency in the fight against these new phenomena» (Council of Europe, 2001b).

2. International legal sources on cyber-crime

[6]* Fausto Pocar is, Professor of International Law at the , University of Milan (Italy) and Vice President of the International Criminal Tribunal for the former Yugoslavia, The Hague (The Netherlands). The substance of this article reflects a paper submitted by the author to the International Conference on ***Crime and Technology: New Frontiers for Legislation, Law Enforcement and Research***, held in workshop on cyber-crime held in Courmayeur on 28-30 November 2003.

The National Hi-Tech Crime Unit (NHTCU) is a part of the United Kingdom's National Hi-Tech Crime Strategy (NHTCS), founded in April 2002, based in London whose role is defined as follows: supporting and leading activity against serious and organized hi-tech crime of a national and transnational nature; responding with an investigative capability to all threats to and attacks upon the critical national infrastructure; undertaking strategic threat assessments; developing intelligence; supporting and coordinating law enforcement operations; offering '"best advice"' to other law enforcement agencies, business, industry and the IT world.

[7] Commission of the European Union, Proposal for a Council Framework Decision on Attacks against information Information systemsSystems, in *Official Journal of European Communities,* C 203 E, 27 August 2002, pp. 109-113.

[8] ***Ibidem***.

In order to identify the issues that combating cyber-crime may raise, it is important to briefly describe the relevant international legal sources and instruments that have been elaborated so far on the matter. They pertain to different levels of cooperation, both at the universal and regional level.

At the universal level, the United Nations has been called upon to play an important role. This Organization works through its policy-making body (developing pertinent recommendations[9]) and its many agencies, such as the Commission on Crime Prevention and Criminal Justice (inside the Economic and Social Council) or the Office of Drug Control and Crime Prevention: the first one adopted a *Plan of Action* dealing with the prevention and control of high-technology and computer-related crimes (UN Economic and Social Council, 2001); the second is carrying out this plan.

Notwithstanding that not all transnational computer crimes belong to the area of "organized crime", attention should also be given to the *Palermo Convention against Transnational Organized Crime* (signed on 15 December 2000),[10] whose purpose is the «prevention, investigation and prosecution» of this kind of criminality. The latter is comprised of enumerated crimes (arts. 5, 6, 8 and 23), as well as of crimes referred to simply as «serious crimes», each «conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty».[11]

The United Nations is not alone in approaching the issues raised by cyber-crime; other entities actively work on this topic from different perspectives. One could mention the OECD (Organization for Economic Cooperation and Development), whose effort is directed towards establishing transparent relationships inside private sector companies, in order to ensure free competition. In this perspective the Organization adopted the *Guidelines on the Security of Information Systems and Networks* (OECD, 2002),[12] that call for the development of a 'culture of security', to ensure the stable evolution of the digital economy and information society.[13]

On a different level, one also has to consider the activity of non-governmental entities, such as the International Association for Criminal Law, whose resolutions and recommendations may guide policy-making authorities.[14]

Among regional organizations, the activity of the Council of Europe and the European Union is particularly relevant.

The first circle of cooperation has led to the adoption of the *Convention on Cyber-Crime* (Council of Europe, 2001a)[15] and its *Additional Protocol* (Council of Europe, 2003). The Council of Europe Convention is the first multilateral treaty on cyber-crime. It provides the basis framework for the establishment by contracting States of domestic substantive and procedural laws aimed at combating all types of computer-related crimes,

[9] See, in particular, General Assembly rresolutions 56/121 of 19 December 2001 and 56/261 of 31 January 2002: in the first resolution the General Assembly underlines the need for enhanced cooperation among States in combating the criminal misuse of information technologies and stresses the role that could be played by the United Nations and the other universal and regional international Organizations; in the second one the General Assembly took note of the UN Plan of Action (UN Economic and Social Council, 2001) (see *Official Records,* 2001) and invited member States and the Secretary-General to consider the formulation of legislation policies and programmes on the matter.

[10] The text of the Convention is available at http://www.odccp.org/palermo.

[11] Art. 2, lettiert. b) of the Palermo Convention.

[12] So called '2002 "Security Guidelines"', available at http://www.oecd.org/dataoecd/59/0/1946946.pdfhttp://www.oecd.int/document.

[13] OECD discussed also the principles contained in the first edition of a *Global Action Plan for Electronic Commerce* (Ottawa, October 1998), prepared by the Alliance for Global Business in October 1998(AGB), that urged governments to rely on business self-regulation and the voluntary use of empowering technologies as the main drivers, behind the creation of trust across the whole spectrum of users and providers of e-commerce goods and services; it also stated that governments should focus on the provision of a stable and predictable environment enabling the enforcement of electronic contracts, the protection of intellectual property and safeguarding competition. The second edition of this Plan (Alliance for Global Business, (October, 1999)) establishes a set of fundamental principles as the basis for the framework in which policymaking for electronic commerce should take place.

[14] As to cyber-criminality see, for example, I recall the resolutions and recommendations adopted at the Association Internationale de Droit Pénal mMeeting of the International Association for Criminal Law held on of 28 October 2002 (resolutions and recommendations are available at http://www.penal.org/generale).

[15] The Convention was signed in Budapest on 238 November 2001, in *ETS* No. 185.

and the means whereby States can cooperate expeditiously with one another during the course of transnational investigations. Its Protocol is devoted to combating acts of a racist and xenophobic nature committed through computer systems.

As regards the second circle, the acts adopted within the framework of the so- called third pillar of the European Union (arts 29 ff. of the EU Treaty) should be mentioned. For the time being, the efforts against cyber-crimes are spelled out in the above mentioned *Proposal of the Commission of the European Union for a Council Framework Decision on Attacks against Information Systems*, in the *Council Decision of 29 May 2000 to Combat Child Pornography on the Internet*,[16] in the *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency,*[17] in the *Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime,*[18] as well as and in the *Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on Negotiations Relating to the Draft Convention on Cyber Crime held in the Council of Europe* [19] and in the *Joint Position of 29 March 1999 defined by the Council on the basis of Article K.3 of the Treaty on European Union, on the proposed United Nations Convention against Organised Crime*.[20] The European Commission should also been active in the debate with its *Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer related-Crime.*[21]

In the European context, it has also to be noted that the EU member States have ratified the *EUROPOL Convention,*[22] which provides for a framework of police cooperation against organized crimes, thus also involving cyber-criminality.

In light of the foregoing indications, it appears that the list of international legal instruments dealing with cyber-crime is rather long. However, it is far from exhaustive for the purposes of covering all aspects of the subject matter concerned. Moreover, it has to be noted that, apart from EU legislation, not one of the mentioned legally binding international instruments is yet in force. In general terms, existing international rules have been structured along two different though compatible routes. On the one hand, they provide for the duty of contracting States to implement within their own borders internationally agreed norms, with a view to bringing the legal system of contracting States closer both as to the substance and the practice of criminal law. On the other hand, these rules establish procedures for relevant international relations, aimed at providing such forms of cooperation between national judicial authorities, that may interact with each other both swiftly and efficiently.[23]

---

[16] Council of the European Union, ~~O~~Council Decision of 29 May 2000 to Combat Child Pornography on the Internet, ~~fficial Journal of European Community, L 138, 9 June 2000, 1 ff.~~in *Official Journal* ***of the European Communities***, L 138, 9 June 2000, pp. 1-4.

[17] Commission of the European Union, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, ~~Presented by the Commission on~~ 11 February 2003, COM (2003) ~~,~~ 63 final.

[18] Council of the European Union, Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime~~Recommendation of 25 June 2001~~, in ***Official Journal of European Communities~~y~~,~~*** C 187, 3 July 2001, pp. 5-6.~~.~~

[19] Council of the European Union, Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on Negotiations Relating to the Draft Convention on Cyber Crime held in the Council of Europe, in ***Official Journal of the European Communities~~y~~***, L 142, 5 June 1999, pp. 1-2.~~1 f.~~

[20] Council of the European Union, Joint Position of 29 March 1999 defined by the Council on the basis of Article K.3 of the Treaty on European Union, on the proposed United Nations Convention against Organised Crime, in ***Official Journal of the European Communities~~y~~***, L 87, 31 March 1999, pp. 1-2.~~.~~

[21] Commission of the European Union, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', 26 January 2001~~, 52000DC0890~~.

[22] ~~Adopted by the~~ Council of the European, ~~U on 26 July 1995, Official Journal of European Community, C 316, 27 November 1995.~~Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), in ***Official Journal of the European Communities***, C 316, 27 November 1995, p. 1.

[23] In a similar perspective as regards international legal efforts on combating corruption, see Parisi and Rinoldi (2004).

3. Defining cyber-crimes in international legislation

Among the various issues that may arise from existing international legislation on cyber-crime and efforts aimed at establishing new legal instruments, two appear to be especially sensitive: the definition of cyber-crimes and the sanctions to be applied to perpetrators.

The first issue concerns an aspect which may appear at first sight to be of a purely terminological nature, i.e., the definition of the activities included in the expression 'cyber-crime'. It is however a very substantive issue, both because it deals with the problem of identifying the elements of cyber-crime, which is a central prerequisite for criminal prosecution, and because of its impact on the effectiveness of international cooperation in the field. The problems that arise in this context may be summarized as follows.

Firstly, the terms 'cyber-crime', 'computer crime', 'computer related-crime' and 'high-tech(nology) crime' are often used interchangeably, without an appreciation of different substantial grounds. However, these terms cover different crimes. By way of example, Europol assumed that 'high technology crime' consists of the use of information and telecommunications technology to commit or further a criminal act, against a person, property, organization or the network computer system. 'Cyber-crime' (and its sub-categories) is the criminal use of any computer network or system on the Internet; attacks or abuse against the systems and networks for criminal purposes; crimes and abuse from either existing criminals using new technology; or new crimes that have developed with the growth of the Internet.

Secondly, this terminological confusion exists in addition to diverging international praxis and domestic laws: different views exist on what constitutes crime involving in some way the Internet. In other words, national legal orders have different approaches towards this phenomenon (Podgor, 2002).

A common aspect is represented by the *noyau dur* of six kinds of behaviours, i.e. intellectual property theft or software piracy, hacking and virus attacks, organized on-line paedophilia, denial of service attacks, extortion, and fraud. As one can see, some of these crimes may also be perpetrated outside of the Internet. And indeed, almost any crime that can be committed in the real world can also be perpetrated in the virtual one; but, it is beyond doubt that some crimes have been revitalized as a result of the electronic environment.

This situation entails the need for clarification at the legal level, based on a consideration of distinct factual situations: a computer may be the 'object' of the crime (because it is targeted), the 'subject' (as it is the physical site of the crime), or the 'source' (as viruses and worms start from it).

It follows that a comprehensive definition could only be very general, such as defining cyber-crime as the criminal use of any computer network or system on the Internet, which implies attacks or abuse against the system and network for criminal purposes.

Scholars also distinguish between 'vertical' computer crimes and 'horizontal' ones (i.e. computer related crimes) (Clarberg, 2003: 2). This partition is also followed in the solution offered by existing international rules as well as by some international instruments in the course of their adoption, which appear to distinguish between 'computer specific crimes' and 'traditional crimes performed with the aid of computer technology'. Such is the case of the Council of Europe *Convention on Cyber-Crime*,[24] and its *Additional Protocol*,[25] as well as of the mentioned *Proposal for a Council Framework Decision on Attacks against Information Systems*.

In this context, international legal instruments should be aimed at harmonizing the material elements of crime envisaged by domestic legislations, with a view to establishing a common international *minimum standard* of relevant offences internationally imposed. It is self-evident that this task also entails a revision of substantive laws in many areas of national legislation, such as the data protection legal regime (and privacy), electronic surveillance, abilities to secure traffic data, and others. Unfortunately, a precise description of cyber-crimes is currently left by existing legal instruments to domestic legislation, and this may entail major difficulties in their effective application when they will come into force, unless parallel harmonization efforts are successfully carried out.

[24] Arts 2-13.

[25] ~~Strasbourg, 28 January 2003: a~~Arts 3-7~~.~~;

A second delicate area is no doubt the area regarding sanctions. Two different issues may be identified as emerging from existing legal instruments or proposals. The first one relates to the type of sanctions that should be imposed on perpetrators. Following a well-founded practice, international legal instruments oblige contracting/member States to establish sanctions that are «effective, proportionate and dissuasive». The Budapest Convention contains provisions in these terms (art. 13); the same applies to the European Union *Proposal for a Council Framework Decision on Attacks against Information Systems*. However, the nature (criminal, administrative or civil) of the sanctions tends to be left to each State, as pertaining to its domestic jurisdiction.[26] Here too, as in the area of definition of crimes, serious difficulties may arise in coordinating activities intended to combat cyber-crimes, unless efforts aiming at harmonizing national legislation are not only encouraged, but successfully carried out, in order that sanctions may constitute an effective deterrent against the commission of violations in this field. The second issue relates to the need to establish criminal liability also for legal persons, and to provide the possibility of imposing on them monetary sanctions, following a route indicated by the *OECD 1997 Convention on Combating Bribery of Foreign Officials in International Business Transactions* (OECD, 1997).[27]

4. Enhancing international cooperation on combating cyber-crimes

The above mentioned difficulties show that international legislation and efforts aimed at the harmonization of national laws and procedures would almost miss the mark if they were not accompanied by effective international cooperation: the world-wide dimension of the Internet implies that its illegal use and related offences must prompt responses and concerted efforts from all relevant domestic and international authorities.

In this context, mutual cooperation among domestic judicial authorities plays a critical role. Such co-operation is mainly based, in traditional legal instruments concerned with combating serious crimes, on the principle *aut dedere aut judicare*. The same approach also tends to be followed as far as cyber-crime is concerned.

In this scenario the principle may experience new developments, at least at the European level, from the adoption of the European arrest warrant,[28] which involves a form of handing over the suspect person based on the recognition – by the judicial authorities of the requested State – of the restrictions on personal freedom (albeit not definitive) adopted by the judicial authorities of another member State. The mutual trust in the system of administration of criminal justice allows the transfer to take place in the absence of the traditional evaluation of political considerations by non-judicial authorities as in the case of extradition. Furthermore, the warrant excludes the need to respect the criterion of double jeopardy, thus minimizing the impact of differences in the domestic legislation of member States. Whether a system of this kind, based on the principle of mutual recognition, may be exported to other countries is hard to say, in light of the difficulties that its establishment encounters in the European Union itself. However, there is no doubt that the form of cooperation that it implies would contribute substantially to fighting such crimes as cyber-crimes, which are international in nature (Parisi and Rinoldi, 2004).

In any event, and apart from this scenario, it has to be stressed that almost all different forms of mutual cooperation presuppose the respect of the dual criminality criterion. But, in turn, the application of the latter requires a harmonized approach to the definition of the crimes involved. An efficient cooperation in the implementation of the principle *aut dedere aut judicare* is therefore strictly linked to successful efforts in bringing domestic legislations on cyber-crime closer.

---

[26] Following the teaching of the Court of Justice of the European Communities in the so called '~~"~~mais case'~~"~~ (judgement 21 September 1989, case No. 68/88). -

[27] ~~The text can be found on the website www.oecd.org/EN/document/0,EN-document-88-3-no-6-7198-88.00.html.~~ The Convention came into force internationally on 15 February 1999.

[28] Council of the European Union, Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States~~Framework decision 2002/584/JHA of 13 June 2002 *on the European arrest warrant and the surrender procedures between Member States*~~, in ***Official Journal of the European Communities***~~,~~ L 190, 18 July 2002, pp. 1-20-.

5. Investigation and prosecution of cyber-crimes

From another point of view, international mutual cooperation is also necessary for investigation and prosecution purposes. Indeed, combating offences such as those under consideration requires strategic intelligence on hi-tech criminality, tactical intelligence aimed at identifying new hi-tech criminality targets for investigation, and intelligence support to the operational activities of international agencies, such as Interpol and Europol.

One has to wonder whether traditional procedural measures (such as search and seizure) are also useful in the new technological environment, or whether new measures should be envisaged. One could think, for example, of expediting the preservation of data, in order to ensure that traditional measures of collection remain effective in the volatile technological area; or developing and implementing a tactical hi-tech crime intelligence database and a confidential source register, which would allow for the protection of the identity of sources of information, following the example of national agencies such as the British National Hi-Tech Crime Unit. In this context, one could mention that the European Union is adopting a very interesting *Framework Decision on the European Evidence Warrant for Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters*.[29]

Finally, one has to stress that interstate cooperation may not be sufficient to cover all aspects of cyber-crime. High priority should also be given to enhancing cooperation between public authorities and private companies involved in the production and commerce of hardware and software, as well as of those involved in the delivery of services in the area. Strategic and closer relationships could help both the policy and legislative level and the investigative and law enforcement level, in particular as far as some types of cyber-crimes (such as on-line fraud, hackers and virus writers) are involved (UN Economic and Social Council, 2002).

6. Some remarks on jurisdiction over cyber-crimes

Prosecuting and trying persons allegedly responsible for cyber-crimes also raises difficult problems in the field of jurisdiction. These problems relate to the determination of the place where the offence was committed (*locus delicti),* to the application of *ne bis in idem* principle when several jurisdictions are equally competent, and to the avoidance of negative jurisdiction conflicts.

It is well known that the existence of various principles to ground domestic criminal jurisdiction is generally recognized and that jurisdictional problems are not new in the practice of international relations (Jennings and Watts, 1992: 137-139). The principles on which criminal jurisdiction is normally based in domestic legislation are the *territoriality* principle, whereby an alleged perpetrator can be brought before the courts of the State where the crime was committed, and the *nationality* principle, whereby the courts of a State have jurisdiction to try a national of that State, irrespective of the place where the crime was committed. The nationality principle is also frequently invoked in order to attribute jurisdiction to the courts of a State over a foreigner when the victim of the crime is a national of that State, irrespective, again, of the place where the criminal activity was performed.

It has to be stressed, however, that the territoriality principle may appear to be of limited value when cyber-crimes are at issue, in light of the borderless nature of the Internet. However, legal practice appears to accept it, coupled with the principle of nationality, which may be more suitable in several cases, especially if it were to be used in relation to victims of cyber-crimes, since it would at least enable a State to protect its nationals, if not all the victims of the crimes.

Finally, one could mention in this context the principle of *universality* as a ground for criminal jurisdiction. Normally, this principle has been invoked as applicable to the exercise of jurisdiction over a narrow range of

[29] Commission of the European Union, Proposal for a Council Framework Decision on the European Evidence Warrant for Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters, ~~Proposal~~ 14 November 2003, COM (2003) 688 final~~.~~.

crimes (no one typically computer-related), such as crimes against humanity, war crimes, and genocide. It has also received some recognition in a few treaties aimed at combating other crimes that the international community regards as crimes of an international nature, such as aircraft hijacking.[30] In light of the borderless character of cyber-space, one may wonder whether universal jurisdiction, accompanied by an obligation to follow the principle *aut dedere aut judicare* would provide an interesting approach for the resolution of jurisdictional issues in this area, which merits careful consideration.

It appears, on the contrary, that international courts and tribunals would hardly have a role to play in this field, unless specific cyber-crimes result in serious violations of human rights, which would be regarded as crimes against humanity. Only in such a case would the intervention of international jurisdiction to try cases which would not be brought before domestic courts, due to the inability or the unwillingness of States to do so, be justified.

[30] As of the Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963, which was followed by the Hague Convention for the Suppression of Unlawful Seizure of Aircrafts, 1970, and by the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971. For a consideration of these and other conventions that adopt the principle of universal jurisdiction, see e.g. ~~M. Shaw, *International Law*, 4th ed., 470 ff.~~Shaw (1997: 470 ff).

References

Alliance for Global Business (1999). *A Global Action Plan for Electronic Commerce* (2nd edition). October.

Clarberg, B. (2003). Cyber Crime. Paper presented at the Conference on *International Cooperation on Trans-national Crime*, The Hague, 9-10 October (unpublished).

Council of Europe (2001a). *Convention on Cyber-Crime.* Budapest, 23 November.

Council of Europe (2001b). *Convention on Cyber-Crime, Explanatory Report.* 8 November.

Council of Europe (2003). *Additional Protocol to the Convention on Cyber-Crime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.* Strasbourg, 28 January.

Jennings, R. and Watts, A. (Eds) (1992). *Oppenheim's International Law*. London: Longman, 9th edition.

National Hi-Tech Crime Unit (2002). *Operational Protocol between the National Hi-Tech Crime Unit and Parties within the Strategic Stakeholders*. May.

OECD (1997). *Convention on Combating Bribery of Foreign Officials in International Business Transactions*. 21 November.

OECD (2002). *OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security*. Paris: OECD.

Parisi, N. and Rinoldi, D. (2004). Recent Evolutions in the Fight against Corruption in the International Trade Law. *Le droit des affaires internationales,* 1.

Podgor (2002). International Computer Fraud: a Paradigm for Limiting National Jurisdiction. *U.C. Davis Law Review*, 35.

Shaw, M. (1997). *International Law.* New York: Cambridge University Press, 4th edition.

UN Economic and Social Council (2001). *Official Records of the Economic and Social Council, 2001, Supplement No. 10 (E/2001/30/Rev.1)*.

UN Economic and Social Council (2002). *Effective Measures to Prevent and Control Computer-Related Crime. Report of the Secretary-General.* 29 January.

Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation

Lucie ANGERS[31]
Senior Counsel, Criminal Law
Policy Section, Justice,Canada

Nothing has more revolutionized and shrunk the world we live in than the Internet. This network of networks of computers, initially intended for communication between an elite working on military issues, has become one of the most prevalent way in which we do business, entertain ourselves and work. No more do we call our colleagues to invite them for lunch; we send them an e-mail instead. Doctors in one country can make a diagnosis of a disease affecting a person thousands of miles away. We purchase goods through the Internet, we make friends over the Internet and we access huge amounts of information on the Internet. The Internet is at the heart of a considerable part of our busy days.

The purpose of this paper was initially to deal with international cooperation in combating computer and computer related crime or as it is more known today, cyber-crime. However, it is impossible to address the issue of international cooperation without first dealing with two of its pre-requisites at the domestic level: the criminalization of computer and computer--related offences and the creation of procedural powers to investigate and prosecute those committing such crimes. International cooperation mechanisms are a necessary response to cyber-crime, but not a sufficient one. A substantial portion of cyber-crime is transnational in nature, but some can happen at a purely domestic level. More importantly, it will usually be impossible to respond effectively to foreign requests for assistance unless adequate domestic powers covering criminal offences and investigative procedures are in place, and unless there are officials trained and equipped to administer and enforce them. The fight against cyber-crime has to start with -the adoption of strong substantive and procedural legislation at the national level. However, it is only by having all countries taking such steps that successful international cooperation can be achieved. A chain is only as strong as its weakest link: if even a few countries fail to adopt or enforce adequate measures, electronic "safe havens" are created which can be exploited by offenders.

After dealing with ways in which computers are used by criminals and the challenges at stake, this paper will deal with both substantive offences and procedural powers that need to be adopted before a country can be relied upon to provide international cooperation. It will then review the international cooperation mechanisms that contribute to a successful fight against cyber-crime and the work that is being done at the international level in this respect. It will conclude with a brief look into the future of cyber-crime and the measures that will be needed to control it, while still maintaining the benefits of the technologies involved.

Use of computer systems

At the heart of the Internet are millions and millions of computers interlinked together.[32] These computers, which were once used by a few to do complex mathematical operations, are now used by children and the elderly, men and women, scientists and salespersons alike to communicate and facilitate their way of doing their daily tasks. As most new technologies, computers can be used in ways that are beneficial but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of a country. Criminals have been quick in foreseeing what computers and networks can do for them.

[31] Senior Counsel, Criminal Law Policy Section, Justice Canada. The author wishes to express her appreciation to Christopher D. Ram for this helpful comments and suggestions. The views expressed in this paper may not necessarily represent the views of the Government of Canada or any department or agency thereof.

[32] For an overview of Internet expansion, see Christopher Ram in International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC) 2002 and sources there cited. The first public access to what later became the Internet occurred in 1969, and the total number of known computers (Internet hosts) in January 2004 was 233.1 million. Growth has been roughly exponential. Between 1969-1992, only 10 million computers were connected. The number passed 100 million in late 2000, stood at 162 million in mid-2002 and reached 233.1 million at the beginning of 2004. Source: Ram, 2002 and Internet Systems Consortium, http://www.isc.org/index.pl?/ops/ds/, visited March 2004.

First, using computers as a **tool**, they have understood how computers can help them in committing traditional crimes in a more efficient way. For example, child pornography, which was not so long ago a hidden activity shared among a few initiated pedophiles, has become more readily accessible to the general population. Governments wanting to shut down websites containing obscene or hateful material within their jurisdiction might, if they have the necessary legislation to do so, find out that the same website reappeared the following week in a far away country. But it is not just these "communication crimes" which have been facilitated, but the planning of more traditional crimes, such as murder and theft as well. Fraud scams developed in one country create victims in countries thousands of kilometers away, and offenders can target thousands or even millions of victims with a single e-mail. Potential profits increase dramatically, and there is often much less risk of detection, prosecution and punishment than with more traditional means of committing the same offences.

Second, computers help criminals to keep track of their transactions, such as drug deals and phone numbers of accomplices. Used as a **storage device**, computers serve as repositories of evidence relating to a crime, as well as records of criminal activity. This, however, is a double-edge sword for criminals, as such data could also be legally obtained by adequately trained law enforcement officers in their investigations and subsequently used in the prosecution of criminal offences if the country's legislation allows for the obtaining of electronic evidence. In addition, offenders are also becoming increasingly sophisticated at using security technologies and choosing storage locations in other jurisdictions, greatly complicating the task of law enforcement officials seeking access to digital evidence.

Finally, computers themselves have also become **targets** for those who wish to exploit their advantages to the detriment of their owners. This category, which is obviously linked to the first category of computers used as a tool, includes hacking, denial of service attacks, release of viruses and other malicious code, website defacements and the installation of worms and Trojans. These actions are all different ways of getting access to or attacking the availability, integrity and confidentiality of data contained in these computers. However, contrary to the two previous categories in which a computer is used either as a tool or a storage device, most countries have adopted or will require amendments to their criminal legislation to deal with situations in which a computer is the target of a crime. While common traditional offences such as mischief, fraud or forgery might be applied when a computer is the target of a crime, there will be a number of cases in which these offences will not be adequate. Traditional theft offences, for example, may not extend to cases where intangible information is taken, or only copied from a computer system, or where monetary losses to the owner cannot be established or quantified.

Challenges and possible solutions

These three different ways in which criminals resort to computers to help them in pursuing their criminal activities have posed a number of challenges, not only to the state in which such persons commit their crimes, but also in the different countries in which the effects of the crimes are felt. One of the major challenges in dealing with cyber-crime is created by the borderless nature of computers and the Internet.

For most people using a computer, the location of the website they are accessing or the person they are contacting is of no relevance, nor is in many cases the identity of the person they are communicating with. They search for, access and download the information they seek with little regard for the location or identity of the source – and often too little regard for the quality of the information. However, for the criminal justice system of the country or countries in which a computer or computer-related crime is occurring, the question of the territory in which the crime is committed lies at the heart of the main concern, i.e., who can prosecute such crimes? Linked as it is to the issue of sovereignty, the question of jurisdiction is also one of the main issues that needs to be addressed by all international or regional organizations dealing with cyber-crime. As the G8[33] has experienced during its negotiations concerning the *Principles on Transborder Access to Stored Computer Data* or its *Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations* or as was experienced by the Council of Europe, during its

[33] The documents adopted by the G8 meetings can be found at: http://www.g7.utoronto.ca/meetings.html. The text and other materials relating to the Council of Europe Convention are available on-line at: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

discussions leading to the adoption of the *Convention on Cyber-crime*[34] on issues in relation to which no agreement could be reached, such as data retention or transborder intercepts, states are willing to work together to fight cyber-crime but experience serious difficulties when such a fight entails pushing or shrinking the boundaries of their jurisdiction.

In addition to the problem of borderless crimes being investigated by countries in which law enforcement is constrained by borders, are those problems related to the nature of computer and computer-related crimes themselves. There is not yet a common understanding of what constitutes a computer or computer-related crime. Although the Council of Europe *Convention on Cyber-crime* has paved the route in this regard by requiring all States Parties to the *Convention* to criminalize eight computer or computer related crimes, more harmonization is needed before such a concept meets with a common general understanding. This is particularly true in developing countries, many of who have development strategies which involve the use of information technologies but who may have a very different understanding of what computer crime is or how it should be dealt with.

Finally, the ultimate challenge faced in the fight against cyber-crime relates to the apparent proliferation of such crime and the equally apparent lack of adequate human and financial resources and training to appropriately allow for that fight to happen. While there is a clear lack of statistics in relation to the amount of computer and computer-elated crimes as most countries do not take into account whether a crime was committed through traditional means or with the assistance of a computer,[35] most people are under the impression that those committing such crimes are under a minimal risk of apprehension and the risk of detection of such activity is also low. The combination of this perception, along with the fact that the investigation and prosecution of such crimes can be extremely complex and onerous since the evidence relevant to such crimes is contained in data that is intangible and transient by nature, is probably sufficient to threaten the growth of electronic commerce allowed by the Internet.

States, as well as regional and international organizations, have been struggling to keep pace with the challenges created by these rapidly evolving technologies. In some ways, these technologies make it more and more difficult to gather the information and evidence required to carry out effective investigations and prosecutions in a single jurisdiction. In other ways, the technologies actually create and preserve evidence that would not have existed before, but often require a high degree of training and sophistication on the part of investigators, and fully up-to-date legal powers, to take full advantage of the new opportunities. To maximise the advantages and minimise the problems, a number of states have been putting their efforts together, developing different international or regional instruments to fight cyber-crime, and assisting one another in areas such as legislative development and the training of investigators.

The most well known international legal instrument is the Council of Europe *Convention on Cyber-crime*, referred to earlier. This international treaty provides States Parties with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence. The *Convention* calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, and the promotion of international cooperation through mutual assistance and extradition in a criminal realm that knows no borders. The Convention, which is open to countries outside Europe provided some basic requirements are met,[36] will help states fight crimes committed against the integrity, availability and confidentiality of

---

[34] The *Convention on Cyber-crime* (ETS No. 185) was opened for signature on November 23, 2001. The text and other materials relating to the *Convention* are available on-line at: http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm. As of March 19, 2004, 32 countries had signed the Convention and 5 have ratified it and it is scheduled to come into force on July 1, 2004. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[35] The need for global research into the nature, extent and development of crimes involving computers, networks and other information and communications technologies is a major challenge in and of itself. Some developed countries have begun to gather information, but a truly global picture, critical in understanding the problem and developing effective responses, remains a long way off. For a review of some of the issues involved, see: Report of the Secretary General to the 10th Session of the United Nations Commission on Crime Prevention and Criminal Justice, (conclusions of the study on effective measures to prevent and control high-technology and computer related crime), E/CN.15/2001/4, available on-line at: http://www.unodc.org/unodc/en/crime_cicp_commission_session_10.html.

computer systems and telecommunications networks as well as traditional offences committed using networks such as on-line fraud or the distribution of child pornography over the Internet.

The Commonwealth has also dealt with the issue of cyber-crime and developed model legislation to help its member States at the domestic level. In 2002, Commonwealth Law Ministers adopted a model law entitled the *Computer and Computer Related Crimes Act*[37]. This model law, which has a common framework with the Council of Europe *Convention on Cyber-crime*, provides law enforcement with effective and modern tools to fight cyber-crime.

However, the solution to cyber-crime does not only reside in better international cooperation by adopting international or regional instruments to address the jurisdictional problems created by the borderless nature of computers networks. International cooperation is of no use if a country does not have in place the proper legal framework to first address the problem at the domestic level. Several of the major challenges posed by cyber-crime are at this level. Legislation setting out traditional offences needs to be adjusted to make it effective when the same offences are committed using information technologies, and new offences are often needed, especially for conduct in which the technologies and their users are themselves targeted by offenders. Once adopted, keeping abreast of new technological developments is also essential, and this is a significant problem even for countries with a high degree of socio-economic development and access to a high degree of technical expertise. It will prove a much more serious problem for developing countries. Finally, creating and maintaining the technical expertise needed to investigate and prosecute offences at home and to respond quickly and effectively to requests for cooperation in transnational cases is also a major demand, both on resources and technical expertise.

It is essential that all states must take a multi-faceted approach. First, all States need laws that will criminalize computer and computer-related crime by establishing adequate definitions and offences in this respect. Second, they need to develop adequate procedural laws and training courses to allow for the timely and efficient investigation and prosecution of cyber-criminals. This implies the development of the technical expertise needed to obtain and preserve data and to ensure that it can be produced as evidence in court. Finally, they need the commitment and capacity to improve international cooperation in order to trace criminals on the Internet and assist one another in the conduct of transnational investigations and prosecutions.

Substantive legislation

a) The principles

Without national legislation to deal with the use of computers as tools, storage devices and targets, no international cooperation to fight cyber-crime is possible. However, such legislation cannot be developed in a vacuum and needs to be harmonized from one country to the other. Each country must apply its own legal framework, but consistency between countries in their approaches to the framing of offences and investigative powers and procedures greatly simplifies and expedites matters of mutual legal assistance, extradition and other forms of cooperation. This is a major factor in dealing with all forms of transnational crime, but will be particularly important in the fast-moving investigations commonly required to deal effectively with cyber-crime cases.

Even more important is the requirement that each and every country must take some action. Unlike most traditional forms of transnational crime, cyber-criminals can commit offences in or through a country without ever actually going there themselves. This means that only a few countries not having such legislation will allow for safe havens and prevent a successful fight against cyber-crime at the international level. Not only will this be damaging for the countries that might be impacted by such crimes, but those countries being used as safe havens might also be challenged in their capacity to benefit from the widespread advantages of computer networks such as the Internet. Even those countries in which the high technology

[36] Four non-European countries participated in the negotiation of the Convention and are in the process of ratifying the treaty: Canada, Japan, South Africa and the United States.

[37] The model law can be found on the Legal and Constitutional Affairs Division of the Commonwealth Secretariat's web pages at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf.

sector does not play as an important role as in developed countries need to realize that their economy, which is linked to the provision of essential services such as postal or banking services, air traffic control and critical infrastructure protection, might possibly be impacted by such crimes.

Developing adequate substantive offences requires focusing on the domestic legal framework at the outset, taking into account legal traditions. A "one size fits all" solution will not work. Rather, the solution lies in the harmonization of national legislation to ensure that while countries keep their national specificities, they will still be able to provide cooperation to one another at the international level. A good approach is to develop a list of elements, which must be addressed in an offence or group of offences, and to use such a list as the outline for legislative drafting in accord with national practice.[38] National legal perspectives may vary, but the illicit conduct to which they are addressed is usually consistent from one country to another, particularly with cyber-crime, where *modus operandi* can be shared by e-mail. Another important principle in drafting substantive offences is to ensure that these offences will not become obsolete as ever-newer technologies are rolled out. While laws need to be continually reviewed to ensure their relevance to the changing environment, they should be drafted as much as possible in technology-neutral language that will stand the passage of time.

Substantive offences also need to be drafted bearing in mind that countries will not wish to criminalize conduct if it is done for legitimate purposes. For example, a person protecting his or her computer against cyber-attacks might be willfully intercepting private communications in that context. A computer professional might equally be breaching the law if she produces or possesses security devices that could also be considered as being devices designed primarily for the purpose of committing a computer crime. If the offence is not specific in providing for an express requirement that the conduct is done without right, such provisions could be overbroad. Finally, because of the nature of computers and the possibility of persons interfering with or accessing data with lawful authority to do so, all substantive offences should require a clear criminal intent for criminal liability to apply.

b) The offences[39]

Most countries today have understood the necessity of being able to prosecute crimes committed with the assistance of a computer, whether that crime was committed with a computer as a tool, a target or a storage device.

In order to respond to the use of computers as **tools** in the commission of offences, states might not be required to enact legislation if the conduct prohibited by the specific offence is criminalized regardless of whether or not the offence is committed with the use of a computer. For example, countries wishing to address the growing problem of child pornography on the Internet will want to make sure that their offences of distributing, making, printing, distributing and importing are equally applicable in that context. In Canada, although the latter offences did not require any modifications as they were equally applicable to a paper world and to data, the government believed that the creation of new offences of "transmitting", "accessing" and "making available" child pornography were required to bring the offences up to speed with new technologies, in particular the Internet.

[38] Increasingly, the principle applied in international cooperation is that where dual-criminality is required at all, it is the underlying conduct or basic elements of the offence which must correspond, and not the mere form or drafting of the offences in each country. See, for example, *United Nations Convention against Corruption*, GA/RES/58/4, Article 43, paragraph 2.

[39] For a range of typologies and descriptions of cyber-crime offences, see: Piragoff, D. K., "Computer Crime and Other Crimes against Information Technology in Canada", in International Review of Penal Law, Association internationale de droit pénal, 1993, p. 201; Grabowski, P., "Computer Crime: A Criminological Overview", 1(1) Forum on Crime and Society, United Nations Centre for International Crime Prevention, February 2001; Charney, S. and Alexander, K., "Legal Issues in Cyberspace: Hazards on the Information Highway" 1996 45 Emory L.J., pp.931-957; O'Neill, M.E., "Old Crimes in New Bottles: Sanctioning Cybercrime", 2000, 9 Geo. Mason. L. Rev. pp.237-88; Sieber, U., *The International Handbook of Computer Crime* (English Edition), Wiley, N.Y., 1986; and United Nations, "Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime", Report of the Secretary General to the Commission on Crime Prevention and Criminal Justice at its Tenth Session, E/CN.15/2001/4, 30 March 2001.

Another significant modification in relation to "communication offences" such as those related to child pornography and hate propaganda might be necessary in order to allow for a court to delete illegal material from a website situated within its jurisdiction, as courts are currently able to do when they order the forfeiture of illegal material. While this does not prevent the same material from appearing in or from another jurisdiction if that other jurisdiction does not have similar legislation, it is a step that will contribute to better fighting cyber-crime. Once again, it is worth repeating that it is only if all countries work together in harmonizing their legislation that any successful fight against cyber-crime will succeed.

Traditional offences such as theft, fraud and forgery might also require some amendments if they are only applicable to tangible documents. While the national concepts of such offences may differ significantly from one country to another, legislators should at least ensure that these offences will apply in the context of computers and computer networks.

The problem in relation to dealing with the use of computers as **storage devices** may be more one of human and financial resources than one that needs to be addressed through legislative amendments. As mentioned earlier, a number of countries already have legislation dealing with electronic evidence or data. Models have also been developed by regional organizations, such as the Commonwealth *Model Law on Electronic Evidence*[40].

Addressing the problems of computers being the **targets** of crimes has required creativity by lawmakers since crimes against the integrity, availability and confidentiality of computer systems are complex, of a technical nature and somewhat different from traditional crimes in which a person suffers harm or damage. Both the Council of Europe *Convention on Cyber-crime*[41] and the Commonwealth Model Law entitled the *Computer and Computer Related Crime Act*[42] propose the creation of offences relating to illegal access, interfering with data, interfering with a computer, illegal interception of data and offences related to illegal devices.

Procedural legislation

a) The principles

The second step in the fight against cyber-crime is to ensure that the appropriate procedural powers are in place at the domestic level. This is essential both to ensure that domestic law enforcement officials have the powers they require to conduct domestic investigations and to ensure that they are able to take many of the same steps for purposes such as tracing criminal communications and to preserve, obtain and transmit electronic evidence when requested to do so by another country. One major problem with implementing these powers is related to the nature of computers in general and of the Internet in particular. Before the advent of computers, most criminals were returning to the scene of the crime. Today, not only does the person committing a computer crime rarely return to that scene but, in most cases, that person will not even have been close to the place where the crime was committed. That person might be in another town, country or continent. Having in place adequate powers to allow investigators to follow the electronic tracks of a criminal is essential, and in no area of investigation is inter-operability between the national systems of different countries more important. Old legal tools will almost certainly have to be modified, entirely new ones may have to be created, and consensus among States as to what ought to be done and how, is, if not essential, then certainly a major advantage.

Not only do domestic authorities have to be able to trace the trial of a criminal, but they must do so in a timely fashion. The volatility of data and its intangible and transient nature lies at the heart of the problem. Law enforcement authorities need to have the tools necessary to find and safeguard the evidence of a crime, whether it is of a tangible or intangible nature. Electronic evidence can usually be destroyed at the touch of a

[40] Commended by Law Ministers in 2002, it adopts system reliability as the basic test for admissibility of evidence and adapts general rules of evidence to meet new technological possibilities.
[41] See articles 2 (illegal access), 3 (illegal interception), 4 (data interference), 5 (system interference) and 6 (misuse of devices).
[42] See articles 5 (illegal access), 6 (interfering with data), 7 (interfering with a computer), 8 (illegal interception of data) and 9 (illegal devices).

keyboard. A related problem is the fact that communications can easily be – and frequently are – routed through many countries between source and destination, and such is the nature of the Internet that fragments of the same communication may even have taken different routes. Communications must often be traced back through many countries, one after another, quickly enough that electronic traffic data is not automatically erased before the tracing can be done.

b) The powers

The basic investigative powers need to be revisited by national authorities in order to make sure that they can be resorted to in the context of computer crime investigations and prosecutions. In countries where limits on the scope of a search for evidence are subject to strict limits as a procedural safeguard, these may have to be reconfigured or broadened to ensure computer systems can be searched effectively. For example, the traditional power of search and seizure might require a number of modifications to ensure that the place to be searched can include a computer system. When a network of computers in different cities is searched, at what "place" is the search conducted? What are the limits to be included in national legislation and how should such limits be dealt with at the international level? Should a domestic search power allow for a search in a territory outside the jurisdiction of the judge issuing the search warrant in circumstances in which the data is available through the computer system located in that jurisdiction? While sovereignty concerns might be raised depending on the way in which these questions are answered, on the other hand, some of the criticism addressed to current mutual legal assistance procedures might be alleviated.

Another problem from a law enforcement perspective arises from the complexity of computer systems, the volumes of data that they may contain, and the increasing prevalence of security measures to protect privacy and prevent unauthorized access to data. These factors have led a number of countries to adopt legislation to compel those in control of computer systems to use the systems themselves to search for and identify the target data, to produce it and to transfer it to those authorized to order its production, usually in a form in which it can be read and produced as evidence. Usually referred to as production orders,[43] such powers have previously been enacted in a number of countries to allow for the obtaining of physical records. Countries already having such legislative powers in relation to physical documents might want to look at them again to make sure that the production orders can also be used to compel custodians to produce data and that the courts issuing such orders will do so under thresholds appropriate to the nature of the data or documents produced. For example, an order requiring a service provider to produce the information needed to identify customers or subscribers (subscriber information)[44] or the traffic data needed to trace a communication might be issued at a lower standard than an order requiring the production of the actual content of the communications involved where these can be considered as private correspondence.

The interception powers that were drafted for analog telephones equally need to be looked at to ensure that they are applicable to the real-time tracing of content or traffic data on computer networks. Court authorizations need to be reconsidered to ensure that they can be obtained for both content and traffic data under appropriate standards reflecting the different expectation of privacy that persons have in relation to these two types of data. What also needs to be revisited is whether the "list approach" that a number of countries have adopted in relation to the interception of the content of private telecommunications is also applicable in the context of computers. The "list approach", which entails that court authorizations to intercept private communications can only be issued in relation to serious offences or offences punishable by certain maximum sentences of imprisonment, might need to be set aside in relation to the real-time interception of traffic data, especially since the full range of offences involved may not be apparent until after the opportunity to intercept has passed. The fight against cyber-crime requires that investigations be carried out in a timely and effective manner. As was mentioned earlier, it is more and more common that data contained in a computer may afford evidence of a number of types of crimes and not only evidence in relation to computer and computer related crimes. In addition, the privacy interests at stake in relation to traffic data are not as high as in relation to content data. It is important, therefore, that states ensure that

[43] Council of Europe *Convention on Cyber-crime*, article 18; *Commonwealth Computer and Computer Related Crimes Act*, article 15.

[44] An interesting definition of subscriber information may be found in article 18(3) of the Council of Europe *Convention on Cyber-crime*. It can generally be described as the name, billing address and phone number of the customer, as well as the name of the service provider.

traffic data can be readily accessed following the obtaining of a court order issued under an appropriate standard in order to allow for the investigation of all criminal offences and not only the most serious ones.

In both the context of search and seizure and interception orders, countries might also want to consider how the assistance of third parties can be compelled. Assistance orders may be issued where a third party's assistance is reasonably required to give effect to these orders. The scope of such orders might need to be spelled out more clearly in order to deal adequately with challenges such as encryption or the provision of passwords, bearing in mind human rights, such as the right to be protected against self-incrimination.

Another important tool is the preservation order[45], which deals with the fact that data is particularly vulnerable to loss or modification. Typically, this procedural mechanism allows for the immediate safeguarding of stored data or documents in the control of the custodian, usually a service provider, in cases where law enforcement officers believe that such documents or data are relevant to a specific investigation or proceeding. Such a power, which should not be confused with data retention[46], is a "do-not-delete" order that will require the custodian of documents or data to save documents or data they currently have. The order is temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a search warrant to seize the data or documents or a production order to deliver the data or documents. This is a stop-gap measure to ensure that information vital to a particular investigation, but that could have been deleted because of normal business practices, is preserved before the appropriate court order is obtained.

Combined with the preservation order is another measure aimed at ensuring that a communication may be traced back to the initial service provider. This measure, the expedited preservation and partial disclosure of traffic data, allows law enforcement authorities to request the disclosure of enough traffic data to be able to trace back all the service providers that were involved in the transmission of data[47]. This measure is one of the pre-requisites for adequate international cooperation since service providers located in several jurisdictions is the norm rather than the exception.

International cooperation

a) The principles

Two pre-requisites are necessary for international cooperation to occur. First, as mentioned earlier, no international cooperation can occur without having in place, at the domestic level, the appropriate substantive offences and procedural powers. Second, the harmonization of domestic laws of different countries and the establishment of a legal framework on which cooperation can be requested and delivered is also essential. Harmonization of offences is needed for both mutual legal assistance and extradition where dual criminality is a requirement. An international legal framework (which may be multilateral, bilateral or even case-specific) provides a basis on which all of the countries involved play a role in determining whether the domestic legal requirements of the various countries concerned have been met.[48] Once these two pre-requisites are taken care of in domestic legislation, international cooperation is possible. Most often, international frameworks take the form of treaties or agreements, which cover a general range of subject matter, but increasingly, as with domestic legislation, these may have to be adjusted to take account of the unique nature of cyber-crime.

b) The powers

The two main mechanisms that need to be looked at in order for a country to be able to contribute to the fight against cyber-crime at the international level are mutual legal assistance and extradition. Mutual legal

[45] **Council of Europe** *Convention on Cyber-crime*, article 16; *Commonwealth Computer and Computer Related Crimes Act*, article 17.

[46] Data retention is a general requirement that could compel service providers to collect and retain a range of data concerning all of its subscribers. See the interesting discussion contained in paragraph 151 of the Explanatory Report to the Council of Europe *Convention on Cyber-crime*.

[47] Council of Europe *Convention on Cyber-crime*, article 17.

[48] Extradition, for example, will be a matter for the courts of the State in which the offender is located, but extradition treaties, agreements or arrangements provide the basis for another State to request the extradition and to provide evidence or information needed to justify the extradition.

assistance and extradition may be governed either by a treaty, an agreement or an arrangement. Treaties or agreements can be of general application (e.g., the *United Nations Convention on Transnational Organized Crime*) or subject specific (e.g., the Council of Europe *Convention on Cyber-crime*). The Council of Europe *Convention on Cyber-crime* provides for a hybrid scheme in relation to international cooperation[49]. While the Convention may serve as the basis to make requests if there is no existing treaty or to supplement provisions of existing treaties, existing treaties and arrangements take precedence. Such a scheme was believed to be important to states that negotiated the *Convention* since all states tailor their bilateral relations to take into account particular sensitivities or safeguards.

In order to fight cyber-crime, states have to find ways to provide for timely and efficient mutual legal assistance to the widest extent possible. Obtaining access to the legal investigative powers of another state is crucial to that goal. As mentioned earlier, the types of substantive offences for which mutual legal assistance should be granted are not only those related to the availability, integrity and confidentiality of a computer system, but any crime where computers can be used as storage devices for or repositories of evidence of any crime. The same principle applies for the procedural powers: international cooperation should be possible not only for the investigations or proceedings of computer and computer related offences, but also for the collection of evidence in electronic form of any crime[50].

A few words need to be said in relation to some of the possible modifications that need to be made for a state to be able to provide adequate mutual legal assistance in the context of cyber-crime. First, in relation to preservation orders for stored content or traffic data, which are probably even more important tools at the international than the national level, states should endeavor to remove their dual criminality requirement as it would be counter-productive to the timely investigations of cyber-crime. If such a requirement cannot be forborne in the context of cyber-crime, it should be saved only for the more intrusive investigative measures, such as searches or the interception of private communications. In addition, states should endeavor to better cooperate with each other in both the real-time collection of traffic data, as well as the interception of content data. Obviously, this requires a more profound rethinking of fundamental values as most states do not currently allow mutual legal assistance mechanisms in relation to these latter types of intercepts. Once again, it is the timeliness of such cooperation that will allow states to fight cyber-crime.

Mutual legal assistance mechanisms will not be sufficient, however, for states to successfully fight cyber-crime. While such mechanisms are useful to collect evidence and assist in identifying criminals, the prosecution and punishment of such persons may require the extradition of the fugitive to the state that has the jurisdiction, the means and the will to prosecute. Extradition schemes must therefore be reviewed to ensure that all computer and computer-related crimes are considered to be extraditable offences. In countries where a *de minimus* threshold applies to extradition cases (usually by excluding offences punishable by less than one year) substantive offence and sentencing provisions should ensure that the basic computer and computer-related crimes meet these requirements. For the States Parties to the Council of Europe *Convention on Cyber-crime*, such offences are deemed to be included in any existing treaties or other extradition arrangements.[51] Consideration could also be given to ensuring that maximum punishments are four years or greater, in order to trigger application of the *United Nations Convention against Transnational Organized Crime*, where the other triggering requirements are present.[52]

—

Conclusion

Information and communications technologies have tremendous potential benefits. Most countries have come to recognize this, and the acquisition and deployment of such technologies has become a key element of development strategies around the world. The extent to which they are present and available in a country has even become an important indicator of development.[53] Not all of the effects of the technologies are of a positive nature, however, and gaps in distribution and availability have prompted calls from the United

[49] Articles 23 and following.
[50] See Council of Europe *Convention on Cyber-crime*, article 25(1).
[51] See article 24.
[52] Apart from the punishment requirement the major condition is the involvement of an organized criminal group as defined by the Convention. See *United Nations Convention against Transnational Organized Crime*, GA/RES/55/25, Articles 2 and 3.

Nations to bridge the "digital divide"[54]. However, all countries have or will in the not so distant future feel their impact for better and for worse.

Given the projected growth of the Internet and its number of users and the corresponding expansion in the use of new technologies and the Internet to commit crimes, cyber-crime has proven a formidable challenge to all states, including even the most developed States, in which the companies, which develop and market the technologies are located. It also poses a very serious challenge to the efforts of less developed countries as well in terms of accelerating the delivery of health care, education, electronic commerce and the like as part of their development strategies. For this reason, a number of countries, as well as international and regional organizations, have been addressing the challenges posed by the emergence of computers and the Internet through the development of model legislation, technical assistance in drafting legislation, training of law enforcement officers, legislative drafters and policy makers and the establishment of links between governments and industry.

As mentioned earlier, the G8 has been active in this area mainly by adopting principles, recommendations and statements in relation to various aspects of high-tech crime[55] and in promoting a 24/7 network of law enforcement cyber-crime units. Following the adoption of its model law entitled the *Computer and Computer Related Crimes Act* in 2002, the Commonwealth Secretariat has held training seminars for drafters and policy makers to assist them in developing national legislation on this issue. The Organization of American States (OAS) is developing an integral OAS cyber-security strategy and will be holding regional legislative drafting workshops on cyber-crime. The Asia-Pacific Economic Cooperation (APEC) is currently conducting a capacity-building project on cyber-crime for member economies in relation to legislative frameworks and investigative capabilities. APEC economies that are advanced in this respect will assist other member economies in developing legislation and forensic training. Finally, the United Nations has also adopted a number of resolutions on this issue over the last fifteen years[56] and, within this forum, some Member States have been putting forward the idea of developing an international convention on cyber-crime over the next few years.

The idea of developing an international convention on cyber-crime as a solution to the challenges faced by the international community as a whole in dealing with cyber-crime is interesting in many respects. While this discussion goes well beyond the scope of this paper, a few elements can be pointed out. On the one hand, the steady increase in global access to the Internet and the resulting equally steady increases in cyber-crime can be expected to increase pressure for a concerted international effort, including some form of international legal instrument as the basis or framework for such action. On the other hand, serious technical and legal problems will need to be addressed before such an instrument can be developed.

First, developing countries would have to be assisted in raising standards for technical security and investigative techniques from an operational perspective as such techniques may raise security concerns on the part of other governments, and in some cases concerns about economic interests and proprietary technologies among the companies which produce the technologies and the countries in which they are based. Second, human rights standards in areas such as privacy and the legal rights of persons facing

[53] See, for example: "OECD Science, Technology and Industry Scoreboard 2001 – Towards a knowledge-based economy", http://www.1.oecd.org/publications/e-book/92-2001-04-1.

[54] United Nations General Assembly, *We the peoples: the role of the United Nations in the twenty-first century,* A/54/2000, 27 March 2000, paragraphs 150 to 167.

[55] *Principles and Action Plan to Combat High-Tech Crime*, 1997; *Principles on Transborder Access to Stored Computer Data*, 1999; *Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations*, *Principles on the Availability of Data Essential to Protecting Public Safety*, *G8 Statement on Data Protection Regimes and Data Preservation Checklists*, 2002.

[56] *Plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century,* A/RES/56/261, 15 April 2002, Part XI (Action against high-technology and computer-related crime); *Combating the criminal misuse of information technologies,* A/RES/56/121, 23 January 2002; *Combating the criminal misuse of information technologies,* A/RES/55/63, 22 January 2001; *Computer-related crimes,* Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 1990. Two very interesting reports of the Secretary-General presented to the United Nations Commission on Crime Prevention and Criminal Justice also need to be pointed out: *Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime,* E/CN.15/2001/4, 30 March 2001 and *Effective measures to prevent and control computer-related crime,* E/CN.15/2002/8, 29 January 2002.

criminal prosecution would have to be rationalised to support some of the closer forms of cooperation, such as cross-border or cooperative search and seizure operations, for example. An obvious related issue in this respect is how are sovereignty concerns addressed. Third, while an instrument, such as the Council of Europe *Convention on Cyber-crime,* is opened to non-European Member States, some countries may find that such an instrument does not suit their needs or specific circumstances. On the other hand, developing another international treaty will take time to negotiate in view of the different legal systems, stages of development and cultural backgrounds.

While the resolution of some of these issues is clearly not an immediate prospect, this need not delay work in all areas. Before work on a global legal instrument can begin, capacity-building efforts can be undertaken to ensure that when time is ripe for an instrument is be developed, all countries will have the expertise needed to implement it. -
The format used for the *United Nations Convention against Transnational Organized Crime*, in which core elements were included in a parent Convention, with additional specific crime problems dealt with in supplementary Protocols, also suggests a possible solution to some of the problems. It might equally be possible to develop a group or cluster of instruments, beginning in areas where consensus is possible, and supplementing this with further provisions in additional instruments later on. Much the same approach has been taken with respect to anti-terrorism treaties, with a series of specific treaties on subjects such as terrorist bombing and financing successfully concluded in the absence of any immediate consensus for a comprehensive treaty on terrorism.

Whether it takes the form of the Council of Europe *Convention on Cyber-crime* being ratified by an important number of developing and developed states or an international convention negotiated within the United Nations, an international consensus is required on how all countries have to work together to fight cyber-crime. No government can afford ignoring these emerging crime trends or work in isolation in adopting domestic laws to deal with them. The new reality that we are facing today has changed forever the world we live in and we cannot afford to fight 21st century crime with tools put in place some centuries ago. This requires a new way of thinking and a challenge to the rights and freedoms that are more and more taken for granted. The impossibility of achieving one way or another an international consensus on how to deal with cyber-crime will jeopardize one of the most important tools for sustainable development.

In a nutshell, States need to react and start thinking more creatively. Not only does their national legislation need to be revisited regularly to ensure that they have the proper substantive offences and procedural tools in place to fight cyber-crime, but they also have to work together at the national and international levels with all stakeholders, including industry, in ensuring that the proper tools are in place to allow for more efficient and timely ways of providing international cooperation.

As was mentioned by the Honourable Anne McLellan, former Minister of Justice of Canada, at the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders[57]:

> *"There are no simple solutions. Any effective solution will attack beliefs, which are fundamental to both countries and individuals. This is the key difficulty in developing practical and useful solutions to cyber-crime. The underlying reality is that any legislative measures we adopt, whether domestically or internationally, will have to involve a re-thinking of our basic notions of sovereignty, human rights and privacy. While it is imperative that we continue to protect all those rights, we must also recognize that our current notions were formed in a context that is much different from the world in which we live today.*

The landscape in which law enforcement now operates when investigating computer-related crime looks quite different from that of the past. We therefore have to adapt our laws and our deeply entrenched notions to accommodate this new reality. Without dispensing with our time-honoured conceptions of human rights and sovereignty, we must find a way to adapt these notions to a new environment so that they apply to the world in which we currently live.

[57] Speech delivered on April 15, 2000, in Vienna (Austria) at the Computer Crime Workshop. The speech may be found at http://canada.justice.gc.ca/en/news/sp/2000/doc_25311.html.

In addition to creativity, our new challenges require courage. Courage to re-think our firmly held assumptions about how the world and our legal systems must operate, and courage to forge ahead with the bold steps necessary to confront the challenges facing us this new age. With creativity and courage, we can eventually overcome these challenges, make the Internet safe and preserve our basic freedoms and values."

And this is what the fight against cyber-crime is all about.

Giuseppe BUSIA
Officer, Department of Communications and Telematic Networks,
Personal Data Protection Authority of Italy

Relationship between security and human rights

**Privacy and investigative exigencies:
progressing from incompatible to complementary positions**

by Giuseppe Busia[1]

Relationship between security and human rights…...1
Privacy and investigative exigencies:
progressing from incompatible to complementary positions……1

1. The right to anonymity as a right to liberty……2
2. Risks and opportunities linked to the development of new technologies…….3
3. Limitations to the concept that the acquisition of more information will necessarily assist investigations……5
4. The legislative response regarding personal data and the duties imposed on the police authorities……6
5. The regulation of specific categories of personal data……..6
   5.1 Electronic traffic data……6
   5.2 Data on location……9
   5.3 Video-surveillance and biometric analysis……..10
   5.4 Genetic data……11
   5.5 Security v. rights

All too frequently, security and the protection of human rights are presented as alternatives, being considered as mutually incompatible and therefore mutually exclusive objectives. Such a schematic proposition, however, is not one with which one can agree, since in a system calling itself democratic, the exigencies of security must necessarily be reconciled to the demands of basic human rights. As a result, one must advance from the idea of contrasting standpoints to an essential and incontrovertible where each such element complements the other.

Therefore it is in this light that one will endeavour to underline how, in particular, such an objective can (and must) be pursued with full respect for that detailed and intricate complex of rights which has now come to be grouped under the general umbrella of the protection of personal data.

The same rights, as well as being safeguarded as a Constitutional asset under Italian domestic law (as the Constitutional Court has regularly confirmed) have also been hallowed in the European Union in its Charter of Basic Human Rights (Arts. 7 and 8). Above all, these rights serve to

categorise our system as a democratic one, helping us to avoid the pitfall of believing that everything that it is possible to do will thereby become both lawful and morally acceptable.

In the following pages, after taking a look at the risks to the individual arising form the acquisition of personal data and the employment of new technologies, we will indicate some of the limits inherent in the idea that the collation of more information will necessarily assist investigative activity. We will thus refer to the principal juridical safeguards contained in the legal regulations on personal data, especially in the limits prescribed for their handling for the purposes of the police authorities, and we will look in particular at certain specific categories of information utilised in the course of investigations. Finally, we will examine international experiences in the field of co-operation in the interests of security, which may be recognised as a valid instance of how it can be possible to balance and reconcile the needs of security and the needs to safeguard fundamental human rights.

1. The right to anonymity as a right to liberty

In this connection, it is often necessary to recognise that whenever data on an individual is acquired and stored, even with the best possible and incontrovertible intentions, such as the prevention of crime and the preservation of security, this sphere of liberty is to some extent inevitably infringed. Indeed, if one knows something about another person, the possibility is lost of such information falling into oblivion, even if, for example, that person has changed profession, mode of life, attitudes, habits, ideas, etc: he loses the possibility of hiding it, even when he is intent on reconstructing his own identity on the basis of a new and different personality (the right to anonymity). In consequence, he loses some part of his freedom of personal choice and self-determination.

Being a prisoner of one's past means losing hope of ever changing or improving oneself: one thinks of the prostitute – I refer to actual cases without of course giving real names – who, having freed herself of those exploiting her, began to work in the world of show-business and achieved a certain reputation there, yet all the time had her past thrown in her teeth as an obstacle to her career advancement. And it is the same for so many women with similar experiences, for whom the past simply represents an obstacle to making a new life for themselves out of the limelight, building a family and re-establishing and identity so as to forget and cause to be forgotten a less happy phase of their existence.

One thinks also of those who have committed crimes, then paid their debt to society, reintegrated themselves in the world of employment and genuinely wish – as society has the duty to wish and to encourage – not to meet great impediments in their progress as a result of continuing reminders of their past. In the face of such cases, one has to ask how much the, albeit necessary, conservation and accessibility of their criminal record can assist the attainment of the aim of the fine provision in the Constitution – one of its most attractive ones because it is full of optimism for the individual – whereby the sentence served by the wrongdoer should look to his useful re-education (Art.27)

Often, as a result of the traces that we leave from an increasing use of electronic devices, we restrict our own freedom by putting others in a position to know more about us that we are able to anticipate. One thinks – relating once again an actual episode – of the young person participating in one of the many Internet chat-shows who uttered, simply in jest and without real intent, certain political opinions. Well, some years later – after he had completed his studies and in all probably acquired different views – he had to undergo an interview for work in which his interviewer, after having examined his *curriculum vitae*, had the idea of consulting one of the many research engines on the Net in which he found the subject's electronic address and discovered the opinions that he had expressed so many years earlier. Leaving aside the question of the legitimacy of the interviewer's conduct, this episode shows how the conservation for a long period of personal information, perhaps even inadvertently, comes to represent a crucial element in the individual's life: simply because others have free access to such data; he is haunted by the ghosts of his past and so suffers a diminution of his personal liberty.

The legal system is not always able to make proper provision for such situations. Sometimes it gives just partial protection, being obliged to balance the yearning for anonymity with the other rights belonging to other individuals or society at large. However, it is incumbent upon everyone – beginning with those who work in the field of public security – to remember always that the mere conservation of personal information regarding an individual can have repercussions upon that person's life. So it should lay down that personal data should be gathered and retained only so far as pertinent, to the extent necessary and in accordance with the principles of proportionality – in other words, only so far as really vital for achieving aims that are appropriate and in cases where it is not possible to reach the same objective without resorting to personal data or by using less invasive techniques.

2. Risks and opportunities linked to the development of new Technologies

Technological development increases exponentially the possibility of collecting and storing personal data regarding individuals. Indeed, there is a growth in the *number of data-banks* and their *inter-connexions*, both in the public and private sectors: one thinks, on the one hand, of the creation of a unified network in the field of public administration, which is surely opportune, in order to facilitate and enhance the quality of dealings with citizens, and on the other hand of the growing number of centralised private indices in which information is collected on the records of debtors and those seeking loans or extended credit.[2]

At the same time there is an increased *memory capacity* for information in such electronic archives, enabling more and more personal data to be stored for ever longer periods of time. Together with the availability of increasingly rapid and sophisticated *research and indexing* facilities, this assists the identification of subjects and the revelation of ever greater information about them.

It is also becoming easier to gather personal data *without the subject being aware of this*: one only has to think of *cookies*, the small pieces of software which are downloaded on the user's equipment the moment he visits given pages on the web. Some of these are necessary to ensure a functional utilisation of the sites in question, but others collect a great deal on information on those surfing the net, with particular reference to the sites visited and thus to the tastes and interests of the people involved.

Finally, there is an increase in the *economic advantages* of collecting and handling data. The technologies have in fact made cheaper – and thus more widespread – certain forms of intrusion into the private lives of others: one only has to think of the phenomenon of "spamming", which has attained such dimensions as to prompt legislative intervention to contain it, even in countries like the United States, which hitherto had thought it possible to rely solely on the "invisible pressure" of market forces to deal with such problems.

All this inexorably brings about an increase in our vulnerability, not only with reference to the appearance of new offences, which are specifically based on the use of such technologies (one thinks of the so-called *computer crimes*) but – in the area which interests us – also with the widening diffusion of the so-called "identity thefts", tied to the fact that we are increasingly being represented not in terms of our true identity but by identifying codes and signs transmitted on the electronic communication networks, which can be duplicated and used improperly by third persons to the detriment of the people to whom they refer or belong.

In general, therefore, we are witnessing a comprehensive increase in the risks tied to the improper use of data-banks, which inevitably reflects on investigative activities, both in regard to the use of various data-banks existing for the use of the police authorities and to the creation of electronic archives dedicated to security purposes and the repression of crime.

The unremitting advance of new technologies clearly presents an opportunity of which our society should take full advantage. The diffusion and constantly increasing use of them by the various categories of user, overall, is a symptom and consequence of the development, even in terms of democracy, of our society.

Yet, even in this case, it is always essential to recognise that, potentially at least, the more sophisticated such technologies become and – in parallel – the more useful they are in simplifying daily life, the more their utilisation leaves its electronic footprint: data showing when a given service has been used, for how long, for what reasons, in what location at which time, in inter-connection with what other subjects through the same instrument, etc.

The totality of such information, even when apparently detached and non-invasive, still reveals much about the relationships resorted to by an individual. If then, the data is stored for a long period – as is permitted at ever lower cost by these technologies – it becomes possible to construct the whole network of an individual's social relationships over a period of time, exceeding even the extent of which the subject himself is or can be aware.

These considerations also apply to those systems which purport to preserve the anonymity of the users, as with various services offered in the electronic communication networks. On the contrary, such services nearly always will permit the identity of the users to be discovered. This will happen unless one uses particularly cunning or sophisticated technologies, such as those employed by people with special reasons for remaining anonymous – perhaps because they are committing or intending to commit crimes.

3. Limitations to the concept that the acquisition of more information will necessarily assist investigations

We now come to one of the paradoxes that we must confront, which supports ever larger collections of personal information for the purpose of preventing or repressing crime: in the very largest archives of information, data on all citizens come together…including people with greater interest than others in not being included, because they are more concerned to avoid such inclusion, in particular those who have committed or intend to commit crimes.

Moreover, one must remember – as the organs responsible for protecting public security increasingly recognise –that indiscriminate acquisition of data, apart from being in excess of the desired objectives (and thus in violation of the principles set out above) do not always bring any advantage for the police. In fact, very often an excess of information imports a reduction in its quality and delays achieving success in the investigative operation, even when such indiscriminate collections do not hide deficiencies in the investigative process.

Finally, it is always necessary to consider that the collection and storage of data for long periods of time incurs very high costs, which – directly or indirectly – represent a burden on society, whether through the burdens imposed on businesses, which are passed on to the users, or through the costs charged to the public, which are ultimately borne by the taxpayers

What mostly interests us here, it that we must certainly accept that progress in technology creates important opportunities, with specific reference to their use for investigations, determining a quantitative and qualitative increase in the instruments available to operators in this field. Yet it has to be noted not only that such use must always conform to the limits imposed by law for the protection of personal data but also that, simply because of its expansion, its efficacy may be reduced in achieving its objectives.

4. The legislative response regarding personal data and the duties Imposed on the police authorities

These risks have been met by the regulations for the protection of data by a series of measures, which not only seek in general to prevent third parties from trespassing into the private life of individuals, according to the traditional concept of privacy, i.e. the right to be left alone. They also allow a decision on what use others may make of data concerning them, choosing not only whether a third party may have access to given items of personal information, but also the purposes for which it can be used, how long it can be stored, to whom it may be communicated, etc. The protection of data has become in this way a right of informational self-determination, gathering under its umbrella a growing number of rights, which, in the name of protecting the person and personal dignity, embrace and thereby enhance traditional rights, such as those of personal identity, and of the representation or freedom of manifestation of personal opinioons. Thus it acquires its own autonomy, which has been hallowed in a series of Constitutional texts, culminating in the European Union's Charter of Fundamental Human Rights.

The laws of the EU and Italy rest on certain fundamental forms of protection – referred to above – which are fully applied even in relation to the police authorities and more generally to everyone engaged in the maintenance of security. These are the principles of pertinence (the police may only gather and store data relevant to their investigations), degree (data collected may not exceed what is necessary), reasonableness and due proportion between the objective and the mode of attaining it.

Further: since the police forces, unlike the rest of the community, are not obliged either to inform those interested of the fact that they are using data concerning them or to request their consent, and indeed are able to use personal information with many fewer restrictions (see Art.53 et seq. of the Code regarding the protection of personal data, Legislative Decree of 30th June 2003,No.196 and then the Privacy Code), it is essential that they adhere to the above-mentioned principles with particular rigour.

In fact, even the minor controls which any interested party may take over their operation – because, *inter alia*, of the permitted lack of notification and freedom from obtaining the consent of the subject – impose a particular "auto-control" in the grading of data to be obtained, in determining the periods of retention and in identifying individuals who may be subject to the totality of information from time to time considered necessary.

5. The regulation of specific categories of personal data

Having set out the foregoing considerations of a general nature, we should now concentrate on the specific disciplines for certain types of personal data of special importance, which are often used by the forces charged with the maintenance of public security, so as to show how the principles enunciated have been operated in the particular regulation of various classes of data.

5.1 Electronic traffic datas

Because of their intrinsic importance and the controversies regarding their regulation, we should begin with data concerning telephonic and tele-communications traffic. The Privacy Code, following the letter of Directive No.58 of 2002 to which it gives legal force, considers as traffic data "any data handled in transmitting a communication on an electronic network of communication or billing the same". Therefore, it provides a very broad definition, which derives from the most recent EU Regulations. These, recognising the growing convergence between instruments such as telephones, computers and televisions, have adopted a "technologically neutral" approach and – with the exception of certain details – tend to provide a common discipline for all electronic communications regardless of the terminal equipment used to effect them.

For this, data on electronic traffic includes not only telephony from fixed or mobile terminals (through which "calls" are achieved, i.e. the connections establishing bilateral communication in real time: see Art.4, para.2(b) of s.Igs.196/2003), but also other types of electronic communication, particularly fax, sms, mms. and e-mail.

Before describing the regulation of these, a basic clarification is needed: data on electronic traffic do not contain the content of conversations of messages but only certain "external" information, such as the numbers or addresses of electronic mail, including the fact of the communication and the time it occurs. So then, it will be asked: what is the risk in the acquisition and storage of these? In reality, when one puts together information on the numbers called by an individual, it is possible to assemble a network of his personal and social relationships. By establishing the frequency and length of communications, and whether they occur at any time or merely during office hours, one can identify the type of relationship existing between the communicating parties.

For this reason, the Constitutional Court, well before the coming into force of the legal provisions on personal data, unequivocally recorded how "….the extent of the safeguard for communications contained in Art.15 of the Constitution…. comprises not only the secrecy of the content of the communication but also the identity of the subjects and references to the time and place of the communication itself" (Decision no.18 of 1993).

For the same reason, as we have said, such information is regulated by a series of specific provisions, both in the EU Directives and in the Italian legislation giving effect to them. The Privacy Code provides in general terms, in fact, that data on electronic traffic must be cancelled or rendered anonymous when no longer necessary for the purposes of transmitting an electronic communication (Art.123). However, the provider of services is authorised to handle information that is strictly necessary for invoicing and payments for a period not exceeding six months, excepting the further specific retention that is required for court proceedings. A further handling is also permitted to the extent and for the period necessary for promoting electronic communication services or providing added value services, but this is subject to the consent of the subscriber and user, which may be withdrawn at any time. All this is also covered by specific safeguards concerning both the information to be given to the interested parties and certain limitations to the access to such information on the part of people working for the service provider[3].

Apart from the handling that is necessary under the terms of a contract, the Privacy Code laid down – and this is of particular interest – that only data relative to *telephonic* traffic (and so excluding all other communications on telecoms networks) may be retained by the provider for two and a half years for the purpose of discovering or repressing criminal activity within the terms of a Ministerial Decree adopted on a Declaration in accordance with the Authority (Art.132).

In the endeavour to broaden the scope of this last provision, which was considered too restrictive for the purposes of investigations, on the eve of the coming into force of the Privacy Code, the Government approved a Decree Law (no.354 of 2003) which provided an extension to five years of the permitted retention of data on telephonic traffic and a similar extension of the same rules relating to Internet communications, as well as a suspension – until 2006 – of the former regulations (Decree Law no.171 of 1998) which should in fact have ceased to operate last January. The effect of this, in fact, is to reduce significantly the safeguards of every citizen's liberty, albeit for the laudable purpose of repressing crime.

Such periods of permitted retention of data were notably greater than those in effect in other European countries, which, however, only had to face up to the terrorism emergency after 2001 and encountered major opposition to the introduction of even much shorter periods. This was due not only to the resistance among the organizations protecting civil rights but more generally to all those who were accustomed to relying on legal provisions such as those protecting privacy in the European Unions Charter of Basic Human Rights (see the cited Arts.7 and 8).

Fortunately, however, after a mobilization of institutions and citizens, the Italian Parliament did a significant about-face. So, the Law converting the Decree re-limited the scope of applicability of Art.132 of the Privacy Code to telephonic traffic, laying down an initial permitted period of retention of two years (rather than the two and a half years in the emergency provision). After that

period, the same information may be retained for a further two years (rather than a further two and a half years) only if this is for the repression of the crimes listed in Art.407, para. 2(a) of the Code of Criminal Procedure (for which there is an extended period permitted for the continuation of investigations) as well as those damaging to informatics and telecoms systems.

By contrast with the original text of the Code, the emergency provision had provided a detailed description of the mode of acquiring data. And in this field also the converting Law has provided for the introduction of a series of modifications tending to offer greater safeguards, laying down in particular that only the court (and not even the Public Prosecutor) may order the acquisition of data requested by the authorities or by one of the parties. Moreover, after the first two years, the court may only authorise the acquisition if there is sufficient evidence of the crimes previously cited. Finally, the Italian Parliament has also decided to empower the Authority (rather than the Minister of Justice) to define – through a declaration under the terms of Art.17 of the Privacy Code - the measures and devices to safeguard the interested party, so extending the guarantees for the protection of personal privacy.

5.2 Data on location

Among the most sensitive and overall most valuable information for police investigations, emphasis must be laid on data concerning the location, or information indicating the geographic site, of the terminal equipment of the user of an electronic communication service. This permits not only locating with great precision the subject, his map reference, altitude and direction of movement, but at the same time can help construct an important image of the subject's personality. The handling of such data is generally connected to the provision of the so-called "added value" services, such as the description of the neighbourhood, the indication of where commercial forces of a given category that are being sought are to be found or the remote control of vehicles, animals or persons.

Services are becoming more available which permit the location of third parties other than those making the request for information: indeed there are commercial services aimed at locating everyone who has a mobile telephone number, provided that that the terminal is kept open and is recorded in a relevant list. Such a list could be a group of friends or a family (within which such treatment could create very delicate problems, notwithstanding the safeguards contained in the Law, to which we will briefly allude). But what is not excluded may slip through into forms of control of employees by an employer, despite the prohibitions concerning the remote control of workers.

To give an idea of the rapid spread of such services, it suffices to mention that, until a few months ago, there was a heated debate on the legitimacy of the use of "electronic bracelets" to control the movements of prisoners released on probation. Last summer a very similar device was used on beaches by mothers fearful that the children might stray too far……

It seems well established that the knowledge of such information makes it possible to reconstruct precisely the various actions taken (one thinks of questions as to the nearest petrol station or restaurant) or the interests (every time information is requested as to the location of something) of the person who has utilised or been the object of the service, to the point of constructing a personality profile of that person. Moreover, it is clear that the knowledge of such facts becomes even more important – and hence threatening to the persons concerned – the longer they are stored, even if the aim is the apparently useful one of better personalising the service offered; indeed this is exactly the logic of added value services.

Because of the specific risks connected to their handling, the Privacy Code, consistent with the intent of Directive no.58 of 2002, devotes to such data a specific discipline in relation to information on electronic traffic, which we have already examined in some detail. More particularly, data on location may be handled only if made anonymous or with the prior consent of the user or subscriber, (which may be revoked at any time) and to the extent and for the period necessary for the provision of the requested added value service. Even after the grant of such consent, the user and subscriber retain the right to request, free of charge and by

a simple procedure, the temporary interruption of the handling of such data for each connection to the Net or for each transmission of communications (Art.126).

The provider of the service, before requesting consent, is also required to inform the interested parties as to the nature of the data to be handled, on the aims and on the duration of such handling, as well as on the possibility that data may be transmitted to a third party for the provision of added value services.

Finally, as a further precaution, the Privacy Code has laid down that the handling of such information may be permitted solely to those handling it under the direct authority of the provider of the electronic communication service, or, as the case may be, the provider of the Net or of the third party providing the added value service. In every case, the handling must be limited to what is strictly necessary for the provision of the service and must ensure the identification of the person responsible who has access to the data including such access through an operation of automated interrogation.

5.3 Video-surveillance and biometric analysis

Particular importance for police activities attaches to personal information accessible from video-surveillance installations, the growing use of which for the protection of persons or property, despite being often justified in the interests of security, still represents an increasing intrusion into individual privacy.

Indeed, with growing frequency, such systems come to be combined in various ways with sophisticated instruments which will ensure the identification of persons through "biometric analysis" (geometry of the face, irises, etc.) which enables the newly acquired information to be compared with previously memorised data.

No-one doubts the usefulness and sometimes the indispensability of the use of such technologies in supporting the security of citizens. Nevertheless, it is clear that even in this case too, it is necessary to ensure a proper balance between such exigencies and those linked to respect for the fundamental rights of people, who must not be condemned to live under the perpetual surveillance of others, even if such an operation may ultimately be of benefit to them.

The organs charged with protecting personal data have spoken a number of times about such problems, both in the Council of Europe and the European Union. The Italian Authority also, as well as setting our a ten-point pronouncement on the use of such instruments, has had cause to intervene innumerable times to prevent excessive on non-consented data use. In this case also, the guideline principles are those mentioned above: relevance, non-excess and proportionality, which prohibit the generalised collection of personal information which is not justified by situations posing a concrete risk tied to objective circumstances.

These are principles which should govern not only the phase of information-collection (for example, avoiding the installation of an excessive number of video-cameras, giving access to them up only when really necessary, adjusting their catchment- area in such a way as not to collect excessive data, etc.) but also – and this is surely the most important element for investigative applications - the subsequent phases of data-storage.

In this regard, there is the rule under which the data collected must be erased as soon as it is no longer needed to meet its purposes, while access to it may in certain cases only be sanctioned for the police authorities where a criminal act has been confirmed. All this prevents the ever increasing number of video-camera installations leading to the systematic storage of data secured over time, which is permitted only if justified to provide evidence on given events. This is the case even though recognition of the usefulness of such records may support and in practice has supported investigations into a variety of crimes.

With specific reference to video-cameras, it should finally be mentioned that the materials will be more fully and organically systematised in a specific code of deontology and good practice "for the treatment of personal data obtained by electronic instruments for recording photographic images", which will need to

lay down specific modes of handling and simplified forms of providing information to the subject-party in order to ensure the lawfulness and correctness of the operation (cf.Art.134, Privacy Code).

5.4 Genetic data

The general p[principles described above are obviously more stringently applied in relation to particularly sensitive data, such as genetic data, being more and more often used for identification purposes in the course of police investigations. As part of data appropriate for revealing a state of health, genetic information is the most intimate, with a capability, inter alia, of incurring the risk of discrimination. This is so, not only when representing a permanent element immutable on the part of the subject, but also because information is contained directly which is not confined to the subject but may concern also his relatives; and finally because not only past history is revealed but also prospects for the future. Such is the case, for example, in techniques of "predictive medicine", capable of identifying possible delayed-onset illnesses and thus of providing an insight into the future which perhaps should not be known and certainly should not be disclosed.

Because of these characteristics of theirs, the handling of genetic data, no matter who has generated it, is only permitted in cases where the Authority has given specific consent with the knowledge of the Ministry of Health, and after obtaining the favourable opinion of the Senior Health Council. It has been further laid down that such an authorization must contain, *inter alia*, the indication of the elements to be recorded, with particular reference to the specification of the objectives pursued and the prospective consequences of unexpected information coming to light as a result of the handling of data as well as the right to subject data to the same treatment for legitimate purposes (Art.90, Privacy Code).

6.Security v. rights

The international and domestic climate following the terrorist outrages of 11th September 2001 and subsequent tragic events up to the present day, have prompted every occidental State to adopt especially stringent measures in the field of public security.

Unfortunately, behind the emotive pressure of such events, some measures have been adopted which do not always respect the principles and criteria mentioned above: measures which too often fail to give due regard to the long-term consequences of such policies (see in this connection Opinion 10/2001, approved on 14th December 2001 by the Group of European Guarantees provided for in Art.29 of Directive no.95/44/EC).

It is probably true that such greater stringency has represented a partially inevitable response to the various emergency situations confronting governments and organs responsible for safeguarding their citizens' security. Nevertheless, even such extreme circumstances can never justify an excessive diminution of basic human rights.

This is because, when everything has been duly taken into account, such rights are also the mirror of the values which those threatening security aims to jeopardise and destroy.

Notes

1 .Advocate, journalist, expert in public law, Director of the Studies and Documentation Service of the Authority for the protection of Personal Data, and President of the Appeal Committee prescribed by Art.24 of the Europol Convention (responsible for giving the final judgment on complaints by citizens against Europol).

2. Art.117 of the Code dealing with the protection of personal data (Legislative Decree of 30th June 2003, no.196) provides for the profiles linked to the protection of data in the creation and handling of such data-banks to be regulated by a special code of deontology and good practice. It is in implementation of this

provision that the Personal Data Protection Authority has specifically promoted the approval of a code of deontology "for the handling of personal data obtained within the ambit of informational systems relating to private citizens, which are utilised for the grant of credit to the consumer or assessing credit-worthiness and regularity of payments, also identifying specific means of safeguarding communications of exact and up-to-date personal data affecting the rights of the person concerned.

3. In this connection, it may serve to record that the Group of European Guarantees established in Directive no.95/46/EC, concerned with "the storage of traffic Data for billing purposes", has concluded its work, stating that "the reasonable interpretation of the Directive ss that this should ordinarily involve a routine storage period of a maximum of 3-6 months, with the exception of particular cases of dispute, where the data may be processed for a longer period".

3. NEW CHALLENGES FOR LAW ENFORCEMENT

Introduction

Gloria LAYCOCK
Director, Jill Dando Institute of Crime Science
University College of London, UK

Technology and Intelligence Collection

Neil BAILEY
Directo, Intelligence Services
National Criminal Intelligence Service, UK

4. NEW CHALLENGES FOR RESEARCH AND NEW PATHS FOR DEVELOPING CURRICULA

Introduction

Ronald V. CLARKE
School of Criminal Justice, Rutgers University, NJ, USA

Research on crime and technology

Cindy J. SMITH
Director, Criminal Justice Graduate Programme, University of Baltimore

Technology presents special circumstances for criminologist researchers. To date, much of the crime research has been in areas where the technical aspects of the crime do not interfere with the research. For example, it is not necessary to understand how an automobile is powered to research auto theft. However, new technology has presented new challenges. For example, the researcher must understand how to identify a virus before he or she can count it.

The purpose of this paper is to reflect on the resulting challenges new technology has presented for those who conduct research on the nexus of crime and technology. There are three key issues in this reflection. First, the research development process helps to understand why we do not have more research in the public domain at this time. Next, a discussion of some of the research methods used to date with examples is presented. Finally, this paper presents a discussion of the implications of conducting research in the high tech sciences along with the responsibilities of the researchers, data owners, and policy-makers.

Research Development Process

Cutting edge research follows a general four step developmental process (See Figure 1). Practitioners are often the first to observe a new crime. They discuss it at meetings and write about it in their own newsletters, trade journals, and other publications. Researchers depend on practitioners to raise their awareness to this new concern. For example, practitioners knew about worms (computer viruses) long before the researchers became involved. For example, in this text Ms. Angers from Canada presents:

> There are three ways of committing a crime with a computer; using the computer as a tool (i.e., contact between organized crime figures), using the computer as a storage device (i.e. pornography), and using the computer as a target (i.e., viruses).

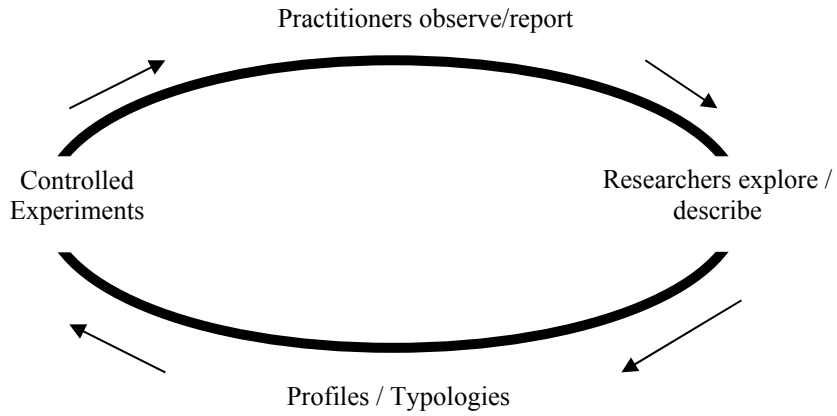

Figure 1. Research Development Process

The second step occurs when researchers become aware of and interested in the new phenomenon and begin to explore or describe the crime, impact of the event, or simply to count the occurrence while working closely with practitioners. Once the crime, offenders, or victims are sufficiently described, the researchers begin to classify or categorize the new crimes. They develop profiles and typologies that are useful in developing controlled experiments or creating theories. The practitioners and researchers discuss these preliminary typologies in terms of the characteristics of the crime as they struggle to generalize and create an abbreviated common language. For example, David Wall described this typology of cybercrime in his text in 2001. There are three categories of cybercrimes:

1. The internet is used as a tool to commit an old crime (i.e., pedophilia, fraud);
2. The internet is used to commit a new crime that did not exist before the technology was developed (i.e., appropriation of music or software); and
3. The internet is used as a communication device (i.e., hate speech, bomb talk).

The research process on technology is currently somewhere between the exploratory step and the profiling step. The good news is that the research development process is progressing comparably to the way other new crimes have progressed through this cycle. Additionally, researchers are beginning to be quite interested, are probably funded at some level and there should be a rapidly growing body of published research over the next few years as the researchers begin to develop controlled experiments, risk and needs assessments, theories and other useful tools.

Throughout the research development process, the researchers and practitioners work simultaneously to raise awareness among the stakeholders. Generally, these stakeholders include raising the awareness of governments of the need for new or revised laws and funding, funding agencies of the need for research, and the general public and/or victims for prevention and intervention.

Within the research literature on high tech crimes, many articles spend considerable time raising the level of awareness to the seriousness of this or that particular issue by discussing two key points:

1) This problem exists at a much higher rate than currently is known. Evidence for this belief of under reporting is because victims are unaware that they have been victimized and victims are unwilling to reveal the crime. For example, stockholders would be upset if they knew a computer system was compromised.
2) This problem is costing a considerable amount of money. Estimates are very high in the literature and include, for example, the loss of current and future sales.

These two key points set the stage for increased funding availability, which results in increased research.

Research Methods

What is new in research methods? The answer to that question to date is *not much.* To date the methods used in the research literature have been the same methods used in other research for many years. However, as the research process moves toward controlled experiments, it is possible that these methods may need to be expanded, such as those suggested in Dr. Savona's article included in this text. Additionally, there may be a need to expand the analytical techniques, such as those suggested by Hans DeRoo, also found in this text. However, for now, the old methods appear to be sufficient during this exploratory research era.

A survey of the literature to date includes a wide variety of methods. For example, one study used secondary data (Dertouzos, Larson, & Ebener 1999). In this study the researchers sufficiently gained the confidence and trust of the data owners and were able to obtain and analyze the data. Gaining trust is a key issue when researching sensitive materials. For example, the Dertouzos study determined the economic costs of high tech hardware theft using manufacturing and security costs from computer firms.

Next, the Delphi method was used to predict future types of computer crimes (Coutorie 1995). This widely used method compared the predictions of high tech criminal justice experts with the predictions of techies to determine what types of crimes would become more prevalent in future years.

The third method is observation. One study observed the behavior of those participating in a newsgroup - alt.drugs.chemistry - that educated participants on how to make synthetic drugs (Schneider 2003). The second study observed that internet users who were going to a legitimate website were found to be quite likely to try to download illegal material once at the site (Demetriou & Silke 2003).

Additionally, survey and case study methods also appear in the literature (Dertouzos, Larson, & Ebener 1999). A comparative study authored jointly by researchers from US and India developed a model that tests the economic benefits of maintaining different or incompatible DVD standards across geographic regions to prevent piracy (Chellappa & Shivendu 2003). Finally, interviews were conducted with 13 convicted men who downloaded child porn (Quayle & Taylor 2002).

Challenges of High Tech Crime

The challenges that high tech crimes pose to researchers are not very different than other new crimes or new methods of crime have posed to researchers in the past. The first challenge is the ability to access the data. There are four possible explanations for this challenge: 1) unfamiliarity of the way crimes are committed or newness of some of the crimes; 2) new vocabulary, as discussed in the Hans De Roo article in this text; 3) difficulty in understanding the technology; and 4) lack of partnerships, which is discussed later in this article.

The second challenge is accurately and completely interpreting the findings. This is as a result of the technical language and nuances of the technology. For example, when Demetriou & Silke (2003) designed their sting operation to tempt internet users to download illegal material, they logged his website with various search engines with words indicating the legal activities found on the website. His intention was to attract non-deviant individuals and see if they would commit an illegal activity once they were on the website. However, some search engines conduct word searches, which enabled some visitors to come to the website expecting to find the illegal material. While this is a very basic piece of search engine information, those not adequately schooled in technology or not partnering with a techie would have included the "intentional deviants" in the findings with the non-deviants.

Three policy implications related to these challenges are found; 1) count crime, 2) develop partnerships, and 3) learn technology basics. First, baseline databases must be developed. In other words, there exists a need to count things. For years Freda Adler, who is well known to ISPAC members, has promoted simply counting things. The first step in researching crime is to understand how much of it exists

– in other words, count it. Graeme Newman (2003), in the Expert meeting on the World Crime and Justice Report 2004-2005, highlighted the importance of counting by suggesting we count all true threats to human security, such as homicide rates. In fact, he suggests that we increase the number of items that we routinely count to develop a social vulnerability index. Counting is not an easy task. This takes considerable trust that the data will be used appropriately and that the member states or corporations will be held harmless.

It is not likely that researchers will become experts all areas necessary to conduct good research. For example, researchers will not become experts in technology, experts in research, and experts in crime, plus learn the necessary diplomatic behavior to obtain the data. Therefore, it would be wise to develop partnerships (See Figure 2). These partnerships must include the data owner – the corporation, the victim, or the government. It must include a techie, who can assist in the design, collection, and interpretation of the data to ensure high quality data and that the fine distinctions are included. Lastly, a researcher must be included in the partnership to ensure that the data collected are the type of data that will be useful for research that will inform policy.

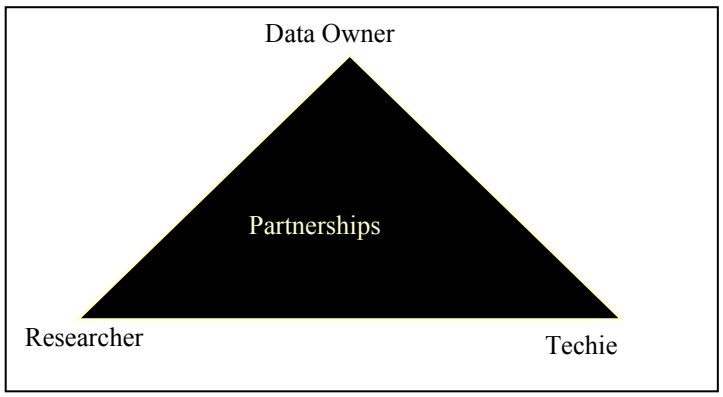

Figure 2. Partnerships

Finally, the researchers must learn technology basics to ensure accurate and complete communication between the partners. The researchers who do policy relevant research often partner with practitioners who know considerably more about the topic or data than the researcher. An appropriate level of respect, humility, and effort to learn the basics will increase the effectiveness of the partnership.

Responsibilities of Researchers and Policy-makers

Researchers and policy-makers have several separate responsibilities. It is the responsibility of the researcher to be trustworthy, confidential, and use the scientific method. In this text, Lucy Angers suggests that researchers should be more responsible, ensuring the data reported are accurate, complete, and interpreted in the context in which they exist. Researchers must build trust by being trustworthy in their behavior. Additionally, researchers have a responsibility to hold appropriate information in confidence when gaining access to sensitive information. This includes aggregating data in such a way that the victims, perpetrator, and country or corporation are not identifiable – especially if it is embarrassing to anyone involved and to ensure false accusations are not perpetuated. Finally, researchers have a responsibility to

conduct quality scientific research. This includes random assignment where appropriate, using control groups, discussing limitations and educating all members of the partnership about why a particular method is best. Additionally, the partnership must use language that is understandable and useful to policy-makers and the readership.

Data owners and policy-makers have responsibilities also. It is imperative that the data owners provide a structure and climate of willingness to participate in research to enable researchers to count and later conduct controlled experiments, risk and needs assessments, or other research to help guide policy. By providing the opportunity, structure, and climate to partner in research efforts, the data owners ensure that policy is based on the state-of-the-art knowledge. Policy makers have a responsibility to use quality reliable research results to inform policy.

References

Chellappa, R. & Shivendu, S. (2003). Economic Implications of variable technology standards for movie piracy in a global context. *Journal of Management Information Systems 20(2), 137-168.*

Coutorie, L. (1995). The future of high-technology crime: A parallel Delphi study. *Journal of criminal justice. 23 (1), 13.*

Demetriou, C. & Silke, A. (2003). A criminological internet 'sting.' *British Journal of Criminology*, *43, 213-222.*

Dertouzos, J., Larson, E., & Ebener, P. (1999). *The economic costs and implications of high-technology hardware theft.* Santa Monica, CA: Rand.

Quayle, E. & Taylor, M. (2002). Child pornography and the internet: Perpetuating a cycle of abuse. *Deviant Behavior: An Interdisciplinary Journal 23, 331-361.*

Newman, G. (June, 2003). World crime trends: Notes on recommendations for the second global report on crime and justice. *Expert Meeting on the World Crime and Justice Report, 2004-2005.* Meeting held in Turin, Italy.

Schneider. J (2003). Hiding in plain sight: An exploration of the illegal (?) activities of a drugs newsgroup. *Howard Journal, 42(4), 374.*

Wall, D.S. (ed) (2001) CyberCrimes and the Internet, Chapter 1, in Wall, D.S. (ed) (2001) *Crime and the internet.* London: Routledge.

The contribution of research to the development of more effective policies against crime

Sandeep CHAWLA
Chief, Policy Analysis and Research Branch, UNODC, Vienna

Defining new curricula to train new professional figures

Jerry H. RATCLIFFE
Criminal Justice Professor, Temple University, Philadelphia, US