ISPAC

International Scientific and Professional
Advisory Council
of the United Nations
Crime Prevention and Criminal
Justice Programme

CIBERCRIMINALITY: FINDING A BALANCE BETWEEN FREEDOM AND SECURITY

Edited by
Stefano Manacorda

Co-ordinators
Roberto Flor, Joon Oh Jang

Selected papers and contributions from the International Conference on
"Cybercrime: Global Phenomenon and its Challenges"
Courmayeur Mont Blanc, Italy
2-4 December 2011

STEFANO MANACORDA
Professor of Criminal Law
University of Naples II, Italy;
Directeur de l'Equipe
Internormativités dans l'espace
pénal, Collège de France, Paris
ISPAC Deputy Chair and Director

ISBN 978-88-96410-02-8

3, Piazza Castello – 20121 Milano, Italy; phone: +39-02-86460714; Fax +39-02-72008431
E-mail: *cnpds.ispac@cnpds.it*; Web Site: *http://ispac.cnpds.org/*

The views and opinions expressed in this volume are solely those of the authors and do not necessarily represent the official position of the United Nations or the organizations with which the authors are affiliated.

Acknowledgements

ISPAC wishes to thank the Fondazione Courmayeur and its President, Dr. Lodovico Passerin d'Entrèves, as well as the Korean Institute of Criminology and its President, Prof. Dr. Il-Su Kim, for their generous contribution towards the publication of this book.

CONTENTS

FOREWORD

STEFANO MANACORDA[1]

Like many other fields of criminology, the borders of cybercrime are not set in stone. Even the way cybercrime is defined by legislators or by scholars suffers from the extreme semantic looseness of the terminology adopted. This book of selected papers and contributions from the international conference on "Cybercrime: Global Phenomenon and its Challenges" (Courmayeur, 2 - 4 December 2011) offers one of the many specific perspectives from which the issue may be analysed. Our aim is to tackle an array of themes arising out of the evolution of punitive responses adopted internationally and domestically in the fight against cybercrime, as may be evinced from the publication's title: "Cybercrime Between Global Enforcement and Civil Liberties".

Every criminal phenomenon appears, to the institutions that make it a priority of their actions, and for the scholars who dedicate themselves to it, as being characterized by certain specific aspects that make it unique in terms of criminal policy approach. For instance, organized crime is considered to be one of the greatest threats to peaceful societal cohabitation, based on the assumption that its penetration is tentacular and uncontrollable, even if it must be acknowledged that any definition is beyond the scope of rational control in the legal sphere. Terrorism is an insidious and devastating threat to security, capable of subverting the very foundations of the State; nevertheless it must be acknowledged that it can lead to criminalize conducts that are extremely problematic with respect to the harm principle – if not clearly in contrast with it – so highlighting the "shadow side" of the concept.

All these issues require the use of *extra-ordinem* tools of control and sanction – or at least they provide *ex post* justification for. Such a need for a severe punishment constitutes indeed the *raison d'être*, and therefore the political legitimization, for the international institutions intervention. At least two unintended consequences are generated: one is a sector-defined "differentiation" of models of punishment between one sector and the next, which loses sight of the need for systemic coherence; the other is that it pushes criminal policy into a repressive spiral, as criminal law penalties become ever more stringent. In both of these cases, the criminal law and procedure appears as being "emergency-led". The potentially repressive and exemption-based approach to the basic guarantees for perpetrators ends up affecting a number of other fields, one of which is what

---

[1] Professor of Criminal Law, Seconda Università di Napoli; Collège de France, Paris, Deputy Chair and Director, ISPAC.

we refer to as cybercrime. This category may also, alas, interface with organized crime or terrorism, leading to an additional impetus towards repression.

Indeed, the increasing number of international documents that seek to establish a criminal framework for containing the phenomenon of cybercrime would appear to have the effect of a "global enforcement", the first of the cornerstones highlighted in the title.

First and foremost, the intangible and evasive nature of cybercrime's means that it is destined to include conduct that is barely harmful to legally-protected values. One good example may be found in the debate regarding virtual child pornography, that is to say, producing or simply possessing images portraying minors with a sexual connotation, and which wholly result from computer processing: such a case illustrates a moralizing drift in the criminal system, something to which European and international inputs have strongly contributed. At a strictly operational level, we have witnessed a strengthening of operational police and judiciary tools as part of an increasingly close focus on control and sanction: the setting up of specialist teams, covert investigation techniques such as communications surveillance, and the potentially never-ending option of accessing electronic storage, are some of the consequences of such a global enforcement. Moreover, the territorial scope of cybercrime is, obviously, global: this type of crime has become de-localized with respect to the place where the harmful result is occurred; in some cases it has become de-territorialized and occurs in cyberspace, which lacks any relations with the State as traditionally understood, and therefore falls outside the realm in which the punitive powers are exercised. As a result of this, wide-ranging decisions have been taken regarding jurisdiction, alongside the introduction of enhanced mechanisms for cooperation.

The above-mentioned ongoing drive towards global enforcement leads to difficulties in striking an appropriate balance between civil liberties and the need for collective security, once again highlighting the classic dilemma – the "double-edged sword" – of criminal law. Above all, the swing of the pendulum between these two extremes is particularly problematic, especially when we remember that basic liberties are structurally associated with using the new technologies: the risk of putting undue pressure on freedom of expression and opinion, of forms of political dissent, and the right to freely manifest one's own religious or ethical beliefs, are particularly hot button questions.

By combining a theoretical analysis, a survey of sanction-related responses and investigation tools, and presenting operational experiences, this book helps find answers to the challenging issues of security and freedom in this arena.

INTRODUCTION

CYBER-CRIMINALITY: FINDING A BALANCE BETWEEN FREEDOM AND SECURITY

ROBERTO FLOR
Assistant Professor of Criminal Law
Professor of ICT Criminal Law and International Criminal Law
University of Verona, Italy

This volume features the proceedings of the conference on "*Cybercrime: Global Phenomenon and its Challenges*," which was organized by the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme - ISPAC, the Centro Nazionale di Prevenzione e Difesa Sociale - CNPDS, the Courmayeur Foundation in cooperation with the United Nations Office on Drugs and Crime-UNODC and the Korean Institute of Criminology-KIC of Seoul.

A prime motivation for holding this Conference was to inspire a dialogue between the scientific community, the experts, the law enforcement agencies, involving the private and public sectors, and the international organizations on the challenges posed by the evolution of cybercrime in the "Globalization Era", at regional and international level.

The Internet and other new technologies are playing an important role in today's global information society, are now essential in every sector of human life and can be used for the preparation and commission of serious and transnational crimes.

The Internet has frequently been considered as intrinsically free from regulation, a place where liberty, freedom of expression, sharing, creativity and mutual inspiration would be assured by the very nature and architecture of the networked environment.

Against this "dream of soaring"[1] and unfettered liberty, there is the reality of different interests that are increasingly dominating the world.

There is no internationally recognized legal definition of the terms "computer crime" or "computer related crime" or "cybercrime".

The history of "computer crime" dates back to the 1960s when first articles dealt with computer manipulation, computer sabotage, illegal use of computer systems and computer espionage[2].

---

[1] See E. Viano, *Balancing Liberty and Security Fighting Cybercrime: Challenges for the Networked Society*, infra, part I.

[2] See U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, COMCRIME Study, 1998, 18.

In the 1980s and 1990s "computer crime" was no longer limited to economic crime, but included attacks against a diverse range of interests, such as privacy infringements and copyright infringements, but also the use of computers and communication systems by organized crime[3].

The advent of the Internet has brought substantial changes: at phenomenological level, the dissemination of illegal contents (Intellectual Property infringements, child pornography, incitement to racism and xenophobia, ect.), illegal access to computer systems, system and data interference, illegal interception of non-public transmissions of computer data, new communication tools also useful for the preparation of serious crimes (such as terrorism)[4].

The worldwide proliferation of Information and Communication Technologies has facilitated the commission and the preparation of these types of "criminal activities", which pose threats not only to the confidentiality, integrity or availability of computer systems and data and to the security of "critical" infrastructures, but also to the Intellectual Property rights, property and public confidence.

At the terminological level, the terms "Internet-crime" and "Cybercrime" have increasingly been used and Authors started to distinguish between "computer crime" and "cybercrime" [5].

The offence conduct characterizing the category "cybercrime" includes not only specific computer related crime, but also the use of the new technologies and Internet to commit a wide variety of "traditional" crimes which may be committed also "through means other than by the use of a computer"[6].

More precisely, cybercrimes are often divided into three categories:

---

3 In 1983 a group of experts of the OECD defined the term "computer crime" or "computer related crime" as any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission of data. See U. Sieber, *The International Handbook on Computer Crime*, 1986, 1 et seq.

4 About "cyberterrorism" see U. Sieber., P. Brunst, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes - Threat Analysis and Evaluation of International Conventions,* in Council of Europe (ed.), *Cyberterrorism - the use of the Internet for terrorist purposes,* Strasbourg, Council of Europe Publishing, 2007.

5 About the etymology, content and function of the terms see U. Sieber, *Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law,* in M. Delmas-Marty, M. Pieth, U. Sieber, (eds), *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15.* Paris, Société de législation comparée, 2008, 127 - 202; U. Sieber, *Computerkriminalität und Strafrecht*, Köln/Berlin/Bonn/München, 2. Auf., 1980. See also infra, note 6.

6 See M. F. Weismann, *International Cybercrime: Recent Developments in the Law*, in R. D. Clifford (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011, 257, 258.

crimes in which the computer (and, in general, new technologies and Internet) is a tool used to commit a crime; crimes in which the computer system is the target of the criminal activities; crimes in which the use of the new technologies and the Internet is an "incidental aspect" of the commission of the crime[7]. In other words, they play a non-essential role in the commission of the offence and the computer could be a source of evidence.

With specific reference to the structure of the criminal offence, some Authors[8] distinguish beetwen:

"Computer crime in the narrow sense" (computer and, in general, new technologies is/are an essential element, or the computer, or information stored on the computer, is/are the subject or target of the criminal activities); "Computer crime in the broader sense" (new technologies are not an essential element in the structure of the criminal offences, but could be a tool used to commit a crime, or are the environment or context); "Cybercrime in the narrow sense" (Internet or the connession are an essential element in the structure of the offence); "Cybercrime in in the broader sense" (Internet or the connession are not an essential element in the structure of the criminal offences, but could be a tool used to commit a crime, or are the environment or context).

The new technologies can play also an important role in the fight against crimes.

In this case the question concerns the limits within which the legislators can operate in the impairment of fundamental rights and in the fight against serious and transnational crimes, through Internet search and seizure measures, access to private communication, monitoring and investigating the Internet, clandestinely intercepting and searching for communication via the Internet, and/or to secretly access its information technology systems[9].

---

7 See S. W. Brenner, *Defining Cybercrime: A Review of Federal and State Law*, in R. D. Clifford (ed.), *Cybercrime*, cit., 15-104, 17. About the terms and the "Spektrum von Fällen" see U. Sieber, *Computerkriminalität*, in U. Sieber, F. H. Brüner, H. Satzger, B. Von Heintschel-Heinegg (Hrsg), *Europäisches Strafrecht*, Baden-Baden, 2011, 393-421; U. Sieber, in Council of Europe (ed.): *Organised Crime in Europe: The Threat of Cybercrime*, 2004 (2005).

8 See, for example in Italian literature, L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec*., 4, 2011, 827.

9 On the 27th of February 2008, the German Federal Constitutional Court recognised in a landmark ruling for the first time a new constitutional right in the confidentiality and integrity of information technology systems. The primary question the Court had to decide was the constitutionality of a law authorising the secret services of North Rhine-Westphalia to surreptitiously monitor and investigate the Internet. In particular, the law would have granted the secret services the right to clandestinely

In recent years, the international community has become more aware of the need to further understand and tackle cybercrime. This is expressed in the increasingly important mandates that the United Nations, including the United Nations Office on Drugs and Crime (UNODC), have received from its Member States and governing bodies.

After the adoption of the recommendations of the Council of Europe (1989), the Convention on Cybercrime of the Council of Europe (2001) is the most important international treaty.

Open for signature by the Member States of the Council of Europe and by non-member States which have participated in its elaboration, in Budapest, on 23 November 2001, its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work of the experts of the Council of Europe, but also by the United States, Canada, Japan and other countries, which are not members of the Organisation. It has been supplemented by an Additional Protocol, which makes any publication of racist and xenophobic propaganda via computer networks a criminal offence.

The Budapest Convention does also serve as a guideline and many countries have used it as a "model law" when preparing domestic legislation.

Recently the 11th UN Congress on Crime Prevention and Criminal Justice, held in Bangkok, Thailand in 2005, recognized the seriousness of cybercrime, and a workshop was held on computer-related crimes. The Bangkok Declaration on Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, endorsed by General Assembly resolution 60/177 of December 2005, welcomed the efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime. In 2010, the 12th UN Congress on Crime Prevention and Criminal Justice, held in Salvador de Bahia, Brazil, which had a strong focus on cybercrime, resulted in two very concrete outcomes. The Salvador Declaration recommended that the United Nations Office on Drugs and Crime (UNODC) provides, upon request, technical assistance and training to States, in order to

---

intercept and search for communication via the Internet, and to secretly access its information technology systems. The Court ruled that § 5.2 of the Act on the Protection of the Constitution in North Rhine-Westphalia was not in compliance with the constitution and therefore null and void. See W. Abel, B. Schafer, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008*, 822, in SCRIPTed, 6, 1, 2009, 106-123; R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2009, 695-716, also for further references.

improve national legislation and build the capacity of national authorities in order to deal with cybercrime. In addition, the Salvador Declaration requested UNODC to convene an intergovernmental expert group to carry out a comprehensive study on the problem of cybercrime and responses to it by Member States, the international community and the private sector. The first meeting of this open-ended intergovernmental expert group took place from 17-21 January 2011 and, among other things, the group endorsed the topics, methodology and timeline for the study. Both mandates were subsequently echoed by the Commission on Crime Prevention and Criminal Justice (Crime Commission), the Economic and Social Council and the General Assembly in resolution 65/230.

In April 2011 the Crime Commission adopted two resolutions relating to UNODC's work on cybercrime, underscoring the importance of the mandates of the Salvador Declaration: resolution 20/7 on the promotion of activities relating to combating cybercrime, including technical assistance and capacity-building which requested UNODC to continue to provide, upon request, technical assistance and training to States, based on national needs, especially with regard to the prevention, detection, investigation and prosecution of cybercrime in all its forms; and draft resolution I (currently at ECOSOC for endorsement) on "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children".

Combating cybercrime is especially challenging due to problems of jurisdiction that arise at both the national and international level. The traditional forms of jurisdiction are based on the concept of boundaries, and laws are based on "territorial sovereignty". Because cyberspace has no physical boundaries, criminals can change their locations from one country to another within seconds in the cyber-world, irrespective of their physical location[10].

Consequently, all States must also be able to use and contribute to international cooperation mechanisms. This is especially important for developing countries as they are often technologically less able to combat cybercrime, and thus especially vulnerable to being used as platforms from which to stage cybercrime.

At European level, the Lisbon Treaty provides a first list of areas of "serious crimes" in Article 83 TFEU[11]: the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary

---

10 In this context rules on data retention are important and remain necessary as a tool for law enforcement, for the protection of victims and for the criminal justice systems. About the European Union rules on data retention and important decisions of European Constitutional Courts which annulled the laws transposing the Data Retention Directive (2006/24/EC) see R. Flor, *Data retention rules under attack in the European Union*?, in *Illyrius*, 1, 2012, 69-86.

legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime include also terrorism, computer crime and organized crime.

The Treaty of Lisbon provides, together with an express recognition of the Union's competences in criminal matters through the use of directives, a number of provisions of "procedural nature", while strengthening the role of Eurojust and Europol. It also provides the possibility of establishing a European Public Prosecutor, and the instruments of police cooperation, with the aim to establish measures concerning the collection, storage and processing of data and information, and shared investigative techniques to identify serious forms of organized crime.

In this context, after the adoption of the directive on combating the sexual abuse, sexual exploitation of children and child pornography, repealing the framework decision 2004/68/JHA[12], the European Commission has presented two new measures against attacks on major information systems: a proposal for a directive on attacks against information systems, which repeals the framework decision 2005/222/JHA[13], and a proposal for a regulation to strengthen and modernize the European Network and Information Security Agency (ENISA). The two initiatives have their basis in the European Digital Agenda[14] and in the *Stockholm Programme* to boost *trust and network security*[15].

The proposal for a directive, in particular, keeps the provisions of the framework decision on criminalizing illegal access to computer systems and unlawful system and data interference (corruption of data, information, programs or systems), adding, in terms of substantive criminal law, the criminalization of tools aimed at committing a crime, the illegal interception of data and information and, in terms of international cooperation, rules to improve criminal justice and cooperation among States.

---

11 On the Art. 83 TFEU, in subiecta materia, see U. Sieber, *Computerkriminalität*, cit., 393; M. Gercke, *Impact of the Lisbon Treaty on Fighting Cybercrime in the EU. The redefined role of EU and the change in approach from patchwork to comprehensiveness*, in *Cri*, 3/2010, 75; L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 4, 2011, 827.

12 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

13 Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA [COM (2010)517 - C7-0293/2010 - 2010/0273(COD)].

Joon Oh Jang
Senior Research Fellow
International Center for Criminal Justice Korean Institute of Criminolology
KIC - Seoul - Republic of Korea

The challenges posed by the "new society" require a process of political choices in criminal matters, in particular in cybercrime, more extensive than the scopes of the European countries. It needs to involve the United Nations and more specifically, with the European countries, the main "Internet countries", such as USA, Latin America, China and Russia[16].

In light of the above, it was essential that UN PNI members had the opportunity to discuss the global challenge of cybercrime and its countermeasures as a theme of the 2011 ISPAC annual Conference, taking into account some of the most important questions of the Internet Era.

Part I has been devoted to finding the right balance between security and civil liberties in the fight against cybercrime, debating topics under the light of Human Rights in the Technology Era, privacy and freedom of expression included.

Part II reviewed technology development and analyzed specific case studies, taking into account the social dynamics of "cybercrime markets", the relationships with organized cybercrime and the victimization in the cyberspace.

In Part III speakers examined National Enforcement and Investigation practices against Cybercrime, including the comparative analysis also with the Chinese, Iranian and Korean legal systems.

Part IV was focused on new National and International Legal Responses to Cybercrime, in particular on the Budapest Convention 10 years on, lessons learnt; the potential new global legal mechanisms on combating cybercrime and global cyber attacks and the current trends in the harmonization of cybercrime legislation.

Each part differs in style and reflects the perspectives of the authors.

To obtain a comprehenisve understanding in the fight against cybercrime,

---

14 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe [COM(2010) 245 final/2].

15 [Official Journal C 115 of 4.5.2010].

16 See part III and part IV.

at substantive criminal law and procedural criminal law level, all views are important, because the legal system's responses have been multifaceted, reflecting the need to combat peculiar types of criminality having different features.

It would be utopian to believe that the criminals of the new millennium do not exploit the opportunities offered by the technological evolution-revolution. It would be equally unrealistic to believe that the fight against these criminals and criminality may be carried out without resorting to the same opportunities[17].

17 R. Flor, *Data retention rules*, cit., 85-86.

OPENING SESSION

KIM IL-SU
President, Korean Institute of Criminology - KIC, Seoul, Republic of Korea

Good afternoon, PNI members, ISPAC representatives, and honored guests.

I would like to formally take this opportunity to relay a warm welcome to each of the delegations from all over the world. I also would like to extend my gratitude to the ISPAC administration for organizing this international Conference.

It is an honorable experience that The Korean Institute of Criminology was able to co-host this Conference with ISPAC on behalf of the PNI family under the theme of "Cybercrime: Global Phenomenon and its Challenges."

The current phenomenon of globalization along with Information Technology advancement has raised various kinds of risks to our society. As you are aware, among these risks, cybercrime has become one of the most conspicuous challenges to the modern society. Newer cybercrime methodologies and patterns are continuously emerging even as we speak. They not only demand imminent strategies for prevention, but also sophisticated investigation tactics.

On a positive note, these challenges will further stretch boundaries for more innovative research and hone new skills that are yet to be developed. I believe that some of the prior efforts that we have dedicated to prevent cybercrime has been very successful. But I also believe that it is a duty for all of us to overcome the inconsistent legal frameworks between criminal justice systems for more coordinated international criminal investigation.

In this era of "Combat against Cybercrime," I would like to lay an emphasis on materializing evidence-based countermeasures. These countermeasures denote exchange of information and knowledge while implementing best practices among relevant institutions at international level. Considering the fact that cybercrime networking operates without a specific jurisdiction, international cooperation and commitment is of crucial importance.

One of the examples of international cooperation for cybercrime prevention would be the "Virtual Forum against Cybercrime." This on-line training program had launched by the Korean Institute of Criminology, in cooperation with UNODC, to train law enforcement and judicial officials. The program also provides all the information related to cybercrime, including criminal statistics, laws, publications, professionals, and events. This program is currently training more than a hundred trainees globally.

It is my wish that our gathering not only enables a productive communication within the PNI members, but also functions as a leverage between the members and the UNODC. I hope that the fellowship and expertise that we share today allows us to mark a turning point in the near future.

I feel very privileged to be a part of this valuable experience today. And I would ask that all the representatives work together to show active support during the presentations and discussions.

Thank you.

KEYNOTE ADDRESS

JOHN SANDAGE
Director, Division for Treaty Affairs and Officer-in-Charge
Organized Crime Branch
United Nations Office on Drugs and Crime - UNODC

Distinguished guests, ladies and gentlemen, friends and colleagues, it gives me great pleasure to be present once again at this ISPAC International Conference – this time on Cybercrime.

As you well know, the focus of this conference is cybercrime as a *global* challenge. In the interconnected world of today we are never far away from the technology that allows us to stay in contact with the office, our family or friends, receive emails to a mobile phone or handheld device, check-in for the next flight, or carry out financial transactions on the move. Some see this as good – how did we ever get along without it all? Some see it instead as the destruction of the last boundaries around our private lives and selves. In any event, the underlying infrastructure, servers and networks – whether wireless or wired – that support such mobility mean data may be routed across multiple national borders many times over in the course of a single connection. Regrettably, the same technology that brings so many benefits also offers new opportunities for crime for those able to exploit weaknesses in this global network, usually for financial gain (whether of an individual or an organized criminal group), but also sometimes with a view to the abuse and exploitation of children, to the spreading of incitement to racial or religious hatred or acts of terrorism, or simply to causing loss or damage to computer systems and data. Such crimes may target computer systems or data directly, representing offences against the *confidentiality, integrity and availability of computer data and systems*, or may be crimes that could be committed without the use of IT technology but are nonetheless facilitated by such technology; so-called *computer or content-related offences*, including computer-related fraud, identity crime, and the production, distribution or possession of child abuse material.

The fact that such acts can occur on a global scale, often with no geographic relationship between victim and perpetrator, is highlighted by data that show the degree to which our world has absorbed this new interconnectivity. Between 2007 and 2008, the number of internet users in low and middle income countries surpassed those in high income countries, at around the three quarters of a billion users mark. Between 2008 and 2009, whilst the number of internet users in high income countries increased by about 36 million, the number of

users in low and middle income countries increased by around 194 million. In 2009, there were 1.3 times as many users in low and middle income countries as high income countries (data from World Bank). In 2010, however, the number of secure internet servers (defined as servers that use encryption technology in internet transactions) was 23 times greater in *high* income countries than *low and middle* income countries, despite the larger proportion of global users in low and middle income countries.

Such figures highlight the challenges when it comes to the effective prevention, investigation and combating of acts of cybercrime at the global level. It is clear from the raw data that international cooperation efforts must engage strongly and equally with all countries.

Whilst computer systems superficially offer an appearance of anonymity for those who would use them to commit criminal offences, in reality – even if technologically challenging to trace – criminal acts in cyberspace frequently leave the equivalent of crime scene 'fingerprints', such as in the form of IP records or changed content data. The legal and logistical challenge is that the 'fingerprints' are often on servers or computer systems in a different physical (and, hence, a different legal) jurisdiction. At this point, the ability of law enforcement authorities to request the preservation of digital evidence from another country in a timely – even 'real-time' – manner is critical. Traditional requests for mutual legal assistance or international cooperation through diplomatic channels may not always deliver results in sufficient time. Networks of 24/7 focal points for cybercrime within law enforcement and government institutions offer one clear model for effective international cooperation. Such network points are able to coordinate requests and, frequently, to provide interim assistance pending a full diplomatic request for mutual legal assistance or decision of the prosecutor or court. The increased involvement of developing countries in such networks will be crucial over the coming years to the development of a truly global response to cybercrime.

In addition to forms of international cooperation however, *national* capacity, *in all countries*, is required for the effective prevention and investigation of cybercrime. Although cybercrime is complex, and with its own unique features, a basic national crime prevention and criminal justice infrastructure is as critical for combating cybercrime as it is for any other form of crime, be it trafficking in narcotic drugs, homicide, or smuggling of migrants. In this respect, UNODC has a comparative advantage as the only intergovernmental organization working on crime prevention and criminal justice at the global level with specialized technical competence, operational capacity and long-term expertise in these areas. Recognising the global challenges of cybercrime, and especially, its potential for a particular impact on the developing world, UNODC adopts an approach to cybercrime based on the following four tenants:

- First, strengthening of legislation and development of training programs for law enforcement personnel, prosecutors and judiciary on cybercrime investigation techniques and criminal justice approaches;
- Second, prevention activities and awareness raising, including through enhanced cooperation between law enforcement institutions and the private sector, and through enhanced public awareness of cybercrime victimization;
- Third, enhanced regional and international cooperation through strengthened cross-national communication and coordination; and
- Finally, data collection, research and analysis on the links between organized crime and cybercrime.

These pillars represent the basis of a holistic and comprehensive response to cybercrime that aims to meet the significant challenges it represents (and no doubt, will increasingly represent in the coming years), in a long-term and sustainable manner. I am sure that at this Conference we will have many opportunities to discuss both the technological challenges associated with the investigation of cybercrime in practice, as well as the legal challenges of adopting appropriate regulatory and criminal law frameworks that are balanced against the need for respect of human rights and fundamental freedoms. I wish you luck in your deliberations and look forward with anticipation to our debate and conclusions over these next days.

Part I

SECURITY AND CIVIL LIBERTIES IN THE FIGHT AGAINST CYBERCRIME

BALANCING LIBERTY AND SECURITY FIGHTING CYBERCRIME: CHALLENGES FOR THE NETWORKED SOCIETY

EMILIO VIANO
Professor, Department of Justice, Law and Society, American University & Washington College of Law, Washington DC, U.S.A.

The internet: the promise and the contradictions

The nature of the internet is quite paradoxical and even contradictory. On the one hand, it has been considered and described as the tool that provides an almost infinite capability for wide human interaction without borders and barriers and at any time of any day, a true and genuine open virtual market of ideas and information that can be shared instantly across the globe. The so-called Arab Spring has demonstrably proven the strong and efficient ability of the internet to provide a worldwide platform for networking, organizing, cooperating, sharing information and plans, organize and coordinate mass events, and defy the establishment. During such heady days, the internet is described as an almost unstoppable mechanism for radical change, a powerful force forging unity of purpose, ideas and action, a fantastic means of instant communications and organizing never before known or tested. Especially the connection between the internet, as the carrier, and the news, often live, being shared worldwide, has brought situations of abuse, exploitation, tyranny and enslavement to the attention of the entire world community, providing the impetus for political and social change and reform, or at least worldwide condemnation, revulsion and, at times, intervention. The social media especially have realized the potential and the reality of the internet as the great connector of the entire world for the masses everywhere there is access. Millions are members of Facebook or similar, engage in instant chat with others who may be half the world away, share instantly photographs and comments or videos depicting a specific situation, and blanket the world with their thoughts, wishes, happiness, achievements and defeats. The very way in which we communicate, learn, get the news, see reality, relate to one another, find friendship, love, companionship, obtain advice and information has changed dramatically from that of the previous generation and is constantly changing with new technological innovations and the never ending introduction of new and improved models of electronics like iPhones, iPads, and other intriguing devices. At the 2012 Las Vegas Consumer Electronics Show a panoply of dazzling new

products were introduced from bigger, brighter, thinner televisions to Ultra Violet, the new "Play Anywhere" format on the home entertainment front, to the Ultrabook, a special, very thin type of laptop, to lots of mobile computing products such as smart phones and tablet computers. The seamless connection between all aspects of life, tasks, places, activities, and communications is astonishing, including many devices that impact every aspect of our daily lives, including smart washers and dryers that adjusts to the type and load of clothes and even send a message to the owner's mobile device when clothes are washed and dried to smart refrigerators that sense when daily food products, scanned when first put into the refrigerator, are almost finished and send a list of what is needed to the purchaser or the store. Electronics are now beginning to truly revolutionize how we drive vehicles as, for examples, increasingly cars will be able to communicate with each other and make decisions relative to speed, directions, and distance from other cars, even able to override the driver's commands.

On the other hand, in sharp contrast, the internet can also be exactly the opposite: an implacable and super-efficient tool giving multiple parties the ability to conduct 24/7 surveillance of people, places, movements, communications and exchanges[1]. It can help an authoritarian regime conduct around the clock surveillance to identify and neutralize dissenters, challengers and reformers; it can pinpoint and lead the forces of repression to where the voices of change come from, for those people to be arrested, tortured, silenced, even killed; it can become an instrument of terror, the tool of the omniscient, omnipresent, omni-viewing "Big Brother". It can track the purchases of millions of consumers worldwide, producing vast information on lifestyle, eating and drinking habits, personal hygiene and sexual behaviors that can then be used against the citizen for employment, promotion, insurance, accidents investigations, criminal prosecution and, at times, extortion. It is used as a marketing, advertising, news filtering and propaganda machine to diffuse certain approved messages, indoctrinate, and control the mind of a people; and much more. The Panopticon, conceived and

---

[1] Julian Assange, Internet has Become a Surveillance Machine, Agence France Presse, November 28, 2011, *https://www.commondreams.org/headline/2011/11/28-1*; Paul Sonne, (U.S. Secretary of State Hillary) Clinton Criticizes Sale of Surveillance Tools to Some Countries, Wall Street Journal, December 8, 2011, *http://blogs.wsj.com/digits/2011/12/08/clinton-criticizes-sale-of-surveillance-tools-to-some-countries/*; Jillian York, Government Internet Surveillance Starts with Eyes Built in the West, Electronic Frontier Foundation, September 2. 2011, *https://www.eff.org/deeplinks/2011/09/government-internet-surveillance-starts-eyes-built*; David Eaves, The Internet as Surveillance Tool, http://eaves.ca/2010/01/20/the-internet-as-surveillance-tool/, 20 January 2010

designed by the 18th century philosopher Jeremy Bentham, was supposed to allow for a government officer, a prison guard, to observe (*-opticon*) all (*pan-*) prisoners in an institution without them being able to tell whether or not they were being watched[2]. This was meant to create fear, insecurity, doubt, uneasiness and to control the masses simply with the possibility of the tyrant spying on them while living their daily lives and intervene punitively to stamp out any perceived deviation. The internet can be described as today's growing Panopticon, especially when paired with other electronic technology that can capture our whereabouts, activities, and location around the clock, if necessary or desired, and record and store permanently the sequence of our everyday activities[3].

This stark contrast in the nature and functioning of the internet often passes unperceived or unknown[4]. Most people act and communicate using electronic devices as if they are in their own private world, totally insulated from the surrounding world of marketing, surveillance, tracking by means of cookies, law enforcement, listening in by intelligence agencies, and monitoring on the part of their employers[5]. Especially when using social media, people act as if they have complete anonymity, as if they live, interact and communicate in their own little bubble world, while in actuality there is constant, persistent and aggressive monitoring 24/7[6].

The Internet: constitutional issues

The monitoring capability of electronic devices raises profound and troubling constitutional issues in the United States and elsewhere[7], especially at

---

2 *http://en.wikipedia.org/wiki/Panopticon*

3 For a discussion of Panopticism, see Sonia Katyal, The New Surveillance, 54 Case Western L.R. 318 (2004)

4 The Emergence of Cyber-Security as a Policy Driver, The American Journal of International Law, 102 , 3 (July 2008), 650

5 The unique challenges of balancing communications, business, and economic advantages of the so-called Information Revolution with conservative cultures and/or religions are illustrated in Joshua Teitelbaum, Dueling for Da'wa: State v. Society on the Saudi Internet, Middle East Journal 56, 2 (Spring 2002), 222-230; Garry Rodan, The Internet and Political Control in Singapore, Political Science Quarterly 113, 1 (Spring 1998) 63-89

6 Lawrence Lessig, The Architecture of Privacy: Remaking Privacy in Cyberspace, 1 Vand. J. Ent, L. & Prac., 56, 61 (1999)

7 A.G. Noorani, Cyberspace and Citizens' Rights, Economic and Political Weekly, June 7, 1997, 1299.

the intersection of the right to privacy and the right to property[8]. The right to privacy refers to users of electronics, especially for social communications and entertainment purposes[9]. The right to property is generally exercised by all those involved in the conception, execution, distribution and licensing of media entertainment and general intellectual property[10]. Powerful "Hollywood", "Bollywood" and similar companies in the movie, music, sports and entertainment worlds belong to this latter category. Normally, obtaining incriminating evidence on anyone in the United States is regulated by the Fourth Amendment to the United States Constitution. It is the part of the Bill of Rights which is meant to protect against unreasonable searches and seizures. It also requires that any warrant be approved by a magistrate and supported by probable cause. Search and arrest should be limited in scope according to detailed information provided to the court or magistrate issuing the warrant, generally by a law enforcement officer, who swears to its truthfulness. It is important to note that in *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court decided that the protections provided by the amendment apply only when the person being searched has a "reasonable expectation of privacy". A major test of the meaning and reach of the Fourth Amendment protections has been considered by the U.S. Supreme Court in its 2011-12 year. The case was argued on November 8, 2011 and is probably the most important and challenging case of the year. *United States v. Jones* (No. 10-1259) raises the question of whether it is a search or seizure under the purview of the Fourth Amendment when the police plant a GPS device on a person's vehicle and monitor it for 24 hours a day, for 28 days.[11] Since 1967, when *Katz v. United States* was decided, the Supreme Court has limited the protections of the Fourth Amendment to a "reasonable expectation of privacy." The challenge is to apply it to the *Jones* case. On the one hand, the court has consistently decided that people have no expectation of privacy when they engage in their public activities. Undercover police officers could have followed Jones' car on the public streets for a month

---

8 Sonia K. Katyal, The New Surveillance, 54 Case W. Res. 302 (2004)

9 Right to Privacy on the Internet, Internet and Intellectual Property Justice Clinic, University of San Francisco Law School, 2011, *http://internetjustice.blogspot.com/2010/06/right-to-privacy-on-internet.html*

10 WIPO, Intellectual Property Rights on the Internet: A Survey of the Issues, 2011; *http://www.wipo.int/copyright/en/ecommerce/ip_survey/*

11 Adam Liptak, Court Case Asks if "Big Brother" is Spelled "GPS". *The New York Times*, September 10, 2011, *http://www.nytimes.com/2011/09/11/us/11gps.html*; U.S. vs. Jones, *http://www.scotusblog.com/case-files/cases/united-states-v-jones/*; see also: *https://www.eff.org/cases/us-v-maynard*

and there would not have been an issue of a search or seizure requiring a warrant. On the other hand, citizens expect that police will not be planting an electronic device on their car to spy on everything they do. This also because, with the exponential growth of the technology useable for tracking people, police are increasingly better equipped to follow anyone at any time, even without leaving the police station. One can find out a lot of personal information by following somebody electronically for weeks.[12] An important element in this case is determining the key variable, the "reasonable expectation of privacy", what it is, what it entails. Too often this has been treated as a very elastic, almost disposable item that can be modified at will by Justices who live protected and very private lives not generally available to normal citizens and do not suffer the indignities at times associated with police or immigration authorities encounters.

The U.S. Supreme Court decided that, "Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment."[13] The decision of the Court will have major repercussions on the use or abuse of electronic technology by law enforcement and the private sector. For example, the fact that drones have already been used within the United States for law enforcement purposes[14] and that technology exists to find out, even to see, what goes on in the privacy of a home from the outside or through the screen of a laptop or other electronic device is a source of major concern.

A major problem with this "reasonable expectation of privacy" test is that the government seemingly can nullify it just by deciding and telling people not to expect any privacy in a particular area. The test is not based on empirical research, public opinion polls, or community-based values. It is totally decided by the courts and/or the government without any democratic input. The Fourth Amendment in turn connects to the Exclusionary Rule which is the way in

---

12 The U.S. Court of Appeals for the District of Columbia Circuit rejected the government's assertion that federal agents have an unlimited right to install Global Positioning System (GPS) location-tracking devices on anybody's car without a search warrant. *U.S. vs. Jones*, 584 F.3d 1083, 1086 (D.C. Cir. 2009)

13 U.S. vs. Jones, No. 10-1259, Argued on November 8, 2011; decided on January 23, 2012, at 1

14 Brian Bennett, Police employ Predator drone spy planes on home front, *Los Angeles Times*, December 10, 2011.
http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211**;** *U.S.* News - Report: US drones helping local police agencies, December 11, 2011; *usnews.msnbc.msn.com/_.../9360170-report-us-drones-helping-local*

which the courts enforce the Fourth Amendment[15]. The central point of the rule is that evidence obtained by violating the Fourth Amendment is generally inadmissible in court at the defendant's criminal trial. In addition and importantly, in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920) and *Nardone v. United States*, 308 U.S. 338 (1939), the Supreme Court decided that information and tips resulting from illegally obtained evidence also cannot be used in trials because they are considered "fruit of the poisonous tree"[16]. The main purpose of the rule is to discourage police officers from violating a suspect's Fourth Amendment rights on purpose, willfully. The rationale behind the exclusionary rule is that if the police know that evidence obtained violating the Fourth Amendment cannot be used to convict an accused of a crime, they will respect it.

The internet and the exclusionary rule

Several exceptions to the exclusionary rule have been recently allowed by the U.S. Supreme Court in part in response to and to appease aggressive criticism of the rule on the part of law enforcement and "law and order" politicians as hampering the successful investigation of crime. Thus, the impact and effectiveness of the doctrine has been reduced. Many believe that the rule as it exists today is but a shadow of its original version. An important exception that significantly comes into play in the electronic world of today is that evidence obtained through a search conducted by private parties, without the authorization of a magistrate, is not excluded from trial, provided that the search was not at the direction or under the supervision of law enforcement officers[17].

In other words, while the Exclusionary Rule is designed to protect privacy rights, the Fourth Amendment controls only the behavior of government officials [Bordeau v. McDowell (256 U.S. 465 (1921)]. Thus there is no constitutional limitation or exclusion when all the parties are private ones.

This major exception to the protection of privacy comes into play, for example, when private entities monitor electronic transmissions to control the use of copyrighted material. When private parties monitor the internet to discover infringement, there is a clear danger that they may abuse the copyright law to the detriment of privacy. In other words, legally, the commitment to property trumps the commitment to privacy. The first is much stronger than the

15 *http://en.wikipedia.org/wiki/Exclusionary_rule*

16 *http://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree*

17 *http://www.enotes.com/exclusionary-rule-reference/exclusionary-rule*

latter. As it often happens, the law more readily protects economic and property interests than human and privacy rights[18]. Again we are reminded of the Panopticon symbolism: there is constant, silent, pervasive surveillance out there – irrespective of our privacy rights – meant to discover copyright infringement. Ironically, it is the very cyber networks that allow the easy flow of communications and sharing that also make us vulnerable to constant, unannounced, unperceived surveillance meant ultimately to support and maintain a certain structure of power and economic gain to the detriment of the free flow of ideas that would successfully introduce innovations and allowing artistic expression[19]. The legality of this invasion of privacy is supported by the U.S. Supreme Court's stressing that, to have a seizure that may be regulated and excluded by the Fourth Amendment, there has to be something tangible and tied with the notion of physical trespassing. Thus, in reality, what is most important for the Court is not so much our expectation of privacy but the concreteness, the materiality of the objects searched for and seized. Basically, if there is not something to be touched, taken away physically, catalogued and stored in a "property room" at the police station, there is no search, there is no seizure, there is no protection based on the U.S. Constitution.

This approach is very evident in the landmark *Olmstead* decision[20] that decided the question whether or not using wiretaps outside the walls of the house and office of the suspect was a "search" within the meaning of the Fourth Amendment. Because there was no window pried open, or door forced open, or lock picked, in other words, there was no "materiality", the Supreme Court, in the words of Justice Taft, decided that, "There was no searching… there was no seizure… The evidence was secured by the sense of hearing and that only[21]." In conclusion, since there was no common law trespass, no entry of the house or office of the suspect, the Court found there was no invasion or violation by the government of a privacy interest protected by the Fourth Amendment. Again, for the Court, what counted was really not the suspect's expectation of privacy but, rather, the presence or absence of materiality in the government's actions.

---

18 Gavin Skok, Establishing a Legitimate Expectation of Privacy in Clickstream Data, 6 Mich. Telecomm Tech. L. Rev. 61, 72 (2000), available at *http://www.mttlr.org/volsix/skok.html*

19 Andrew C. Payne, Twitigation: Old Rules in a New World, 49 Washburn L.J. 841, 861 (2010), available at *http://www.washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf*

20 Olmstead v. United States, 277 U.S. 438 (1928), partially overruled by Katz v. United States, 389 U.S. 347 (1967)

21 Olmstead, 277 U.S. at 464

Consequently, *Olmstead* eliminated a vast array of potential violations of privacy from the purview of the Fourth Amendment.

Very noteworthy are the far-viewing dissenting words of Justice Brandeis who stressed the need for flexibility and adaptation to technological changes and advances by the Constitution and its Amendments in order to protect the citizen from abuse of power. With prescient lucidity and futuristic vision, Brandeis predicted that more unobtrusive but also more effective ways of invading privacy may someday be developed "by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home[22]." Thus, for Justice Brandeis, it did not have any significance that in *Olmstead* the wiretapping connection was made on telephone lines outside the home. Privacy can be violated without necessarily involving physical trespassing[23]. The dissent by Brandeis in Olmstead has been analyzed and written about by many legal scholars thinking of subsequent technological innovations and especially of the developing realm of electronic surveillance. Among them, Lawrence Lessig[24] has eloquently written that:

"Even in 1928, much of life had moved onto the wires, and in those first steps into cyberspace, Brandeis argued, the Constitution should not leave the citizens exposed. What had changed, he argued, were a technology of surveillance and a technology of communication. Life existed now in cyberspace, and the Constitution should be read to protect the same interests of privacy in cyberspace that the Framers had protected in real space. Technology had changed, but, Brandeis argued, that change should not be allowed to change the meaning of the Constitution."

The right to property prevails: the case of Napster

A very good example of this dynamic was the case of Napster which was originally established in 1999 as a pioneering peer-to-peer file sharing Internet service. It specialized in sharing audio files, typically music, encoded in MP3 format, through a user-friendly interface[25]. Napster made it fairly simple for music enthusiasts to download copies of songs that were otherwise hard to

---

22 Id. at 474 (Brandeis, dissenting)

23 Id. At 478 (Brandeis, dissenting)

24 Lawrence Lessig, Reading the Constitution in Cyberspace, 45 Emory L.J. 872 (1996)

25 *http://en.wikipedia.org/wiki/Napster*

obtain, like older songs, recordings not yet released, and songs from unauthorized concert recordings[26]. It became extremely popular among young people, especially college students, to the point that many universities had to block its use on campus networks, initially because of the overloading of their operating systems and then also because of copyright infringement liabilities. The original company ran into legal difficulties over copyright infringement, and had to cease operations by court order in 2001.

All of this was accompanied by a fierce debate on the issues: on the one hand, the Recording Industry Association of America maintained that Napster was hurting sales of recordings[27] and depriving artists and others of their legitimate earnings[28]. Others instead demonstrably claimed that the contrary was true, showing that file trading on the internet stimulated rather than hindered sales, especially for songs by less known artists and bands and that Napster actually enriched the music and entertainment world by giving a chance and providing a stage to groups that were not part of the establishment[29].

In a sense Napster represented what has become increasingly one of the more powerful consequences of the universal development and use of the internet: the revolutionary change and opening up of the power and financial structure of the news, music, entertainment and culture worlds, until recently rigidly controlled by established customs and arrangements, often backed up by laws not surprisingly enacted at the urging of those benefitting the most from the monopolies[30].

The technological transition of the music culture is an amazing one. Music as we heard it has disappeared and has been replaced by music as we rip it. We listen to it on our desktop, laptop, iPod, etc. Sales of CDs have plummeted as there aren't any more many buyers for them, as music becomes available for listeners on the www. Nobody saw the revolution coming in when MP3 files surfaced in the mid-nineties. The recording industry, especially, had not anticipated or prepared for what was to hit them, especially the peer-to-peer

---

26 Cohen, Warren. Napster is Rocking the Music Industry. U.S. News & World Report, 6 March 2000: 41-54.

27 Gillen, Marylin A. Study: Napster Eroding Retail, .Billboard 3 June 2000: 5-

28 Courtney Macavinta, Recording Industry Sues Music Start-up, Cites Black Market, CNET News, December 7, 1999 *http://news.cnet.com/Recording-industry-sues-music-start-up,-cites-black-market/2100-1023_3-234092.html*

29 Tully, Shawn. Big Man Against Big Music. Fortune, 14 August 2000: 186. Vogelstein, Fred. Is It Sharing or Stealing? U.S. News & World Report 12 June 2000: 38-40

30 Jeffrey, Don. The Evolution of E-Music and Its Consumers, Billboard 4 March 2000: 104.

nature of the exchange, bypassing the client-server Web architecture served and controlled by Internet Service Providers (ISPs)[31].

Today, rigid professional lines and roles have been greatly softened and in many cases, may even disappear. Anyone can be a reporter, a journalist, a musician, an artist, an expert etc. directly, publishing, performing and seeking a following on the internet, without necessarily having to pass through and be anointed by a power and financial structure that engages in monopolistic and closed shop practices or having to pay for and earn expensive degrees to just get an entry job in journalism. Napster for example was instrumental in launching the then totally unknown English rock-band Radiohead and taking one of its songs to number one on Billboard 2000, something unheard of at the time. It was a revolutionary step challenging the hierarchy of the media and entertainment worlds and their arrangements[32]. The courts however sided with property rights. There is no question that the Napster decision by the Court of Appeals for the 9th Circuit [.A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)] was a major blow to file sharing and to freedom of expression and innovation in the entertainment world[33].

Private surveillance and enforcement: Due process challenges

Napster was the beginning of a trend whereby a copyright holder is free to exercise vigorous surveillance and monitoring of electronic communications, regardless of the privacy rights of other parties. The surveillance is extra-legal, performed as it is by a private, non governmental body and often it leads to an extrajudicial conclusion of copyright infringement. Monitoring is normally done with so called "smart agents"[34] that detect copyright violations and allow

---

31 Manoj Nair, Cry Freedom is Sound Music, India Times, November 19, 2009; *http://articles.economictimes.indiatimes.com/2009-11-19/news/27644975_1_music-files-international-albums-recording-industry*; Sonia Katyal, The New Surveillance, 54 Case Western L.R. 310-311 (2004)

32 Abbie Woefel, The Napster Phenomenon: Turning the Music Industry Upside Down, *murphylibrary.uwlax.edu/digital/jur/2001/woelfel.pdf*

33 Jeffrey Brenner, Napster Fallout: Privacy Loses?, Wired, 03/06/01, *http://www.wired.com/politics/law/news/2001/03/42203*; Sonia Katyal, The New Surveillance, 54 Case Western L.R. 326 (2004)

34 For more analysis on the legal and philosophical notions of piracy in the context of artificial agents see Samir Chopra and Lawrence White, Privacy and Artificial Agents, or, Is Google Reading My Email? *http://www.sci.brooklyn.cuny.edu/~schopra/choprawhite497.pdf*

copyright holders to rapidly identify and get in touch with the infringer[35]. It is essential to recall that, at this point in the U.S. legal system, there are no Constitutional protections if both parties are private, non state entities[36].

Consequently, different fundamental concepts like property, privacy, personhood and autonomy (under the Digital Millenium Copyright Act- of 1998-DMCA[37]) are clearly in conflict. Piracy surveillance as it is practiced today raises considerable due process challenges: there is unofficial, private enforcement, unwanted and unauthorized surveillance, and extra-judicial determination of infringement.

As Sonia Katyal aptly states, we are now publishing in a system of "panopticon publication", that is, for all to see right away without us being aware of it, and are thus liable to being found extra judicially in violation of copyright. The copyright owner has almost complete capacity to monitor the use of that work by others, evading considerations of fair use and free expression (First Amendment) and, moreover, under the Digital Millenium Copyright Act (DMCA), to out any author on the internet even with only a minimal accusation of a violation[38].

There is no question that there is a need for more legal protections here[39]. One of the consequences of the post-Napster legal climate is that there is less legitimate creativity and expression that is innovative and not vetted and channelized through the usual corridors of power, control and at times corrupt practices meant more to protect the established financial interests of media moguls and of the big studios than to promote literary, artistic and creative expression. Thus, there is significant impact on privacy, freedom of expression and the copyright itself.

An inverse relationship is operating here and is continuously expanding: the more copyrights holders can protect their property, the less information privacy there will be[40]. Basically, what is taking place with the support of favorable laws lobbied for by major entertainment and media

---

35 *http://en.wikipedia.org/wiki/SMART_Agent*; Sonia Katyal, The New Surveillance, 54 Case Western L.R. 341, 356-57 (2004)

36 David Navetta, The Law of Privacy on Social Networks, InfoSec Island (Oct. 20, 2010), *https://www.infosecisland.com/blogview/8917-The-Law-of-Privacy-on-Social-Networks.html*.

37 *http://www.copyright.gov/legislation/dmca.pdf*

38 Sonia Katyal, The New Surveillance, 54 Case Western L.R. 360 (2004)

39 For a current list of cases in the U.S., see the Citizens Media Law Project, *http://www.citmedialaw.org/threats/popular*

40 Sonia Katyal, The New Surveillance, 54 Case Western L.R. 360 (2004)

businesses and the agreement of the courts[41] is to institute a "stand-alone, self-contained regime, where copyright issues are resolved without attention to other common law or constitutional values like due process, freedom of speech, or privacy[42]."

Hollywood versus Silicon Valley

This approach that gives property rights supremacy over privacy and freedom of expression continues to generate considerable controversy[43] especially in the United States with the proposed "SOPA" and "PIPA."

---

41 Analyses of cases where the courts ordered the disclosure of private social media communications:
Molly DiBianca, Romano v. Steelcase: Defendant Granted Discovery of Plaintiff's Facebook Profile, Delaware Employment Law Blog (Sept. 27, 2010), *http://www.delawareemploymentlawblog.com/2010/09/romano_v_steelcase_defendant_g.html.*
Marc J. Smith, Court Orders Facebook to Produce "Private" Information, Maryland Employment Law Blog, (Sept. 27, 2010, 7:02 PM), *http://www.slgemploymentlaw.com/blog/2010/9/27/court-orders-facebook-to-produce-private-information.html.*
Noeleen G. Walder, Judge Grants Discovery of Postings on Social Media, Law.Com (Sept. 24, 2010), *http://www.law.com/jsp/law/article.jsp?id=1202472483935*.
Alexandra A Filutowski, "Friends Only" Privacy Settings On Facebook Don't Protect You From Insurance Companies, Filutowski Law Blog (Sept. 27, 2010), *http://www.filutowskilaw.com/2010/09/friends-only-privacy-settings-on-facebook-dont-protect-you-from-insurance-companies*.
Vincent Cino, Labor: "Private" Social Networking Activity Can Be Discoverable, Inside Counsel (Oct. 25, 2010), *http://www.insidecounsel.com/Exclusives/2010/10/Pages/Private-Social-Networking-Activity-Can-Be-Discoverable.aspx*.
Gary Long, Greg Fowler & Simon Castley, New York Trial Judge Orders Access to Private Facebook® and MySpace® Postings, Lexology (Sept. 30, 2010), *http://www.lexology.com/library/detail.aspx?g=09503f39-1202-4775-85b0-703810bdf0d7*
Eric Goldman, Deleted Facebook and MySpace Posts Are Discoverable – Romano v. Steelcase, Technology & Marketing Law Blog (Sept. 29, 2010), *http://blog.ericgoldman.org/archives/2010/09/deleted_faceboo.htm*

42 Sonia Katyal, The New Surveillance, 54 Case Western L.R. 370 (2004)

43 Robert Litan and Peter Orszag, A Complicated Intersection: Public Action to Protect Private Property, Brookings Review, 20, 3 (Summer 2002) 20.

The Stop Online Piracy Act (SOPA) (H.R. 3261)[44] is a bill that was introduced in the United States House of Representatives on October 26, 2011[45]. The proposed bill would empower the U.S. Department of Justice and private copyright holders to seek court orders against websites suspected or accused of enabling, facilitating or supporting copyright infringement. The court orders may include prohibiting online advertising networks and payment services, like PayPal, from doing business with the website alleged to be infringing, stopping search engines from providing links to such sites, and ordering that Internet service providers block access to such sites. The most immediate outcome would be that a simple accusation, still to be proven, would put a website out of business. The bill would require Internet service providers to block access to certain foreign websites considered "rogue sites"[46].

SOPA criminalizes the unauthorized streaming of copyrighted content. Most importantly, the bill also provides immunity for Internet services that, on their own private, non-judicially sanctioned initiative, act against websites accused of infringement.

Those who support and champion the law claim that it protects the intellectual property market and the related industry, numerous jobs and considerable earnings. They also claim that the law is necessary to reinforce the enforcement of copyright laws, especially against foreign websites out of reach of the U.S. laws. The emotional card of foreign websites stealing with impunity American ideas and therefore jobs and income is also conspicuously plaid[47].

---

44 *http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act*

45 In the wake of major protests against SOPA and PIPA during January 2012, the U.S. Congress postponed key votes on both laws. Proponents of the laws in Congress agreed to consider substantial revisions and obtaining consensus around the issues. One of the acts of protest was the 24-hours closing of the English version of the very popular Wikipedia and of other websites.

46 Laurence H. Tribe, The SOPA Violates the First Amendment, Tribe Legis Memo, 12/6/11; *http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1*

47 Beth Marlowe, SOPA (Stop Online Piracy Act) debate: Why are Google and Facebook against it?, Washington Post, November 17, 2011, Business Section; *http://www.washingtonpost.com/business/sopa-stop-online-piracy-act-debate-why-are-google-and-facebook-against-it/2011/11/17/gIQAvLubVN_story.html?tid=pm_business_pop*

Opponents instead state that the proposed law violates the First Amendment[48], is basically censorship on the internet[49], will do a lot of damage and engender paralysis on the Internet,[50] and will discourage, even punish, innovation by businesses, large and small, and whistle-blowing and other forms of free speech while protecting the status quo and the de facto existing monopolies[51].

Closing down an account is a major, potentially embarrassing, damaging, dramatic event, the modern equivalent to being socially excluded, excommunicated, that is ejected without further protection by the group, having one's goods confiscated. It may actually mean, at times without warning, the loss of all the virtual assets that one has stored in the account. This is really damaging where in today's virtual world one may have obtained substantial assets. Moreover, there is always the loss of time, money invested, and reputation. Examples are email social networking and web hosting cancellations[52].

International privatization of enforcement

It must be noted that this type of legislation is not unique to the United States. In France, for example, similar legislation directed at the user-pirate went into effect on January 1, 2010. The law established the Haute *Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet,*[53]

---

48 Laurence H. Tribe, The SOPA Violates the First Amendment, Tribe Legis Memo, 12/6/11; *http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1*

49 Chloe Albanesius, SOPA: Is Congress Pushing Web Censorship?, PC Magazine, November 16, 2011; *http://www.pcmag.com/article2/0,2817,2396518,00.asp?obref=obinsite*

50 Chloe Albanesius Will Online Piracy Bill Combat 'Rogue' Web Sites or Cripple the Internet?, PC Magazine, November 1, 2011; *http://www.pcmag.com/article2/0,2817,2395653,00.asp#fbid=6r9KNM2HX7x*

51 Trevor Timm Proposed Copyright Bill Threatens Whistleblowing and Human Rights, Electronic Frontier Foundation, November 2, 2011 *https://www.eff.org/deeplinks/2011/11/proposed-copyright-bill-threatens-whistleblowing-and-human-rights*

52 Eric Goldman**,** "Online User Account Termination and 47 U.S.C. §230(c)(2), *digitalcommons.law.scu.edu/facpubs/124/*

53 High Authority for the Diffusion of (Cultural) Works and the Protection of (Intellectual Property) Rights on the Internet

generally known by its abbreviation, Hadopi[54]. Hadopi enforces the anti-pirating law which has been conceived as a "Three-strikes-you-are-out" type of law. The copyright holders depend on a private company, Trident Media Guard located in Nantes, to monitor the internet and identify the IP address of violators. To catch violators the music industry has prepared a database of 10,000 snippets of the most popular songs that are often downloaded illegally. The IP addresses of the violators are then sent to Hadopi that in turn demands names and addresses from the ISPs. Upon the first detected violation, Hadopi sends an email demanding compliance. Upon the second, a registered letter is also sent. Upon the third, Hadopi can initiate a criminal prosecution which entails a fine of euro 1,500. In the case of an appearance in front of a judge, there is no right to contest the accusation. Depending on the circumstances and seriousness of the offense, a third-strike violator may also be deprived of the internet connection and forbidden to acquire another one under a different name or from a different ISP while continuing to pay the fees of the blocked internet service. One subtle legal twist of Hadopi is that the violator is not accused of being a pirate but of not having stopped the piracy from happening. It is treated as a failure to act, as negligence, as a strict liability crime. Consequently, the offender's electronic device will be equipped with a monitor to stop future transgressions. Software firms are busy writing programs that accomplish this mission. On the other hand, Hadopi is charged with identifying legal downloading opportunities and labeling them as such so that people can be guided to respect property rights and download music and other material legally. The potential of Hadopi is that many, if not most, laptops and other electronic devices in France may be monitored in the near future. One thinks instinctively of "Big Brother" constantly watching what French internauts are doing electronically. It is indeed ironic that the internet, hailed as the global vehicle for free speech and expression, may instead become a major wiretap project in France and elsewhere[55].

It is alleged that a similar "Three Strikes" provision was being considered for inclusion in the Anti-Counterfeiting Trade Agreement (ACTA). The objective of the Agreement is to establish international standards for the enforcement of intellectual property rights and thereby confirm the current existing proprietary and monopolistic order. This Agreement was first proposed by the United States and Japan, and negotiated in secrecy between various countries: the United States, the European Union, Switzerland, Japan,

---

54 *http://www.rue89.com/2010/10/08/lhadopi-expliquee-aux-nuls-et-a-ceux-qui-piratent-sans-le-savoir-169745.*

55 David Eaves, The Internet as a Surveillance Tool, January 20, 2010; *http://eaves.ca/2010/01/20/the-internet-as-surveillance-tool/*

Australia, the Republic of Korea, New Zealand, Mexico, Jordan, Morocco, Singapore, the United Arab Emirates, and Canada. Civil society and developing countries were excluded from the negotiations. It is noteworthy that in ACTA counterfeiting includes "internet distribution and information technology."

The final text was released, still under conditions of secrecy, on November 15, 2010. A signing ceremony was held on October 1, 2011 in Tokyo, with the United States, Australia, Canada, Japan, Morocco, New Zealand, Singapore, and South Korea signing the treaty. The Agreement has been widely challenged and criticized for the secrecy of the negotiations, for the imposition of public policy without open discussion and judicial oversight, and for the threat it poses to human right and the freedom of expression[56]. A conference on ACTA was held at the Washington College of Law in Washington DC on June 16-18, 2010. It was attended by over 90 academics, practitioners and public interest NGOs who expressed profound concern on many aspects of ACTA as threatening many public interests[57].

Other laws similar to SOPA and ACTA have been proposed or introduced elsewhere. Spain has the Law on a Sustainable Economy or SINDE law[58] approved on December 31, 2011. Wikileaks has published a large number of communications and documents showing that it was proposed in March 2010 and then approved under considerable pressure from the United States and strong lobbying by the major U.S. media and entertainment industries. It has a component, the Law on the Services of the Information Society, which covers copyright enforcement and is somewhat similar to Hadopi[59]. In Mexico there has been a proposal to revise the main federal law on Copyrights and Industrial Property to basically make it a Mexican version of the U.S. SOPA.[60]

---

56 *www.eff.org/issues/acta -*

57 *http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement; https://www.eff.org/issues/acta*

58 "Sinde" is the family name of the Culture Minister of Spain at the time who championed the bill.

59 *http://www.ticbeat.com/tecnologias/aprobada-ley-sinde/; http://es.wikipedia.org/wiki/Ley_de_Econom%C3%ADa_Sostenible; http://alt1040.com/2011/01/que-es-la-ley-sinde*

60 *http://www.argenpress.info/2012/01/la-sopa-y-la-doble-cara-de-la-propiedad.html*

Free expression, the Arab Spring and SOPA

Against the background of the heady events surrounding the Arab Spring and other similar reform and democratization movements, an argument also made by SOPA opponents is that proxy servers, such as those used during the Arab Spring to inspire and coordinate the movement, can also be used to oppose copyright enforcement and thus, under SOPA, may be made illegal, and shut down[61]. This would have deprived those insurgencies, protest and democratization movements of their most essential tool to have a chance of succeeding. There are those who warn that SOPA would also have devastating consequences on online communities and social media, like Facebook and others. For example, holding companies liable for the actions of users may have a chilling effect on sites like YouTube that post and make available materials generated by the users[62]. Quite worrisome is that SOPA would override the "safe harbor" provision provided by the Millenium Digital Copyright Act of 1998, by permitting judges to stop right away access to any website found guilty of hosting copyrighted material, technically even if it is only one time out of thousands. This would constitute an approach majorly lacking in balance and proportionality, quite damaging and disruptive. It is seen by many opposing it as an effective tool to guarantee the basic status quo and not allow the next upstart challenge to Google, Facebook, YouTube or the next videogames developer to have a chance at succeeding. It is argued that this would definitely impoverish innovation and competition in internet offerings and slow down the development of the internet as an integral and essential mechanism for a globalizing world[63]. Startups ahead of where the mainstream is may not be able to take hold and flourish because they would be very vulnerable to accusations of infringement that would effectively and easily open the door to their being closed down. They could easily be put out of business simply with an accusation of copyright infringement by private parties. Even if they could obtain redress through litigation, the "David and Goliath" type of unequal economic power would deter any startup from even trying, given the substantial costs involved and the time lag generated by the

---

61 *http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act#cite_note-eff-26*

62 *http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act#cite_note-Stop_the_Great_Firewall_of_America-31*

63 SOPA/PIPA Discussion: Internet Censorship & the Attack on Tech Innovators, Huffington Post, January 17, 2012, Politics Section; *http://www.huffingtonpost.com/2012/01/17/sopa-pipa-internet-censorship_n_1210614.html*

typical judiciary case that would obviously make any victory for the upstart a Pyrrhic one. Thus, once again, there is a clash here between privacy and intellectual property. Both terms are rather poorly understood and even more poorly defined.

Privacy in American jurisprudence

The legal status of privacy in American jurisprudence is relatively weak, especially after the terrorist events of 9/11[64]. It is not a constitutional right clearly defined and expressed in the Constitution or the Bill of Rights[65]. It exists thanks to a U.S. Supreme Court determination that found it in the "penumbra" of other rights explicitly recognized in the Bill of Rights. The conceptual and juridical history of "privacy" is quite complex. A pivotal case in American constitutional and judicial history is that of *Griswold v. Connecticut* [381 U.S. 479 (1965)][66] with the majority opinion delivered by Justice Douglas. In the *Griswold* case, appellants Estelle Griswold, executive director of the Planned Parenthood League of Connecticut, and Dr. C. Lee Buxton, a medical professor at Yale Medical School and director of the League's office in New Haven, were tried and convicted for prescribing contraceptive devices and also giving advice about contraception to married persons in violation of a Connecticut law. They challenged the constitutionality of the statute, which made it a crime to use any drug or medicinal tool to prevent conception, on behalf of the married persons they were professionally involved with. The Supreme Court decided that the Connecticut statute was unconstitutional because it violated a person's right to privacy. In his opinion, Justice Douglas wrote that the specific guarantees of the Bill of Rights have penumbras "formed by emanations from those guarantees that help give them life and substance," (381 U.S. 479)[67] and that the right to privacy can be found within this shadowy area. Since *Griswold*, the penumbra doctrine has principally been used to acknowledge and discover implied powers that derive

---

64 John D. Podesta & Ray Goyle, Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World, Yale Law & Policy Review, 23, 3 (Spring 2005) 509

65 Otis H. Stephens and John M. Scheb, American Constitutional Law. New York: Harcourt, Brace, Jovanovich, Digitized September 30, 2008

66 *law.umkc.edu/faculty/projects/ftrials/conlaw/griswold.html*

67 Stephen Kanter, The Griswold Diagram; Toward a Unified Theory of Constitutional Rights, 28 Cardozo Law Review 623 (2006); *http://www.cardozolawreview.com/content/28-2/KANTER.WEBSITE.pdf*

from a specific rule, thus increasing the meaning and reach of the rule into its outlying areas or penumbra[68].

Contrasting the right to privacy to be found in the penumbra of other rights versus property rights, one can easily see the difference in power, established statutory and case law, tradition and holding power[69]. Property law has been in existence for centuries and is amply recognized and firmly established. Privacy is recognized in U.S. law somewhat since the late 19th century and more clearly only since 1965. Its legal foundations are shaky, depending as they are on the interpretation of the Court. A penumbra is not something where we can see clearly and distinguish features like under the glaring light of the sun. Thus, there is ambiguity, room for disagreement, illusion, potential for mistakes and possibilities of reversals.

Another important consideration is the historical circumstances surrounding the writing of the U.S. Constitution and of the Bill of Rights. At that time the main concern was to protect the citizen, mostly the upper and middle landed classes, from the excessive intrusion of the government, based on the negative experiences with the colonial English government. There was no thought or conception of private entities, like powerful, global, multinational corporations, having power similar, equal to or even stronger than that of the official government to interfere in the free life of the citizen. In a predominantly rural society, where the landed gentry normally owned large tracts of lands and the nearest neighbor may live several miles away, requiring a day long journey and an overnight stay for a visit, privacy relative to intrusion by private parties was taken for granted. There was no reason to expect or even imagine this type of trespassing. This is why today a defense against the intrusion of a corporation or business entity into the life of a citizen must be found in the shadows, the "penumbra" of the more established and clear rights that relate to spatial, temporal, and physical dimensions and variables and could not even fathom "cyberspace" or "the cloud."

At this point it appears that this is a zero-sum situation: the erosion of one set of rights is actually to the benefit of the other. Growing property rights can impact privacy in a negative manner. They often increase at the expense of

---

68 *http://legal-dictionary.thefreedictionary.com/penumbra*

69 Richard A Epstein, Privacy, Property Rights and Misrepresentation, 12 GA.L.Rev. 455,463 (1978) ["Privacy… is the least important tort for a civilized society."]; Richard Posner, The Uncertain Defense of Privacy in the Supreme Court, 1979 Sup. Ct. Rev., 173

personhood, autonomy and freedom of expression[70]. There is no doubt that this represents a constitutional challenge still not firmly decided and very much in need of firming up[71].

The fruits of the poisonous tree

The way in which people communicate and store their communications today has changed dramatically from just a few years ago. The shoebox under the bed, guarding yellowing letters received throughout the years, is long gone. People connect by using electronic devices whose models change at a dizzying speed and that are always on, constantly online. File-sharing, be it music, videos, text, images is a very common and constantly ongoing activity. At the same time, many computer networks are insecure and even those supposedly secure have weaknesses that can be breached by smart and technically savvy hackers. The quality, know-how and expertise of hackers have also grown exponentially. Troves of documents and information are relatively easy to access and search for a variety of purposes, including a criminal investigation. Wikileaks[72] has demonstrated this more than once to the entire world, defying the "Top Secret" ratings of the United States Government. Thus, searching for information and accessing data banks, confidential information, credit cards numbers, medical information and other data by private individuals are quite frequent, constantly ongoing and often successful activities undertaken at times by private parties[73]. Very new, troubling and worrisome, especially to civil libertarians and human rights activists, is the partnership between police or other official investigative bodies and hackers, with the latter providing substantial evidence to the former often on their own volition and then possibly continuing to collaborate to find

---

70 Nadine R. Weiskopf, Social Media and E-Discovery: New Tools and New Challenges, Lexis Nexis (2010), at 3, *http://www.lexisnexis.com/Community/LitigationResourceCenter/cfs-filesystemfile.ashx/__key/CommunityServer.Components.SiteFiles/Documents.LRC Documents/White-Paper-Social-Media-and-E_2D00_Discovery—New-Tools-and-New-Challenges.pdf*

71 Patricia L. Bellia, Paul Schiff Berman, & David G. Post, Cyberlaw: Problems of Policy and Jurisprudence in the Information Age (3d ed. 2007)

72 *http://en.wikipedia.org/wiki/WikiLeaks; Wikileaks.org*

73 Graham Cluley, We Could Hack the Queen's Medical Records if We Wanted To, December 16, 2011; *http://nakedsecurity.sophos.com/2011/12/16/ournalists-under-the-spotlight/*

further evidence of wrongdoing[74]. At times things get even more complicated when there is collusion between the media and hackers or in various combinations, between the media, police, hackers and politicians[75]. Thus, contrary to popular belief, it is not only the state or the police that spy and conduct surveillance on citizens by accessing their electronic devices but also private individuals or firms who often do it extensively and illegally, using strong technical capabilities and ingenious traps to collect incriminating evidence that is then offered to and used by the state to arrest, prosecute and convict[76].

Thus, one of the least noticed but most controversial Fourth Amendment issues in cyberspace is admitting in court private party searches of the computers or other electronic devices of people, even before they become suspected criminals, that is without probable cause.

Electronic searches: partnership between police and private parties

A partnership between police and private parties is not new[77]. Often it is done on purpose, overtly or tacitly, to avoid the strictures and controls of the Fourth Amendment and its Exclusionary Rule. Teachers in school may conduct locker or school bags searches or interrogate pupils about selling drugs at school

---

74 David Folkenflik, U.K. Hacking Scandal Exposes Media-Police Ties, NPR, January 19, 2012; Sarah Lyall, Tip for London Police Officers: Booze and Secrets Don't Mix, New York Times, January 5, 2012, Europe Section; Sarah Lyall and Ravi Somaiya, British Inquiry Told Hacking is a Worthy Tool, New York Times, November 20, 2011, Europe Section.

75 In December 2011, BBC Radio 4 broadcast a documentary claiming that computer hackers were used by the British press to spy on politicians and the military. It was said that some of the hackers learned the tricks of the trade while working for army intelligence. A typical attack would use a Trojan horse (called an "eblaster trojan attack") that could capture keystrokes and allow a remote hacker to actually see what was happening on a compromised computer. This way, all emails and attached documents could be easily read. The phone hacking scandal in Great Britain connecting hackers, police, the media (News of the World) and politicians is a major recent example of this collusion; *http://en.wikipedia.org/wiki/News_International_phone_hacking_scandal*

76 Tengku Mohd T. Sembok, Ethics of Information Communication Technology (ICT), 2003, *http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF*

77 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 250

or participating in other illegal activities and then turn over the information to the police without having to worry about constitutional limitations. The same may be done by a department store private guard catching a shoplifter and obtaining a confession without needing to give the suspect the "Miranda warnings[78]." And of course, informers have been around for millennia[79]. However, when these searches without constitutional limitations happen in cyberspace, it is more troubling and dangerous because a private party, with the appropriate tools, can search vast amounts of information easily, efficiently, silently and anonymously. It can be done across the globe from the safety and comfort of one's studio or living room, with no one knowing, hearing, seeing, suspecting. It can be a quick search or long term surveillance. Under U.S. constitutional law, for the police to conduct a search, they need probable cause and, depending, a warrant. Private parties searching, even in the sense of a fishing expedition, need neither one and the information they obtain is useable for a criminal prosecution[80].

Consequently, data and information saved on personal computers that may physically be locked away, is potentially subject to warrantless searches by private parties that may, in the end, be doing the work of the police. All the private party has to do is to gain entry and obtain access to the stored material of the electronic device, and the rest follows[81].

There is no question that the Fourth Amendment did not envision joint operations by law enforcement and private people to conduct cybercrime investigations. It was alien to the understanding of the function and operation of law enforcement at the time of the writing of the Constitution, even leaving aside the non-existence of electronic devices. As already stated earlier, the point is that the Fourth Amendment traditionally applies only to governmental entities and personnel, not to private parties. The latter can conduct searches of personal computers or other electronic devices connected to the internet; for them, there are no constitutional limitations or constraints[82].

---

78 Miranda v. Arizona, 384 U.S. 436 (1966)

79 Susan Brenner, Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?, 30 Rutgers Computer and Tech. L.J.1, 67-68 (2004) (underlines that the practice to use private parties, especially survivors, for criminal investigations goes back to colonial times in the U.S.)

80 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 266

81 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 260

82 Neal Kumar Katyal, Digital Architecture and Crime Control, Yale Law Journal, 112, 8 (June 2003), 2261

Are there U.S. statutory protections against private cyber searches?

There could of course be statutory protections. In the United States there are three major laws that could be helpful in this respect: the Stored Communications Act of 1986, the Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968), and the Computer Fraud & Abuse Act of 1984.

The *Stored Communications Act* (SCA) is part of the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2701 to 2712). It covers voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).

The Fourth Amendment to the U.S. Constitution addresses the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." However, when applied to information stored online, the Fourth Amendment's protections are much weaker and even non-existent. Why is it so? Because the Fourth Amendment articulates the "right to be secure" in spatial terms ("their persons, houses, papers, and effects"), based on concrete items, that do not easily coincide with the "reasonable expectation of privacy" in an online environment. Moreover, there is no consensus in society about expectations of privacy related to contemporary and future ways to record and/or transmit information. Even more legally weakening is the fact that users normally allow a third party, an ISP, to store their online information. This is especially true now with the advent of the "cloud." In a number of Fourth Amendment disputes, case law has held that, by entrusting information to third parties, users give up *any* expectation of privacy[83]. In addition, there is also the "third party doctrine" which holds "…that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information[84]."

---

83 Bradley J. Schaufenbuel, Social Networking: Open Discovery Versus Privacy and the Battle Between the Coasts, in Thomas J. Shaw (ed.), Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists, Section of Science & Technology Law, Information Security Committee, American Bar Association, 2011

84 Donald L. Doernberg, "Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence, 39 Ind.L.R. 253, 263 (2006), available at *http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1263&context=lawfaculty*

Consequently, while to search someone's home or effects one generally needs probable cause and a search warrant, under the third party doctrine,[85] to force an ISP to reveal the contents of an email or of files kept on a server, one needs only a subpoena and prior notice, a much easier requirement than probable cause[86]. The SCA establishes some limits on the ability of the government to oblige an ISP to furnish content and non-content data (such as logs and "envelope" information from an email)[87]. Moreover, it also limits somewhat the ability of commercial ISPs to provide content information to nongovernment entities. But overall, the protection is weak[88].

The *Wiretap Act* (18 U.S.C. §§ 2510-2522) regulates collecting the content of wire and electronic communications. Before the 1986 amendment by Title I of the Electronic Communications Protection Act (ECPA), it addressed only what existed at the time, wire and oral communications. Title I of the ECPA included also electronic communications. The ECPA's provision limiting law enforcement access to electronic communications was weakened by the U.S. Patriot Act [115 Stat. 272 (2001)] passed after the 9/11 events in the United States[89]. The Wiretap Act originally limited somewhat the access and collection of electronic communications by police but gave ample liberty to the provider of services to do it rather easily[90]. The Provider of Services exception [18 U.S.C. § 2511(2) (a) (i)] permits:

"an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service…."

---

85 Orin S. Kerr, The Case for the Third-Party Doctrine, Michigan L. Rev., Vol. 107, 2009

86 Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, George Washington L. Rev. (2004). Available at DOI: 10.2139/ssrn.421860.

87 Alexander Scolnik, Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment, 78 Fordham L.R. 349, 365 (2009), available at *http://law.fordham.edu/assets/LawReview/Scolnik_October_2009.pdf*

88 *http://en.wikipedia.org/wiki/Stored_Communications_Act*

89 John D. Podesta & Ray Goyle, Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World, Yale Law & Policy Review, 23, 3 (Spring 2005) 509

90 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 258

There is also an "Accessible to the Public Exception" 18 U.S.C. § 2511(2) (g) (i) permitting any person to intercept an electronic communication made through a system "that is configured so that . . . [the] communication is readily accessible to the general public."

The *Computer Fraud & Abuse Act* (CFAA) [18 U.S.C. § 1030, 1984] is meant to reduce cracking of computer systems and addresses federal computer-related offenses. It covers cases where computers of the federal government or certain financial institutions are affected, where the crime itself is interstate, or where computers are used in interstate and foreign commerce. It has been amended several times, especially by the USA Patriot Act[91]. To suppress evidence obtained by a private party illegally hacking into the accused computer, one has to demonstrate that the hacker is a "government agent", someone acting as an instrument of government, a difficult requirement to meet.

Overall, none of the above laws provides firm protection for personal computers[92]. The only one is the SCA that creates Fourth Amendment-like privacy protection for e-mail and other digital communications stored on the Internet. It forbids the government from forcing an online service provider to turn over content and non-content information (such as logs and "envelope" information from e-mail messages) without a warrant issued by a court. Moreover, the SCA forbids commercial online service providers from sharing content information with nongovernment entities unless there is a statutorily defined exception[93]. However, it must be noted that the SCA contains many exceptions to its general prohibition of disclosure to third parties[94]. The Wiretap Act covers only contemporaneous communications, not those stored on computers hard drives. The CFAA does not have a suppression remedy[95].

---

91 John D. Podesta & Ray Goyle, Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World, Yale Law & Policy Review, 23, 3 (Spring 2005) 509

92 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 257

93 Michael Gallo, E-mail Privacy – Whether Court Order Disclosure of E-mail Content, per the Stored Communications Act, Violates the Fourth Amendment, 26 MICH. IT LAWYER 11, 12 (2009), *available at http://www.michbar.org/computer/pdfs/vol26_1.pdf.*

Timothy G. Ackermann, Consent and Discovery Under the Stored Communications Act, THE FEDERAL LAWYER, Nov. Dec. 2009, at 42-43, available at *http://www.pattersonsheridan. com/images/uploads/SCA_Control_article_PUBLISHED-crop.pdf.*

94 18 U.S.C. § 2702(b)

95 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 259

However there is some protection, some extension of the Exclusionary Rule to illegal searches conducted by private parties: the Wiretap Act envisions the suppression of illegal interception of wired and electronic communications, regardless of who does it (government or private party). The Electronic Communication Protection Act should also provide some suppression remedies but it is very weak. The ECPA has been strongly criticized through the years for its failure to protect all communications and consumer records. Under the ECPA it is quite easy for the government to obtain consumer data stored on servers from service providers. All that is needed is a statement in writing certifying that the information is relevant to an investigation of foreign counterintelligence. No judicial review required[96]. The ECPA also lengthened the list of crimes that can be used to justify surveillance as well as the number of those who can authorize this surveillance. Some information can be obtained without a warrant, like traffic and calling patterns. This way the government can obtain valuable intelligence and violate privacy without risk because, formally, the actual content of the communication is not touched. Similarly, in the workplace, theoretically, communications are protected. However, all an employer needs to do is to give notice or not even do that. It is sufficient for a supervisor to "feel" that the employee's actions are not in the interest of the company to gain access to his/her emails. This means that an employer has ample leeway to monitor communications within the company through self-certification. The current high point debate is where to draw the line to limit the government's power to peer into the citizens' lives while reducing national threats[97]. The ECPA falls squarely in the middle of this debate[98]. Both sides are clamoring for revisions and clarifications going their way to be made by the courts and legislatures[99].

The legal void and the need for a suppression remedy

There is no doubt that there exists a legal void that should be eliminated through a statute that provides a suppression remedy against searches by private parties using illegal hacking methods to obtain evidence for a criminal

---

96 *http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act*

97 Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 253

98 Andy Serwin, ECPA Reform – Inconsistent Holdings on Social Media, Privay & Security Source (Oct. 2, 2010), *http://www.privacysecuritysource.com/ecpa-reform-inconsistent-holdings-on-social-media.*

99 Ibid., *supra*

prosecution. The main justification for this remedial law is the anonymity, scope and efficiency of hacker searches coupled with the illegality of hacking itself. This should definitely justify a suppression remedy[100]. That private parties can do surveillance using electronic technology that uses an illegal tool, hacking, for the justice system to then use the information obtained to prosecute and convict can legitimately be considered quite unethical, unjust and encouraging the commission of the crime of hacking without repercussions.

The point of contention is the "backdoor" aspect of all of this: the third party access to private information stored on a computer opening the door for a legally supported government intrusion into private lives. One could say that the more privacy we surrender to private parties as a condition to use electronic services, the less privacy we have in front of the government, betrayed, if you want, by the very technology we cannot do without to function in today's world[101]. The digital file that exists on each one of us has, like it or not, a mix of information: some obtained by private parties, often illegally, without legal consequence to them, and some generated by law enforcement that is more constrained by legal rules in what it can and cannot do.

An example of a group that searches for proof of criminal behavior as described above are the Cyber Angels[102] trained to surf the internet to look for child pornography. Some of these groups use Trojans and viruses to penetrate barriers and hack their way into private accounts to search for possible incriminating evidence. They do surveillance of public and private chat rooms and match content with personal information available on the net, especially through the social media. No need here for probable cause to justify invading someone's privacy. Wanting to engage in a pure fishing expedition is fine and the system will legally use the fruits of these searches to its advantage. Thus, one could say that what can be described as community-based cyber policing is a license to majorly interfere with the private lives of neighbors, friends, and perfect strangers[103].

---

100 Monica R. Shah, The Case for a Statutory Suppression Remedy to Regulate Illegal Private Searches in Cyberspace, 105 Columbia Law Review 1 (Jan. 2005), 272

101 David K. Isom, Romano and Facebook: Muddling Toward the Law of Privacy on Social Networks, Information Law Group (Oct. 12, 2010), *http://www.infolawgroup.com/2010/10/articles/social-networking/romano-and-facebook-muddling-toward-the-law-of-privacy-on-social-networks*

102 Monica R. Shah, *supra* note 79, at 261-62

103 Shannon Awsumb, Social Networking Sites: The Next E-Discovery Frontier, 66 Bench & Bar of Minn. 22, 26 (Nov. 2009), available *at http://www.mnbar.org/benchandbar/2009/nov09/networking.html*

Thus, in the U.S. legal system criminal defendants are not necessarily protected from searches of their electronic equipment by private parties, even though hacking in itself is illegal[104]. Courts hold that these searches are not an "interception" in the sense of the Wiretap Act and/or the SCA. The courts maintain that accessing content already on a private computer is not an interception [U.S. v. Steiger case 318 F. 3d 1039 (11th Cir 2003)].

The *basic legal principle* in the U.S. is as follows: Once a private search is conducted, the original expectation of privacy is frustrated, and as such, the Fourth Amendment does not prohibit Governmental use of the information now non-private any more [*United States v. Jacobsen*, 466 U.S. 109, 117 (1984)].

An interesting illustration of all of this is the case of a Turkish informant who decided to investigate and uncover child pornography on laptops virtually worldwide and report the owners to law enforcement for prosecution. The first case where the evidence uncovered by the hacking searches of "Unknownuser", as he or she was called by the FBI, was successfully used for conviction is the *Steiger* case [*United States v. Steiger*, 318 F.3d 1039, 1044 (11th Cir. 2003)]. The same Turkish informant that brought Steiger to the attention of authorities did conduct other investigations privately hacking into other people's stored searches and data. The methodology of "Unknownuser" was as follows: he attached a Trojan Horse program to a photo that he posted to a news group frequented by pornography enthusiasts. When anyone downloaded the photo, they also downloaded the Trojan Horse program, which provided Unknownuser access to their computers.

Unknownuser in Turkey eventually uncovered and reported a William Jarrett in the United States, another child pornographer. This time there was a closer relationship between the informant and the FBI, following the successful prosecution of *Steiger*[105]. For example, the FBI agents called the informant to help them access Jarrett's computer that was password protected. The District Court sided with Jarrett and suppressed the evidence, holding that the hacker did act as a Government agent and consequently violated the Fourth Amendment when he provided to law enforcement the pornographic material he obtained from Jarrett's files. However, on appeal, the Court of Appeals did not agree to characterize the informant's actions as meeting the government agency standard,

---

104 Priscilla Grantham Adams, Fourth Amendment Applicability: Private Searches, National Center for Justice and the Rule of Law, 2008; *http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf*; Monica R. Shah, The Case for Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace, 105 Columbia Law Review, 1 (Jan. 2005), 260

105 318 F.3d 1039,. 1044 (11th Cir. 2003

which would have provided more constitutional protections for Jarrett [*United States v. Jarrett*, 338 F.3d 339 (4tth Cir. 2003)]. The District Court's decision was reversed and Jarrett was convicted[106]. Thus, the bar is very high to meet the government agency standard, even though there may be close collaboration between the police or the FBI and the informant. The Fourth Amendment applies to private searches only if their behavior reaches the level needed to meet the government agent standard[107].

Constitutional and civil liberties concerns

There is civil liberties and constitutional protections concern over both the *Jarrett*[108] and *Steiger*[109] cases, and other similar ones, because this type of investigative searches is quite different from other searches (for example, of one's home) that may be undertaken by a private party. Moreover, there is the anonymity and also the exponentially higher efficiency in searching several computers connected to the internet at the same time. Additionally, these private searches require good technical abilities, do not give out information on the searching party or leave any traces, and can search many electronic devices at the same time and without any probable cause[110]. A Trojan horse is often used like in the *Jarrett*[111] and *Steiger*[112] cases. A Trojan is software that is intended to perform, at the same time, a desirable (expected) effect and a covert (unexpected) effect. For example, Trojan horses can make copies of them, steal information, and harm or take control of a computer system. Once a Trojan has been installed on a target computer system, a hacker may have remote access to the computer and conduct various operations, like downloading or uploading of files on the user's computer; modifying or deleting files; logging keystrokes; watching the screen in use; search the files for some type of information to steal, and more[113].

Moreover, there is also clearly an element of seizure: the hackers seize the electronic device of the other persons for their use. Also problematic is the legal system implicitly approving this type of search which is actually illegal.

---

106 Jarrett, 338 F.3d at 341

107 Monica R. Shah, *supra,* note 79, at 266

108 338 F.3d 339 (4tth Cir. 2003)

109 318 F.3d 1039,. 1044 (11th Cir. 2003

110 Monica R. Shah, *supra,* note 79, at 260

111 338 F.3d 339 (4tth Cir. 2003)

112 318 F.3d 1039,. 1044 (11th Cir. 2003

113 *http://en.wikipedia.org/wiki/Trojan_horse_(computing)*

These can be real "fishing expeditions[114]." It is much more, in a very different league, than Neighborhood Watch, tips hotlines or an informant. These searches are systematic. They can reach a large number of people across the world. Also, differently from breaking and entering someone else's premises, there is no trace or sign of the intrusion. The victims themselves can be a much larger group of people totally unaware of what is taking place[115]. Courts worldwide are still more comfortable handling physical than electronic violations of privacy. They also find it more challenging to recognize an electronic privacy interest. In a way, the courts' opinions appear to convey the idea that the breach of privacy in cyber space is much more acceptable than in the physical space[116].

Another dangerous element is the apparent approval by the courts to use viruses to penetrate private electronic storage. A virus can impact many people, even thousands, internationally and cause considerable economic harm and loss. The same tribunals that would reject proof derived from a break in, theft or trespassing in the real world are much more inclined to accept it in the electronic one. One could say that courts support and encourage "with a wink and a nod" the alliance between police and hackers or people involved in illegal activities.

Ironically and maybe embarrassingly, this reliance of the FBI or police on private hackers reveals a law enforcement inability or lack of training for this category of investigation. This could be an important point. Traditionally, the court's tolerance and willingness to easily allow a private person's surveillance and investigation of others is based on the view that the private citizen, not being a "professional", is not expected to be that good and therefore cannot do much damage. It is the "professionals", especially the police that truly know what they are doing, they are trained to do it quickly and effectively, they can do a lot of damage and therefore they are the ones who must be controlled. Actually the reverse may be true in today's electronic environment with hackers much better versed and experienced in how to infiltrate an electronic device, and search and seize its contents than the police or the FBI, and then provide the evidence to the authorities[117].

---

114 *http://en.wiktionary.org/wiki/fishing_expedition*

115 Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L.R. 1003 (hypothesizes that there may be more crime on the internet because of the lack of or limited constraints on criminal behavior as compared to the physical world, e.g. crime less visible or invisible)

116 Monica Shah, *supra,* note 79 at 270

117 Monica R. Shah, *supra* note 79 at 266

A pretty strong indication that this may be true can be found in the cases cited, *Jarrett*[118] and *Steiger*[119], where the FBI agents knew and recognized the better technical knowledge and ability of the informer and definitely relied on what Unknownuser produced[120].

If judges continue to hold this attitude, given the growing and ubiquitous use of the internet and electronics in everyone's daily lives, the protections provided by the Fourth Amendment and the applicable statutes (e.g. anti-hacking laws) will also continue to be seriously weakened and diluted.

It is time to introduce an effective remedy which must include especially the ability to suppress the illegally obtained evidence and the "fruits of the poisonous tree." A statutory Exclusionary Rule would be very helpful[121]. There are classical Fourth Amendment approaches, like the integrity of the judiciary, remedies, and deterring unlawful behavior in the collection of evidence, the main points of the Exclusionary Rule, that can provide a solid foundation and justification for this approach, strengthened by the legitimate need to ensure the security of the internet and discourage hacking.

The Internet has frequently been considered as intrinsically free from regulation, a place where liberty, freedom of expression, sharing, creativity and mutual inspiration would be assured by the very nature and architecture of the networked environment. Against this dream of soaring and unfettered liberty, there is the reality of powerful interests that increasingly are dominating the world of intellectual property, seeking to monopolize it even more. Regulation is inevitable[122]. The hope is that it can be done in a balanced way, taking into account the unique nature, essence, and qualities of the cyber world within a strong constitutional tradition of jealous respect for privacy, the uniqueness of every human and his/her expression, and the wondrous aspects of creativity across space and time. Balancing creativity, freedom and privacy with proprietary interests, monopolistic tendencies, capitalistic aspirations and the ubiquitous security justification is a major challenge, a David versus Goliath struggle, a fierce competition between different blocks and nations. The outcome is uncertain and unpredictable. It will be a test of the international community's commitment to universal human rights, privacy and freedom of expression and, ultimately, the flourishing of humanity in an interconnected world.

---

118 338 F.3d 339 (4tth Cir. 2003)

119 318 F.3d 1039,. 1044 (11th Cir. 2003

120 Priscilla Grantham Adams, Fourth Amendment Applicability: Private Searches, National Center for Justice and Rule of Law, 2008, 4-5

121 Monica R. Shah, *supra, n*ote 79, 276

122 Andrew D. Murray, Regulations and Rights in Networked Space, Journal of Law & Society, 30, 2 (June 2003) 187

FUNDAMENTAL LEGAL PRINCIPLES FOR A BALANCED APPROACH

GIOVANNI BUTTARELLI
Assistant European Data Protection Supervisor EDPS, Brussels, Belgium

Introduction

My intervention will deal with one of the great challenges of our time: how to preserve and increase security in society while paying due respect to the protection of the privacy, and other fundamental rights, of our citizens.

"Cyberspace" is no longer a "far away" concept: we know that Cybercrime in general and Cyber Attacks against Information Systems in particular may have great impact on the real world. There are a variety of motivations for cyberattacks, ranging from political causes to fraud, crime and casual hacking. But the "footprints" for those attacks are easy to hide in a globalized world where both prevention and law enforcement pose enormous challenges.

Cyber-crime is part of the seamy side of the Information Society. The use of new technologies brings not only enormous benefits for societies. They also provide the opportunity to commit new kinds of crimes or traditional crimes using new means.

The fight of cybercrime attacks is an area that requires vast processing of data and many times will involve clear risks of intrusions into the citizens' privacy. This is why security and privacy concerns should be equally taken serious. I am convinced that an effective Strategy in the fight of Cybercrime can not be put in place without the support of a solid data protection scheme complementing it. In other words: no zero sums of privacy and security, we need them both.

Fundamental legal principles are essencial in cyberspace, just as they do in the real world. This applies both to the concept of "cybercrime" and to the fight against (i.e. prevention and repression of) cybercrime.

Global dimension associated to cybercrime

Cybercrime is a global phenomenon and has to be fought globally, therefore the exchange of information among the authorities fighting cybercrime is of paramount importance. Because cyberspace has no physical boundaries, criminals can change their locations from one country to another within seconds in the cyber-world, irrespective of their physical location.

Notwithstanding this, cybercriminals act globally in the cyberspace but at the end of the day, they are linked to a physical location where they can be prosecuted and judged. For prosecutions to work, a computer-related offense in one country also needs to be illegal in another.

Cybercrime can not be fought only by traditional methods and requires important skills in the field of data processing that are often out of the set of skills that regular law enforcement bodies have.

Problems of jurisdiction that arise at both the national and international level make the fight of cybercrime especially difficult. The traditional forms of jurisdiction are based on the concept of boundaries, and laws are based on "territorial sovereignty".

Cloud Computing phenomenon makes this global aspect even more prominent and clearer rules concerning the data centers are needed (especially when the same data can be in multiple locations).

The ideal approach to provide legal certainty should be negotiating a international instrument that provides the necessary mechanisms and tools for ensuring security while at the same time establish the necessary safeguards for fundamental rights. However this is a titanic challenge from the moment it is somehow at odds with national sovereignty.

Attempts to negotiate a global instrument at United Nations level are still in their infancy and only very limited steps have been taken. Russia, along with China, Tajikistan and Uzbekistan sent a letter in September to the UN asking for a resolution on a code of conduct in cyber-space, which could include provisions intended to stop terrorists' use of the Internet.

Cybercrime Convention (Budapest 2001)

The most relevant international instrument that sets guidelines for laws and procedures for dealing with internet crime globally has been the Cybercrime Convention (Whose 10th Anniversary took place some days ago).

Indeed, on the 23rd November 2001, 25 of the Council of Europe (COE)´s 47 Member States and four non-members signed the Convention on Cybercrime.

So far, 32 countries have either ratified or acceded, and 15 other countries have signed the Convention but not ratified yet. Another eight have been invited to accede. (In the last few days Australia has declared its intention to sign the Convention).

The harmonization of procedural measures (Chapter II) and international mutual assistance (Chapter III) result in the exchange of personal data (traffic data, content of communications and all other kinds).

The need to strike the correct balance between security and fundamental rights is crucial for the effectiveness and trust in the Convention.

Ten years ago, before the signature of the Convention, the Working Party 29´ (WP 29) welcomed in its Opinion no. 4/2001 the efforts made to harmonize the combat of cyber crime and supported the general objectives since they can contribute to improve the security level for all citizens and in particular for the processing of personal data. Notwithstanding this, the WP 29 also remarked the need to strike a fair balance between anti cybercrime efforts and the fundamental rights to privacy and personal data protection of individuals as regards the extent to which measures are proposed in the whole of the draft convention.

The Budapest Convention does not apply only to cybercrime, as it addresses – generally speaking– the implementing procedures and mechanisms in respect of various criminal investigation activities (inspections, searches, seizure of correspondence and other items, custody, urgent inquiries, etc.) related to other types of crime – i.e. "conventional" criminal offences – whenever the evidence to be gathered is to be found on and/or with the help of electronic media (see Articles 14 and 19).

The Convention envisages various mechanisms of co-operation and mutual assistance between the signatory countries, also for extradition purposes. They apply not only to the criminal offences "*related to computer systems and data*", but also to "*the collection of evidence in electronic form*" of any criminal offence. This might concern a considerable number of cases, since the offences in question are punished by deprivation of liberty for a maximum of at least one year (see Articles 23 and 24).

Given this framework, the criminal investigations carried out in the individual countries – including the investigations arising out of international cooperation requests under the Convention – might ultimately result into collecting and exchanging a considerable amount of personal data (including telephone and internet traffic data) that need not be related directly to cybercrime – or that might be related to fully lawful activities.

Therefore, the measures in question produce especially significant effects on the rights and freedoms of data subjects. Before the ratification process started, there were significant cases in Italy in which searches were carried out for instance in the editorial offices of newspapers and/or at journalists' homes following orders issued by judicial authorities.

The WP 29 highlighted several criticalities during the preparatory work to the Convention, in particular via the above mentioned Opinion no. 4/2001. Such criticalities concerned compliance of the draft Convention with the data protection principles laid down in Council of Europe's Convention no. 108/1981 as well as in other regulatory instruments adopted thereafter.

The final text of the Convention takes account only partially of the objections and suggestions put forward by the European DPAs.

An important amendment that was made to partly accommodate the WP29's concerns relates to the inclusion of more specific provisions as to the criteria justifying adoption of the measures envisaged in the Convention – in terms of their necessity, adequacy, and proportionality as required by the aforementioned data protection instruments.

In particular, Article 15 of the Convention requires the signatory parties to ensure that the provision of assistance is subject to conditions and safeguards provided for under their domestic laws. The assistance measures in question should provide for the adequate protection of fundamental human rights – in particular those laid down in the Human Rights Convention, whose Article 8 refers to the right to privacy. Additionally, they must ensure compliance with "*the principle of proportionality"*.

Let me draw your attention to the fact that application of the principle of proportionality is set forth by the Convention as a mandatory requirement in view of the proper application of the Convention itself.

Hence, it is necessary for this principle to be included (if this is not already the case) and developed appropriately in domestic legislation.

To that end, each of the relevant pieces of legislation regulating investigations and preparatory work in connection with criminal proceedings should contain an *ad-hoc* provision whereby investigational and procedural activities will have to be handled by judicial and/or police authorities in accordance with a proportional, selective approach – that is to say, by having regard to the data and information that are relevant and not excessive in respect of the investigations in progress, and by applying equally proportionate mechanisms. Alternatively, one might envisage a single general rule to be included in the Act ratifying the Convention and subsequently incorporated into criminal procedural law.

The "proportionality" clauses in question should also apply to other investigational activities mentioned in the Convention, irrespective of whether they are already regulated under domestic law – e.g., as regards Italy, to the interception of communications and conversations, in particular "new generation" tapping such as the one applied to VoIP.

Should it prove impossible to ensure that the principle of proportionality is explicitly mentioned in the legal instruments regulating investigations, it is unquestionably appropriate to raise the awareness of the competent investigational bodies in order to ensure that the principle of proportionality referred to in the Convention is abided by in concrete during the investigations.

Impact on third Parties' Rights

I believe that the domestic legislation of each country should also include a provision implementing a similar principle that is laid down in Article 15 of the Convention – whereby the impact of the investigational procedures upon the rights and legitimate interests of third parties should be considered. There is little doubt that the use of computerised means – which might ultimately be the subject of a seizure order – makes it easier to process a huge amount of personal data also related to other parties; this requires an especially selective approach in carrying out the investigations, also in order to avoid affecting the rights and interests vested in individuals that have nothing to do with the facts being investigated upon.

Corporate liability for criminal offences committed by "employees"

Under Article 12 of the Convention, the signatory parties are required to adopt legislative measures to ensure that legal persons can be held liable for criminal offences established under the Convention where such offences have been committed by individuals working for the said legal persons.

I think this is another issue that should be considered more carefully.

For instance, the Italian Act ratifying the Convention expands the scope of the liability vested in corporations and other organisations under Act no. 231/2001 (which is dependent on certain preconditions and relates to criminal offences committed for such corporations'/organisations' benefit) so as to include some criminal offences established under the Convention.

Considering how closely related these issues are, it would be necessary for the ratifying countries to consider application of the punishments in question also to the criminal offences established under domestic data protection laws.

"Freezing" traffic data

The 2001 Convention does not contain provisions that require electronic communications service providers to systematically retain traffic data – in line with CoE's Recommendation no. 3/1999 on the communication of data for judicial purposes (which ruled out such a broad-ranging obligation).

Indeed, the Convention only allows the temporary preservation of specific computer data, including traffic data, that is already in service providers' possession or control (this is the so-called data "freezing"), also in view of international co-operation. This measure is applicable if it is necessary for the

competent authorities to have the data at their disposal and there are grounds to believe that the computer data is particularly vulnerable to loss or modification (see Articles 16 and 17 of the Convention).

In Europe, the retention of traffic data for law enforcement purposes, in particular the prosecution and suppression of serious crime, is regulated by Directive 2006/24/EC ('data retention directive') – which has been transposed by several Member States (and now subject to expected changes after the EU Commission´s Report on its problematic implementation).

On the other hand, the "freezing" of data is especially appropriate in legal systems that do not allow large-scale traffic data retention – or else allow such retention for a very limited period only.

Any measure related to this issue should be evaluated carefully in the light of purpose limitation and proportionality principles, given that the relevant legislation would also apply to non-billing data, as well as in accordance with a selective approach. Account should be taken, additionally, of the provisions made in the Convention (Article 15(2), Article 16(1) and Article 29) with regard to data retention conditions and periods. As for EU countries, reference should also be made to the safeguards laid down in the European data retention directive.

Countries' jurisdiction in investigating and detecting criminal offences

Under Article 22 of the Convention, the signatory Parties should adopt the measures required to establish jurisdiction over any offence established under the Convention, including the cases in which the offence was committed outside the national territory.

To afford the widest possible safeguards to citizens, it is necessary to set out appropriate criteria to facilitate prosecution of computer crimes by a State whenever a given offence can be considered to have been committed "abroad" under the legislation in force – which is currently often the case.

For instance, this applies to Italy.

If one considers the criteria that are currently laid down in criminal procedure laws to establish Italy's jurisdiction – e.g. the place where the act was committed and/or the given fact took place – one can realize that they are not always appropriate in the light of the new computer-related criminal offences, which are committed as a rule via the Internet and with the help of electronic tools that are located in countries other than Italy.

In short, we should call upon States to upgrade their legislation on jurisdiction in order to afford enhanced protection to the victims of these crimes.

EU level. Instruments in the fight against cyber attacks

At the moment, there is no comprehensive EU legal instrument covering all aspects of the fight against cybercrime.

Not all European Countries have ratified the CyberCrime Convention.

Council JHA FW Decision 2005/222 only covers the approximation of the definition of some cybercrime offences and is in many aspects more limited than the Cyber Crime Convention. It is not comprehensive in the number of offences and tackles neither the ways to fight cybercrime nor the data protection safeguards required.

However, the recently proposed Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (2010/517) is a step forward in terms of harmonisation of offences and penalties and some limited definition of the cooperation mechanisms.

In the absence of specific cybercrime instruments, other legislative instruments are used in the fight against cybercrime:

- Directive 2002/58 (ePrivacy) as amended by Directive 2009/136, is also a relevant instrument to be taken into account in the fight of cybercrime; maybe not in the prosecution task but in the implementation of safeguards (data breach, confidentiality of communications, security measures);
- Directive 2006/24 ('data retention directive') brings blanket recording and monitoring of personal data and constitutes probably the most EU invasive tool in terms of data protection. We all know that it is used in the fight of cybercrime but it should be assessed in the context of cybercrime and its real effectiveness/non-effectiveness and also if less intrusive means can be used to obtain the same results;
- National legislation in various MS;
- Cooperation instruments created in the fields of Judicial and Police Cooperation (mainly based on Chapters 4 and 5 TFEU) that can be applicable although not specific to cybercrime.

All these in combination with other elements such as:

- The Action Plan for the protection of critical information infrastructure (2006);
- The plan to establish more cooperation among CERTS;
- The ENISA's role in its advisory tasks, evaluation and coordination of best practices;

- Europol and Eurojust, which are also active in cybercrime matters (expected creation of a Center for the fight of cybercrime);
- The European Forum of Member States (EFMS) improving security and resilience of ICT infrastructure;
- The European Public-Private Partnership for Resilience (EP3R);
- The Data Protection Law at EU level.

It should be noted that existing EU law applies to ensure that cyberspace is neither the "wild west" nor a "big brother" environment. Therefore data protection principles apply (see Articles 7 and 8 of the European Charter of Fundamental Rights) in correlation with Article 16 of the TFEU:

- Everyone has the right to respect for his or her private and family life, home and communications.
- Everyone has the right to the protection of personal data concerning him or her.
- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
- Everyone has the right of access to data which has been collected concerning him or her, and the right to have it verified.
- Compliance with these rules shall be subject to control by an independent authority.

Moreover, the current Data Protection Directive also has a role in preventing cybercrime as it obliges data controllers to analyse risks and take appropriate security measures.

Present rules in terms of data protection for police and justice (including fight against cybercrime) are a patchwork of specific rules and although a general framework (JHA 2008/977) exists, but it is of limited scope as it only applies to data flows between member states. The review of the Data Protection Directive will hopefully provide a clearer environment.

Ensuring the security of personal information being processed is essential both for the enforcement authorities as well as from the perspective of data protection. The prevention of unauthorised access to data collected and further stored, used and transferred by physical or digital means is essential in order to guarantee the effectiveness of the investigation as well as to ensure compliance with individuals' rights to the protection of their personal data.

Final remarks

Let me finally emphasize a few general points, calling for on one hand action in this area and encouragement of the efforts to provide the tools necessary to fight cybercrime but at the same time let me express some caution in this area:

- being successful in the fight against cybercrime does not require continuous and systematic surveillance of users on the internet;
- we must also avoid a situation where such surveillance is left to ISPs and other providers, either or not on the basis of "enlightened self-interest";
- systematic tracking and tracing of users is itself in clear breach of fundamental legal principles and should therefore not be accepted;
- in other words, we should only provide for targeted measures, where required and proportionate, with all appropriate safeguards.

To sum up, we have legitimate and many reasons for striving for more effective protection of everyone's Internet wellbeing. However, it is a popular misunderstanding that less privacy will deliver more security, or even that more security necessarily requires less privacy.

Part II

CYBERCRIME: CASE STUDIES

CONSIDERING THE SOCIAL DYNAMICS OF CYBERCRIME MARKETS

THOMAS HOLT
Associate Professor, School of Criminal Justice, Michigan State University, USA

As technology increasingly permeates all facets of modern life, the risks posed by computer hackers has risen dramatically due to their ability to steal information, compromise sensitive networks, and establish launch points for future attacks (Brenner, 2008; Chu, Holt, and Ahn, 2010; Computer Security Institute, 2011; Denning, 2011; Holt, 2007; Holt and Lampke, 2010; Wall 2007). Malicious software, including viruses, trojan horse programs, and various other tools, simplify or automate portions of a compromise making it possible to engage in more sophisticated or complex intrusions beyond the true skills of the attacker (Brenner, 2008; Computer Security Institute, 2011; Furnell, 2002; Taylor et al., 2010). In addition, the emergence of botnet malware, which combines multiple aspects of existing malware into a single program, enable hackers to establish stable networks of infected computers around the world (Bacher, Holz, Kotter, and Wicherski 2005; Cooke and McPherson 2005; Ianelli and Hackworth 2005; Rajab, Zarfoss, Monrose, and Terzis 2006). Botnets can be used to engage in attacks ranging from the distribution of spam, denial of service attacks, and network scanning (Bacher et al. 2005; Choo 2007).

The significant role and utility of malicious software in cybercrimes has led to a substantial body of research considering technical solutions to reduce their efficacy (Bacher et al., 2005; Cooke and McPherson 2005; Ianelli and Hackworth 2005) or identify the factors affecting the likelihood of infection (Bossler and Holt, 2009; Choi 2008). A smaller body of research has, however, considered the social factors that influence the creation, distribution, and use of malware in the hacker community (Chu et al., 2010; Gordon, 2000; Gordon and Ma, 2003; Holt, Soles, and Leslie, 2008). For instance, the evolution of malware and the growth of sophisticated attack infrastructures via botnets in the computer underground has revolutionized cybercrime and hacking. An on-line marketplace has emerged in forums and Internet Relay Chat (IRC) for the sale and distribution of malicious software, stolen data, and hacking tools that enable less skilled actors to gain direct access to services that extend their abilities (Chu et al., 2010; Franklin, Paxon, Perrig, and Savage, 2007; Holt and Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, and Voelker, 2011).

Examinations of these marketplaces indicate that hackers can now buy and sell resources to facilitate attacks or information acquired after a compromise. Hackers regularly sell credit card and bank accounts, pin numbers, and supporting customer information obtained from victims around the world in lots of tens or hundreds of accounts (Chu et al., 2010; Franklin et al., 2007; Holt & Lampke, 2010; Motoyama et al, 2011; Thomas and Martin, 2006). Individuals also offer cash out services to obtain funds from electronic accounts or ATMS off-line, as well as checking services to validate whether an account is active and any available balance. Spam and phishing related services are also available, including bulk e-mail lists to use for spamming and email injection services to facilitate responses from victims (Chu et al., 2010; Franklin et al., 2007). Some sellers also offer Distributed Denial of Service (DDoS) services and web hosting on compromised servers (Chu et al., 2010; Franklin et al., 2007; Motoyama et al., 2010).

Few studies have, however, considered the social structures and relationships that affect the malware marketplace and the nature of buying and selling cybercrime services in a virtual environment (see Chu et al., 2010; Holt and Lampke, 2010; Motoyama, et al., 2011). Thus this study will explore the normative orders of the malware market using a qualitative analysis of a series of threads from publicly accessible Russian web forums that facilitate the creation, sale, and exchange of malware and cybercrime services. The findings suggest that malware markets are influenced by three factors: price, customer service, and trust.

Data and methods

This data for this study were generated from a sample of 10 publicly accessible web forums where participants communicate in Russian dialects: six forums trade in bots and other malicious code, while four provide information on programming, malware, and hacking. This data was collected using a snowball sampling procedure in fall 2007 and spring 2008. After exploring the content of publicly accessible threads from these two sites, six other Russian language forums were identified via web links provided by forum users. A sample of threads from each of these forums was examined by a native speaking Russian research assistant to ensure the content was focused on the sale and exchange of malware. Four additional Russian language forums were identified through links provided in these sites to create this sample of 10 forums. The names of each forum have been removed to maintain some confidentiality for the participants and forum operators.

Within these forums, all of the available publicly accessible threads were downloaded and saved as web pages. A certified professional translator was identified who translated the first 50 threads from eight of the 10 forums. Additionally, 25 threads from forum 06 and 21 threads from forum 05 were translated. Due to limited translator availability and duplicate translations in some of the forums, a native Russian graduate student was identified who translated additional content. Duplicate threads were translated to determine interrator reliability, which appeared high across the two translators. A total of 909 threads were derived from this convenient, yet purposive sample of 10 forums. The threads were composed of 4,049 posts, which provided a copious amount of data to analyze (see Table 1 for forum information). Moreover, the forums had a range of user populations, from only 35 to 315 users. These threads span a four year period, from 2003 to 2007, though the majority of threads were from 2007.

Table 1. Descriptive Data on Forums Used

Forum	Total Number of Strings	Total Number of Posts	User Population	Timeframe Covered
01	50	183	88	6.00 months
02	50	164	50	20.00 months
03	200	1203	315	10.75 months
04	200	812	273	12.50 months
05	159	369	153	6.75 months
06	50	251	82	36.25 months
07	50	379	116	29.50 months
08	50	291	95	36.00 months
09	50	172	35	10.50 months
10	50	225	95	1.50 months
Total	**909**	**4049**	**1302**	

These forums provide a substantive representation of malware and hacking markets, as 630 of the 722 ads featured language soliciting or selling tools, services, or data that could be used to engage in cybercrime or some other illegal activity (see Table 2). Additionally, the majority of these posts were sales related (73.1%), rather than purchase related (22.8%). The remaining 91 (13%) requests were related to a variety of other legitimate or gray market jobs in programming, web design, or the sale of hardware, software, email accounts, and file-sharing service accounts. Given that 87.3

percent of the requests in these sites were related to tools and services to facilitate cybercrime, this analysis will focus in depth on these items, using quotes from the data where appropriate.

Table 2. Resources Offered in Hacker Forums

Resources	Number of Posts	% of Total	Buy Posts	% of Total	Sell Post	% of Total
Cybercrime Services	219	30	39	17.8	180	82.2
ICQ Numbers	73	10	9	12.3	64	87.7
Malware and Related Services	246	34	103	41.9	143	58.1
Other	92	13	22	23.9	70	76.1
Stolen Personal Information	92	13	21	22.8	71	77.2
Total	**722**	**100**	**194**	**26.9**	**528**	**73.1**

Market processes

In order to understand the normative orders that shape cybercrime markets, it is necessary to first consider the structure of the market as a whole. The forums identified in this study comprised an interconnected marketplace composed of unique threads that act as an advertising space. Specifically, individuals created threads posting their products or services to the rest of the forum. Alternatively, posters could describe in detail what they were interested in buying or acquiring on the open market. Both buyers and sellers provided as thorough a description of their products or tools as possible, including contact information, pricing information, and payment methods. Actors within these markets communicated primarily through the instant messaging protocol ICQ or e-mail, as they can be encrypted to protect both participants during the sales process. Some also used the private message, or pm, feature built into to each forum. Private messages ensure quick contact and act as an internal messaging system for each site, though they may not be as secure.

Prices were stated in either U.S. dollars or Russian rubles, along with the desired method of payment through some web-based monetary system. Forum users regularly paid for their goods and services using WebMoney [WM] or Yandex as noted in the following post from the ICQ seller Creator:

1. [Pay me] Money first, [ICQ] numbers later
2. I work only from Yandex Money and WebMoney.
Course:
1 unit [ICQ Number] =26 wmr [Web Money Rubles] =$1 [U.S. Dollar]
1unit=26 Yandex rubles

Prices listed using the abbreviation wmz indicated that the seller would accept Web Money payments in U.S., or z, currency. The use of electronic payment systems may be due to the fact that they allow relatively immediate payments and require no face-to-face interactions between the participants. This provides a modicum of privacy and anonymity for the participants, but creates the possibility that they may not receive the goods for which they provided payment. As a result, there is a substantive degree of mistrust between participants that must be overcome through various social mechanisms.

Normative orders of the cybercrime market

Examining the exchanges between actors within the open market provided significant insight into the relationships and actions of buyers and sellers. The content reflected a series of social forces that shape the market environment and the relationships between actors: price, customer service, and trust. Each order will be explored in detail using quotes from the data where appropriate.

Price

The cost of goods and services played an important role in the relationships and exchanges between buyers and sellers. Individuals who offered a service or form of malware were scrutinized by potential buyers when a price for a product was perceived to be priced too high or low. This was evident in an exchange where an individual named demcho requested a custom written proxy-socks bot and would pay the coder $1,000 for the program. Several individuals responded to this request, indicating differences in their perceptions on the appropriate cost of such code:

alep: [quoting demcho] “you have probably written similar things for yourself”
true. for_myself_, 2k - is a laughable price.
museo: 2k - that just for the bot

+2k*5 for bypass of fires and full invisibility
Conter: [Quoting museo] "2k - that just for the bot
+2k*5 for bypass of fires and full invisibility"
=(darn. Aye [SIC] some kind of sucker. i'm writing three similar projects now, none of them exceed a thousand... =/

Similar discussions were found across the forums, demonstrating that there may be variations in the costs that individuals find acceptable for a given product.

The importance of price also led some sellers to offer discounts and deals to attract prospective customers. Bulk discounts were a common way to sell products in large quantities. For example, enfold sold log traffic, stating: "The more you order, the smaller the price." Similar prices were evident for DDoS providers, as in this ad from cantar: "When ordering the DDoS service for 3-6 days, discount is 10%, with a DDoS service of more than 7 days, discount is 20%, and with a DDoS service for 3 sites, gives a free service for the 4th site." The pricing and discount structures indicated in these posts suggest that the price of goods and services are variable, with those individuals making large purchases receiving the greatest benefit. In turn, an individual's return on investment in a cybercrime service may increase with volume purchasing.

Customer service

The second and interrelated normative order identified within these forums was customer service. Individuals interested in buying a product or service sought the most satisfactory experience and noted how sellers cater to their customers. One of the most critical issues lies in the speed with which sellers respond to requests from potential buyers. Sellers who are regularly on-line and can be easily contacted were more likely to generate positive reviews and feedback from customers. Some individuals would note "knock me in ICQ, I am there often," or "I am always online," suggesting they could be reached at any time.

Those who did not quickly respond to messages from prospective buyers or were difficult to reach received negative comments from forum users. For example, pientza wanted to obtain services from a SOCKS proxy provider, stating: "I knocked [contacted on ICQ] you are not answering. I would like to try it. How many socks will be in the browsers?" Additionally, a malware seller named slicked was not responding to messages, leading to a conversation about his service:

Planetoid: Does anyone know where slicked disappeared to, I haven't seen him a week on ICQ.
venom: Maybe he had enough with his trojan
Zood: No, he is a secret person. Noone even knows where he is from, sometimes he disappears and reappears again.

In addition to the speed of replies, sellers who immediately provided goods to their customers received praise for their efforts. For example, an individual with the handle grendel purchased a build of the trojan Pinch from Downwind. He was happy with the product and noted the speed with which it was delivered, stating: "Thanks, I ordered it. Four minutes and it was ready. Respect." Thus, sellers who can offer quick distribution of product receive a good deal of respect within these sites.

The quality of the product or service a seller offered was also critical for their prospective buyers. Given the importance of price, customers considered what benefits they would receive for their investment. This was exemplified in a post from the malware installer cyptor, who noted "our price may look to you not so adequate, but the quality will cancel this out, do not forget, that the cheap one pays twice." If a tool was ineffective or data was insufficient, a buyer may post bad reviews or not recommend that provider. For instance, an individual named tripod purchased Pinch logs from a seller and was asked: "Was there anything legitimate?" He responded noting "Not really, it was modest. But I have not seen better stuff from anybody."

The importance of quality was particularly evident in posts from DDoS vendors. These providers regularly noted that they would give customers a free 10 minute test to measure the efficacy of their attacks against a particular target. This was demonstrated in an advertisement by letrin in forum 05:

DDOS Service, with quality and reliable. I think that majority know this DDOS, but I will remind it to you again, if you have competition, who interrupt your work and if someone has hurt your feelings, you can play on the site of this person, best solution is smokin.

Some vendors also offered money back guarantees, as in this example from forum 3: "If the site your order to attack comes alive earlier than the time chosen by you, then you will get money back." Such a measure demonstrated a willingness to negotiate with prospective customers that could increase their overall business and reputation.

Another important indicator of customer service was the degree of support individuals offered for their products. Services, tools, and resources that required a higher degree of knowledge or specification often came with some form of customer support. For instance, anti-abuse web hosting providers

offered a good deal of support for their customers, as in the case of a provider who described how clients could speak live to his sizeable support staff:

> We have implemented real-time client support for the ICQ protocol… ICQ #1 [removed]. . . owner of the service… Complaints and suggestions regarding the work of the service, receipt of payment for services. ICQ #2 [removed].. . . Support. . . decides the same questions, purchase of accounts, general consultation on the service. COORDINATION of the work of support and administrators);
> ICQ #3 [removed].. . . - support, system_administrator, night shift. Solutions on difficult technical issues);
> ICQ #4 [removed]. . . . (Support. . . -Night, support, system_administrator, night shift. Solutions on difficult technical issues);

These posts demonstrate that access to support and regular software updates are a critical service component that may help to develop and maintain a regular base of clients. These posts also demonstrate that principles of customer service found in the legitimate business world appear to shape the interpersonal dynamics of buyers and sellers in this cybercrime market.

Trust

The third order identified in these forums involved trust, which is intertwined with customer service. The participants in these forums sought out commodities that they valued, and had to pay for these goods without actually interacting with others in person. Participants may not receive the goods they paid for or received bogus products with no value. In addition, most data and services sold were usually obtained through illegal means so buyers could not pursue civil or criminal claims against a less than reputable seller. As a result, it was critical that participants know who they may be able to trust and the steps they can take to reduce the likelihood of losing money.

The significance of cheating and mistrust led to the development of three key methods to reduce the likelihood of loss. The first was through the use of checks or tests by the forum administration as a means to validate the quality of a product sold in the forum. For instance, one of the moderators of forum 05 described the checking process, stating:

Administration has the right to ask any seller to present his/her product for check. You present the product in the form that it is being sold, so that it can be checked for a test. No videos, audio, sreens. Forum safety relies on many factors, but the main one is saving the users from possible cheaters.

Four of the forums in this sample utilized checking systems, though the seller was required to initiate the process of checking or testing. For example, an individual in forum 01 offered an iframe tool and at the end of his advertisement stated: "I'd be happy to get checked out, guarantor and all the rest. . . .^_~" In addition to internal checks within a single forum, some sellers advertized that their products had been checked in other forums, and provided web links to verify this information. An interested party could venture out through those links to confirm that he was, in fact, trustworthy. In turn, buyers can look across other forums as a means of validation of a seller's reputation.

The second method employed in the forums as a means to instill trust was the use of a guarantor program. If an individual was uncertain about a prospective buyer, they were encouraged to make a payment through a guarantor system. Guarantors ensure that a payment will not be delivered to a seller until the product is received by the customer. Four of the forums in this sample used guarantor services, with significant value for participants as noted in this post from valentin:

Guarantee and passing a check. If you do not trust the seller or simply want to secure yourself from cheaters, then you can use the services of the guarantee forum. Any administrator can take the role of the guarantee. There are only two administrators. . . I am esxplaining [SIC] to those in the tank, that if you want to pass the check or buy/sell/or present services through a guarantee, then the ICQ of the guarantors is above. Guarantee services are free.

Guarantors and checks offer a way of validating and confirming an individuals' level of trust and reliability within these forums. Without guarantor payment systems, individuals increase their risk of loss and theft.

The third way that individuals can gain or demonstrate trust within the forums was through customer feedback. Individuals who purchased a product or service could provide detailed comments about their experience with a seller for other users so that they may understand how that person operates. Posts with favorable reviews or positive comments demonstrated that an individual is trustworthy. For example, the seller track offered so-called "abuzo reliable hosting services" in forum 01. He received a number of positive comments from customers, as demonstrated in the following posts:

Drag0n: I uze the host! I like it!
Angry: I took a .info host+domain, registered all the people, ****** which I recommend
Psych: I use this hosting+domain in the Info zone. Everything is quick and presise!
Ask3: I bought the domain+hosting+good person=I recommend it!

These favorable reviews clearly demonstrate that a seller or service provider could be trusted to provide quality products on time and without a great deal of difficulty. Such information helps to build a solid and trustworthy reputation for a seller, and may potentially increase their market share and customer base over time.

By contrast, individuals who referred to someone as a cheat or provided negative feedback had an important impact on the social dynamics of a forum. The appearance of negative comments often led to significant debate and some degree of infighting among forum participants. Since negative feedback and name calling foments debate, mistrust, and disorder among participants, forum moderators attempted to limit these discussions. This was exemplified by the forum moderator n30n who posted a message concerning how he would deal with individuals making negative comments:

For groundless complaints, swearing, flood and multi-accounting - BAN. I've had enough…Never give pre-payment, transfer money with a protection code, but don't give it, just show that you have this money. Send test letters to broken-in mailboxes, accs etc. require screens. If you decide to use someone's services, then take an interest as to what other forums this person offers them on and where you can see references regarding his work.

These comments clearly demonstrate the disruptive impact that claims of cheating can produce in these forums, and the significance of trust in structuring the relationships between actors.

Conclusions

This study sought to understand the social processes that structure relationships between buyers and sellers in the faceless environment provided by the market for stolen data in malware markets. The findings demonstrate that sellers take multiple steps to entice customers, including offering services at competitive pricing with support for non-skilled and skilled buyers alike. The glut of products across the market requires prospective buyers to review and evaluate customer feedback to determine the reliability of a seller. This information can prove invaluable to determine whether a seller is trustworthy. In addition, prospective customers can utilize guarantors to complete a transaction with confidence.

The prevalence of informal mechanisms within the market to ensure trust between buyers and sellers may be a consequence of the risk of loss of funds. Participants in these markets are excellent targets for victimization because prospective buyers have money, limited knowledge of an actor's identity, and are unlikely to contact law enforcement if they are cheated. Similar

victimization patterns have been identified in the real world, such as those who rob drug dealers because of the significant profit and low likelihood of law enforcement detection (Cross 2000; Jacobs 1996, 2000; Jacobs, Topalli, and Wright 1996). There are, however, no physical cues in virtual environments to indicate who may be a potential thief or undercover operative. Thus, actors used a unique argot, including the term ripper, to internally police and regulate the market.

Taken as a whole, this study has key policy implications for law enforcement, and computer security. Specifically, law enforcement must begin to examine and monitor the activities of stolen data markets to identify the source of these forums and further our understanding of the problem of stolen data generally. Collaborative initiatives are also needed between law enforcement agencies and financial institutions to track the relationships between large scale data compromises and initial reports of victimization. Such information can improve our knowledge of the role of data markets in the prevalence of identity theft and cybercrime.

There is also a need for increased collaborative relationships between federal law enforcement agencies around the world. Individuals in disparate countries may be victimized as a consequence of information sold in stolen data markets, thus expanding connections and investigative resources are needed to improve the prosecution and arrest of those behind these crimes. Criminologists must also begin to address the lack of attention given to more serious forms of computer crimes, particularly the interplay between large scale data theft, malicious software, and identity crimes. Such information is critical to develop effective prevention and enforcement strategies and improve our understanding of the ways the Internet acts as a conduit for crime, as the ways that cybercrimes parallel real world offending.

References

Bacher, Paul, Thorsten Holz, Markus Kotter, and Georg Wicherski. 2005. *Tracking Botnets: Using honeynets to learn more about Bots.* The Honeynet Project and Research Alliance. Retrieved July 23, 2006 from *http://www.honeynet.org/papers/bots/*

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3,* 400-420.

Brenner, Susan W. 2008. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Choi, Kyung-schick. 2008. Computer crime victimization and

integrated theory: An empirical assessment. *International Journal of Cyber Criminology,* 2: 308-333.

Choo, Kim-Kwang Raymond. 2007. "Zombies and botnets." *Trends and Issues in Crime and Criminal Justice.* Australian Institute of Criminology. Retrieved December, 28, 2007 from

http://www.aic.gov.au/en/publications/current%20series/tandi/321-340/tandi333/view%20paper.aspx

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line.* Washington, DC, National Institute of Justice. [Online] Available online at:

www.ncjrs.gov./pdffiles1/nij/grants/230112.pdf.

Computer Security Institute. (2011). *Computer Crime and Security Survey.* [Online] Available at: *http://www.cybercrime.gov/FBI2011.pdf.*

Cooke, Evan, Farnham Jahanian and Danny McPherson. 2005. "The zombie roundup: understanding, detecting, and disrupting botnets." *SRUTI '05 Workshop Proceedings*: 35-44. Berkeley CA: USENIX Association

Denning, D. E. 2001. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." Pp. 239-288 in *Networks and Netwars: The Future of Terror, Crime, and Militancy,* edited by J. Arquilla and D. Ronfeldt. Santa Monica, CA: Rand.

Franklin, Jason, Vern Paxson, Adrian Perrig, and Stefan Savage. 2007. "An Inquiry into the nature and cause of the wealth of internet miscreants." Paper presented at CCS07, October 29-November 2, 2007 in Alexandria, VA.

Gordon, Sarah. 2003. *Virus and Vulnerability Classification Schemes: Standards and Integration.* Symantec Security Response. Retrieved October 3, 2005 from *http://enterprisesecurity.symantec.com/content/knowledgelibrary.cfm?EID=0*

Gordon Sarah and Ma Qingxiong. 2003. *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Cupertine, CA: Symantec.

Holt, Thomas J. 2007. "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures." *Deviant Behavior*, *28*, 171-198.

Holt, T.J., Soles, Joshua B., and Lyudmila Leslie. 2008. "Characterizing malware writers and computer attackers in their own words." Proceedings of the 2008 International Conference on Information Warfare and Security, Peter Kiewit Institute, University of Nebraska Omaha.

Ianelli, Nicholas and Aaron Hackworth. 2005. *Botnets as a vehicle for online crime*. Pittsburgh PA: CERT Coordination Center

Jacobs, Bruce. 1996. "Crack dealers apprehension avoidance techniques: A case of restrictive deterrence." *Criminology* 34: 409-431.

Jacobs, Bruce. 2000. *Robbing drug dealers: Violence beyond the law*. New York: Aldine de Gruyter.

Jacobs, Bruce A., Volkan Topalli, and Richard Wright. 2000. "Managing Retaliation: Drug robbery and informal sanction threats." *Criminology* 38: 171-198.

Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. An Analylsis of Underground Forums. *IMC'11*: 71-79.

Rajab, Moheeb Abu, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2006. "A Multifaceted Approach to Understanding the Botnet Phenonmenon." *IMC'06*: 41- 52.

Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2010). *Digital Crime and Digital Terrorism, 2nd Edition.* Upper Saddle River, NJ: Pearson Prentice Hall.

Thomas, Rob and Jerry Martin. 2006. "The underground economy: Priceless." *;login: The Usenix Magazine* 31(6): 7-17.

Wall, David. 2007. *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press.

VICTIMIZATION IN THE CYBERSPACE: PATTERNS AND TRENDS

KARUPPANNAN JAISHANKAR
Senior Assistant Professor, Department of Criminology and Criminal Justice Manonmaniam Sundaranar University; Executive Director, Centre for Cyber Victim Counselling Tirunelveli, Tamil Nadu, India

Introduction

From the commencement of the new millennium, the Internet has transformed the way that peoples interact (Mitra & Schwartz, 2001) and it has become a powerful tool in the hands of both expert users as well as the lay public. Though internet started its existence some 40 years ago, the level of its usage has reached its pinnacle in the early 2000's. The amount of internet users and its applications have shot up to a level which the founders would not have imagined. Earlier internet was only used as a source of email transaction or viewing some information, but now internet has become a place of inhabitancy. Because of the growth of internet and its sophisticated applications, a new space named cyberspace was created. Cyber space is a virtual space, a space which does not exist in real terms, but exist (Jaishankar, 2011). "Although imaginary, cyberspace is real because the things that happen in it have real consequences for those who are participating" (Wall, 2010, on personal communication). Most of the activities that occur in the real/physical space occur in the cyberspace; as well some of the activities overlap among the two. The cyberspace has got its equivalence with the physical space and because of its existence; the physical space has got a new name, "meat space" (Jaishankar, 2008).

Though many take cyberspace as a synonym to the internet it is a much more a broader concept and it is a 'place' (Byassee, 1995). The word 'cyberspace' (a portmanteau of cybernetics and space) which is coined by a Canadian fiction writer, William Gibson in 1984, was initially a fantasized science fiction term, including the linkage of people, computers and information through a virtual space (Heylighen, 1994; Jaishankar, 2008). However, in early 90's, John Perry Barlow popularized the term cyberspace from a different perspective, considering the cyberspace as a place and he applied it to the internet. Until Barlow's vision of cyberspace, it was not considered as a place. Hence, some claim that the present cyberspace should be called "Barlovian cyberspace" instead of "Gibsonian

cyberspace" (Jordan, 1999). However, Wall (2010) feels that "Gibsonian cyberspace" has shaped the public imagination through the visual media and have begun to influence social theory.

The cyberspace in its present version gives a feeling to the user that he/she is going to a different world and it is an extension of their thought process (Suler, 2005; Jaishankar, 2008). Suler (2005) explains that cyberspace has become a 'transitional space' and that it has become an extension of an 'individual's intrapsychic world'. Cyberspace is more an exploratory space to many and extension space to some. Myriad forms of behaviours are exhibited in the cyberspace and a new cyber culture has emerged. Social interactions as well the commercial activities have gone to the next level. The swiftness in human interactions both personal as well as commercial is incredible and the interactions are global. Many start and end their day by inhabiting in the cyberspace involving in business, personal, social and academic activities. Except little dissimilarity between the cyberspace and physical space, most of the behavioural aspects of these spaces are the same. In fact, some behaviour that is exhibited in the cyberspace is only the extension of the behaviours that are shown in the physical space (Jaishankar, 2008; Jaishankar, 2011).

Cyberspace also gives a unique freedom to individuals to expose their real self, which is highly controlled by the value systems offered in every society (Jaishankar, 2008). This unique nature of cyberspace has fostered an environment for the exhibition of both positive and negative behaviours of individuals (Suler, 1999, 2004; Suler & Phillips, 1998). Predominantly, positive behaviour is expressed by many individuals in the internet, though, as in the physical space, a minority always forms the negative or deviant behaviour. The deviant/criminal behaviour in the cyber space can be expressed by two types of personalities. One, as specified in the space transition theory (Jaishankar, 2008), a person with repressed criminal behaviour in the physical space and expresses in the cyberspace and two, a person expressing his/her criminal behaviour, in both the spaces with equal vigour. Though the two types of personalities coexist in the cyberspace, devoid of each other, there are always chances of their meeting in the cyberspace and mutual sharing of criminal knowledge is possible (Jaishankar, 2008). Crimes committed by these individuals are now grouped in to a new category of crimes called cyber crimes or crimes of the internet.

Towards a victim focused definition of cyber crime

Though cyber crimes are termed in varied terminologies like *computer crime, computer-related crime, digital crime, information technology crime* (Matt, 2004), *Internet crime* (Wall, 2001), *virtual crime* (Lastowka & Hunter,

2004), *e-crime* (AIC, 2006) and *netcrime* (Mann & Sutton, 1998), it all signifies the application and utility of internet and telecommunication networks to commit these crimes (Jaishankar, 2008). Even though some researchers feel cyber crimes as a case of "old wine in new bottles" (Grabosky, 2001), "old wine in bottles of varying and fluid shape" (Yar, 2005), or "new wine in no bottles" (Wall, 1999), cyber crimes are unique (Yar, 2005). Especially the victim component of cyber crimes makes it more unique. The victimology of cyber crimes is distinct in its character, compared to the conventional crimes. Cyber crime victimization defies the logic of physical proximity (Jaishankar, 2010). Cyber crime offenders need not be physically proximate with their offenders unlike physical space crimes (Brenner, 2004). An offender can victimize any person across the globe, sitting in any corner of the world, using his computer connected to a network (European Commission, 2001). Also as cyber crime is an "automated crime" (using technology to multiply the number of "crimes" someone can commit in a given period of time (Parker, 1999, 2002; Arena, 2001), several persons can be victimized with the same effort. This innovative nature of automation provides the offenders to victimize many in rapid and precise manner (IPWatchdog.com 2003). (For classification of cyber crimes, see, Carter, 1995; Davis & Hutchison 1997; Deflem & Shutt, 2006; Goodman & Brenner, 2002; Wall, 2001, 2010).

Many definitions of cyber crime were evolved in the pre and post millennium. Some of the definitions were simple and some were complex. Some focused on the crime, some the offender, some the victim. A notable metamorphosis in the new millennium cyber crime definitions is that moving beyond the machines (hacking) and focusing on the humans, especially the victims (Halder & Jaishankar, 2012). A definition of cyber crimes provided by the Oxford Reference Online: "crimes committed over the Internet", though simple, gives a full meaning of these crimes. Though, multiple definitions (Statistics Canada, 2002; Thomas & Loader, 2000; Yar, 2006), are available for cyber crimes, there are no consistent and statutory definitions (PJCACC, 2004; Yar, 2005) and also defining cyber crime raises conceptual complexities (Smith, Grabosky, & Urbas, 2004). Matt's (2004) definition of cyber crime gave a holistic focus on cyber crime from an offence perspective:

> Cyber crime encompasses all illegal activities where the computer, computer system, information network or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computers, computer systems, information networks or data (p. 22).

The human element of cyber crime was included by the Convention on Cyber Crime (COE, 2001). The COE was one of the first legislation to think in the direction of human's while most of the definitions were concentrating on the machines (Halder & Jaishankar, 2012). The COE (2001) included offences against children and "attacks on human emotions, banning usage of "improper words" in the cyber space. This was originally meant to prevent usage of derogatory words, which may promote terrorism, danger to national security and/or racial hatred" (Halder & Jaishankar, 2012, p. 14). The COE also helped the law makers and the academics to change their earlier perspective on cyber crimes "i.e., *everything is hacking or attack at e-commercial transactions*. This drift helped to include emotional attack on internet users as offence and transmuted to a more advanced approach to look at it from individual victim's perspective" (Halder & Jaishankar, 2012, p. 14). It was Wall's (2008) definition of cyber crime that first included 'harm' as a component. Wall (2008) explained cyber crime as "online insecurity and risk and it is widely used today to describe the crimes or harms that are committed using networked technologies" (p. 862). The inclusion of 'harm' gave a new focus to cyber crimes as it was inclined more to crimes against human emotions like stalking, harassing and bullying. Even though there were many definitions of cyber crime beyond Wall's (2008) definition, only Halder and Jaishankar's (2012) definition on cyber crime had the victimization perspective.

Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS) (p. 15).

The types of cyber crimes that are included in the above definition are: hacking, morphing, spoofing, tampering the computer sources, obscene publication, trojan attacks, phishing, cyber stalking, cyber pornography, cyber defamation, cyber bullying, e-mail harassment, cyber blackmailing, cyber threatening, cyber murder, cyber terrorism and abetment of such offences (Halder & Jaishankar, 2012, p. 15).

Patterns and trends of cyber victimization

1. *Development of victim turned offenders*
   There are many instances in the physical space crimes such as harassment and abuse where the victims turn in to offenders. Most of

these cases pertain to Children and Women and a small body of growing literature is available on victim offender overlap (Briggs, 2003; Broidy, Daday, Crandall, Sklar, & Jost, 2006; Jennings, Higgins, Tewksbury, Gover, & Piquero, 2010; Jennings, Park, Tomsich, Gover, Akers, 2011; Jennings, Piquero, Reingle, 2012; Klevens, Duque, & Ramírez, 2002; Lauritsen, & Laub, 2007; Mustaine & Tewksbury, 2000; Rumgay, 2010; Shaffer, 2003). Notably, online victim offender overlap is a modern phenomenon (Umarhathab, Rao, & Jaishankar, 2009) and of late we could find instances where some victims have turned to offenders. I have come across cases which come to our Centre for Cyber Victim Counselling (see www.cybervictims.org), where there are many requests from the victims seeking our assistance to hack the offenders email accounts or social networking site accounts. When we disagree citing our policy of non-interfering in others online accounts, they tend to move to professional hackers (Halder & Jaishankar, 2012). However, we have tried to change their outlook to a certain extent, still some way; online victims try to take revenge by becoming offenders.

In cases of money mules, who are recruited by the online offenders in the guise of providing a legitimate job, "receive bad checks and write good ones and as (albeit perhaps innocent) co-conspirators are not protected" (Florˆencio & Herley, 2010, p. 4) by the laws of any country. Suresh and Paul (2010) assert that all money mules are not innocent. "Contrary to popular belief, mules are not innocent people tricked in to illegal business. They are typically mercenary volunteers with scant respect for the law - and for this very reason, they are turning professionals" (Suresh & Paul, 2010, p. 498). Suresh and Pauls's (2010) argument is further strengthened by the 2011 survey of Financial Fraud Action UK and the National Fraud Authority (NFA) among the residents of Newham in East London. This survey found that 27 per cent of victims of money mule scheme did not know that it is illegal and 87 per cent did not report to police.

2 *Growth of victim precipitated crimes*

It is also found that some of the victims have precipitated (caused) their own cyber victimization. While in physical space people tend to follow certain safety norms, they tend to ignore the same while they are in the cyberspace (Halder & Jaishankar, 2010; Halder, Jaishankar, Periyar, & Sivkumar, 2011). In cases of Phishing and money mules, it is the victims' greed and innocent nature that the cyber criminals exploit (Jaishankar, 2010). Many internet savvy users become victims of virus attacks because of their reckless nature of visiting pornographic sites

and using torrents to download films, songs and other files. Norton's (2011) first ever large scale research on cyber victimization found that 80 per cent of their respondents became victims as they watched adult materials compared to 67 per cent of those who did not watch such materials. Some of the internet users are not concerned about issues of privacy in social networking sites and become victims (Halder & Jaishankar, 2009). They upload photographs exhibiting their intimacy with their girlfriends/boyfriends. Sometimes these photographs are used by blackmailers or sometimes they are morphed for blackmailing.

In many cases of Nigerian 419 scams, the victims were very greedy and some even have gone to the extent of selling their own houses purportedly to receive a huge sum of money from the offender. Apart from exploiting the greedy nature of the victims, cyber offenders also exploit the fear of the victims, especially, using scareware. "By playing to Internet users' fears that computers and information can be at risk, cybercrooks have been able to gain unprecedented access to machines while making hundreds of millions of dollars" (McAfee, 2011, p. 7). A research on victims of cyber attacks of a university network by Michel Cukier and David Maimon, both from the University of Maryland, USA, found that the victims expose themselves to cyber attacks and they precipitate their own victimization. Their study applied routine activity theory and found that the "campus was more cyber-attacked during business hours than during down times like after midnight and on weekends" (Eddy, 2011, para 3).

Also the genuineness of some of the victims is questionable. The Norton study (2011) argues that the anonymous nature of the internet provides an opportunity to do illegal activities online which they might not do in the physical space. This supports my Space Transition Theory of Cyber Crimes (Jaishankar, 2008). The Norton study shows that the victims are sometimes involved in illegal activities like downloading music and film files without paying, plagiarism, engage in forms of online theft, misrepresentation, and defacement. Also some victims do not request permission from others to take their photographs from social networking sites. The Norton study found that nearly 80 per cent of respondents became victims because of lack of genuineness.

3. *Increase in mobile phone victimization*

In the recent past, Smartphones like iPhone, blackberry has created a revolution in the society. In addition to that, the introduction of new gadgets like iPad, tablets, android phones have changed the dimensions of information exchange. These mobile phones are no more mere

phones; they are computers or extension of computers. “As increasing levels of online activity once confined to desktop and laptop computers takes place on Smartphones” (House of Commons, UK, 2012 , p. 13). The mobile phones have great advantages and many a times it ensures the safety of an individual (Nasar, Hecht, & Wener, 2007). However, these mobile phones also put individuals in danger. The provision of Bluetooth, wireless and internet connection in these phones provides the same chance of victimization as of the users of the computers with internet connection.

“The McAfee Threat Report for the third quarter of 2011 showed that mobile phone malware had doubled since 2009 and that the majority of new malware on mobile platforms had been targeted at android phones” (House of Commons, UK, 2012 , p. 5). The Norton study (2011) found that 80 percent of the male respondents who use mobile phones have become victims of cyber crime. Also bullying through mobile phones has increased to a great extent (Campbell, 2005; Kumar & Jaishankar, 2007; Erentait_e, Bergman, & Zˇ ukauskien_e, 2012). A research on child sexual exploitation in the UK, found that the offenders initially victimize the children on the internet via computers, later, they move on to mobiles, especially Smartphones to victimize the children. This methodology is also used for victimizing adults (Policy, Research & Media, 2012).

4. *Vulnerability of children and teens increased to a greater extent*

In the new millennium, there is a steep rise of children and teens using the Internet. They are faster than the adults in using the internet and mobile phones. They grasp the technology faster than adults and even they become teachers of older persons in the usage of mobile phones and the internet. However, the same knowledge of the internet and mobile phones puts them in danger. Online predators may exploit their curiosity to understand many things, including sex (Wolak, Finkelhor, Mitchell, & Ybarra, 2008) and many children and teens become victims of cyber crimes. Wolak, Mitchell, and Finkelhor (2006) study on online victimization of youth found that youth are susceptible to victimization and they become victims of online sexual solicitation. A new study in the UK found a steep raise in online grooming for sexual exploitation, since 2010. The study found that the victims were groomed via mobile phones and social networking sites such as Facebook, Orkut, and Twitter (Policy, Research & Media, 2012).

Alternatively, a recent research found that youth and children have become more aware of their victimization online and there is a reduction

of online sexual solicitation, however points out an increase in the online harassment of youth, especially girls (Jones, Mitchell, & Finkelhor, 2012). It should be noted that more and more children and youth flock the cyber space. Though there may be a diminutive rise of awareness of cyber crime among a section of children and youth in the internet, still there are potential victims who are newer to the cyber space.

Also, sexting, a new form of cyber crime in which a teen is both the offender as well as the victim, have created further victimization of children online. Sexting, though considered as a victimless crime (Jaishankar, 2009a&b), brings in more potential victims online. A recent research on sexting and personal victimization (Reyns, Burek, Henson, & Fisher, 2011), found that, not only sexting makes them victims of sexting, but it makes them victim of several forms of online victimization.

5. *Differential victimization of men and women*

The risk taking behavior of men in the physical space and the vulnerability of women in the physical space are the same in the cyber space. However, the patterns of victimization in the cyber space show a differential aspect. The Norton study (2011) suggests that men are susceptible to victimization as they take the risk of visiting pornographic sites and gambling sites and talking with strangers, than women. The study found that 72 per cent of men have become victims compared 65 per cent women. "Men are also more vulnerable because nearly four times more men than women view adult and pornographic sites, while twice as many gamble online and go online dating" (Limsamarnphun, 2011, para 4). The Norton study also found that men between 18-31 age groups spending more time on the internet are vulnerable to victimization.

When it comes to online women victims, they are more vulnerable to be a victim of cyber crime and also the impact of victimization is more on them compared to men. Especially women are prone to online harassment and stalking (Desai & Jaishankar, 2007). This aspect is different when compared to men as they are not that much harassed or stalked online (Halder & Jaishankar, 2012). Men become online victims because of their risky behaviour, but women become victims because of their mere presence online. A cyber stalking statistics (2010) of Working for Halting Online Abuse (WHOA) shows that there is an unequal ratio of men and women victims as well as harassers. Among 349 victims, 73% are women and 27% are men; whereas, 44.5% harassers were men

and 36.5% harassers were women (Halder & Jaishankar, 2012). Comparatively, women don't report their online victimization to the police, than men. So a clear statistics of online women victimization is not available. Also the impact of victimization on women is different than men. Cyber crimes create a deeper wound in women (Halder & Jaishankar, 2008; Halder & Jaishankar, 2012). Halder and Jaishankar (2012) explain the impact of online victimization on women compared with men:

When a man's email id or private data stored in websites and also personal computers are accessed and modified in an unauthorized way, he can afford to live on by informing the police and his acquaintances. Indeed his reputation may be marred due to misuse of the personal data. Unlike a woman victim, he may not be subjected to gross humiliation by the society as a whole; he may neither be reduced to a mere 'sex item' like his female counterpart. His victimization may be judged only from the perspective of economic losses. On the contrary, a woman who may have turned into a victim may be ostracized by the society. Unlike her male counterpart, she may not be able to take the online humiliation so easily; it may engulf her with the feeling of shame and hatred for herself (p. 5).

6. *Lack of reporting behaviour, secondary victimization and reliance on online private policing groups*

Under reporting of cyber crimes is commonly found (Wall, 2001). Reporting cyber crimes is difficult for the victims as most of the victims are educated and knowledgeable. Victims might feel that the police will abuse or ridicule them because of their victimization. Especially women victims cite privacy issues for not reporting to police (Halder & Jaishankar, 2012). "Many victims of cyber-crimes may not realize their victimization until long after the event. Victims may be reluctant to report cyber-crimes due to embarrassment, not knowing where or how to report the crime, or the size of the loss" (Roberts, 2008, 2009, p. 580; Wall, 2004). Also there are instances where secondary victimization is highly prevalent in cyber crime cases, especially cyber gender harassment (Halder & Jaishankar, 2011). Still the criminal justice system including police, prosecutors and judiciary of many countries are not ready to solve the cyber crime cases and provide justice to the victims. This has pushed the victims towards a new trend of reporting their victimization to agencies other than the police. Because of the secondary victimization and lack of proper resources with the criminal justice system, now, victims prefer non governmental agencies which

work in "private policing" (Yar, 2010) of the internet. In the new millennium, many NGO's have come to support and assist the cyber crime victims. The Internet Watch Foundation (IWF) of UK, Working to halt online abuse (WHOA), of the USA, Cyberangels, of the USA, and Centre for Cyber Victim Counselling (CCVC) of India are some of the NGO's that cyber victims rely to report their victimization (Halder & Jaishankar, 2012).

Conclusion

The patterns and trends of cyber crime victimization have given a new dimension to the contemporary criminal behaviour analysis. It has changed the conventional perspective of criminologists, police and criminal justice officials towards cyber crimes, criminal behaviour and victims. Moreover, the complexities involved in the investigation of cyber crime victimization have brought a new culture among police agencies. The cyber crime victimization has made law enforcers to be more techno savvy than before (Jaishankar, 2010). It has become a situation like; either learn technology or leave it to the technocrats. Also as the criminal justice system needs to deliver justice to the victims of cyber crimes, new laws are promulgated in almost all the countries.

Cyber crime victims have not got the same attention by the media, criminal justice system and academics as that of the cyber crime offenders (Wall, 2001). The reason is that, the victims do not provide the kind of novelty the offenders provide. The victims of cyber crimes are not much unique than the victims of conventional crimes, though, they have some distinctive characteristics. They may have created a trap for themselves on the internet and hence they become engulfed in shame, trauma as well as self-hatred. The victims cannot be bounded in any particular age group, nationality, race, religion; they can be children, teenagers, males, females, even aged net surfers or even persons who may be oblivious of the fact that he/she is being attacked in the internet, by fake mails. Adequate attention of these victims from the criminal justice officials as well as victim service providers is needed (Jaishankar, 2010). Also research on these victims is most needed. It will help to prevent and mitigate further victimization and provide policy directions to the governments. The current status of cyber crime victimization needs to be studied in detail.

References

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*. PhD Dissertation submitted to Mississippi State University.

Arena, K. (2001). U.S. targets porn site's customers, CNN.com web site (Aug. 8, 2001), Retrieved on December 15, 2011, from *http://www.cnn.com/2001/LAW/08/08/ashcroft.childporn/*

Australian Institute of Criminology (AIC) (2006). *Cyber crime: Definitions and general information*. Retrieved on January 12, 2012, from *http://www.aic.gov.au/topics/cyber crime/definitions.html*

Brenner, S. (2004). Toward a criminal law for cyberspace: Distributed security. *Boston University Journal of Science & Technology Law*, *10*(2), 1-105.

Briggs, F. (2003). *From victim to offender: How child sexual abuse victims become offenders*. NSW, Australia: Allen & Unwin.

Broidy, L. M., Daday, J. K., Crandall, C. S., Sklar, D. P., & Jost, P.F. (2006). Exploring demographic, structural, and behavioral overlap among homicide offenders and victims. *Homicide Studies*, *10*, 155-180.

Byassee, W. S. (1995). Jurisdiction of cyberspace: Applying real world precedent to the virtual community, *Wake Forest Law Review*, 30, 197, 198 n.

Campbell, M. A. (2005). Cyber bullying: An old problem in a new guise?. *Australian Journal of Guidance and Counselling*, *15*(1), 68-76.

Carter, D. (1995). Computer crime categories: How techno-criminals operate. *FBI Law Enforcement Bulletin*, 64(7), 21.

Davis, R., & Hutchison, S. (1997). *Computer crime in Canada*. Toronto: Thomson Canada Limited.

Deflem, M., & Shutt, J. E. (2006). Law enforcement and computer security threats and measures. In H. Bidgoli (Ed.), *The handbook of information security,* volume 2: *information warfare; social, legal, and international issues; and security foundations* (pp. 200-209). Hoboken, NJ: John Wiley & Sons.

Desai, M., & Jaishankar, K. (2007). *Cyber stalking victimization of girl students: an empirical study.* Presentation in the Second International Conference on Victimology and Sixth Biennial Conference of the Indian Society of Victimology, Chennai, India 9-11, February, 2007.

Eddy, N. (30th November, 2011). Cyber-crime victims often provide access unwittingly: report. Security. Retrieved on January 25, 2012 from *http://www.channelinsider.com/c/a/Security/Cybercrime-Victims-Often-Provide-Access-Unwittingly-Report-549746/*

Erentait_e, R., Bergman, L. R. &Zˇ ukauskien_e, R. (2012). Cross-contextual stability of bullying victimization: A person-oriented analysis of cyber and traditional bullying experiences among adolescents. *Scandinavian Journal of Psychology.*1-10.

European Commission (2001). Communication from the European Commission to the Council and the European Parliament 1.1, COM, 890 final, at 9 (Brussels, Jan. 26, 2001), Retrieved on 15 December 2011, from *http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html.*

Financial Fraud Action UK (2011). East Londoners at Greatest Risk of Falling For Money Laundering Scam. Retrieved on 2nd February 2012 from *http://www.financialfraudaction.org.uk/cms/assets/1/MoneyMulesRelease.pdf*

Florêncio, D., & Herley, C. (2010). *Phishing and money mules.* Redmond, WA, USA: Microsoft Research, One Microsoft Way. Retrieved on January 15, 2012 from *http://research.microsoft.com/pubs/143095/mules.pdf*

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*, 243–49.

Halder, D., & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academy Journal*, Singapore, *3*(1), 48-62.

Halder, D., & Jaishankar, K. (2009) Cyber socializing and victimization of women. *Temida - The journal on victimization, human rights and gender,* September 2009, *12*(3), 5-26.

Halder, D., & Jaishankar, K. (2010). Cyber Victimization in India: A Baseline Survey Report. Tirunelveli, India: Centre for Cyber Victim Counselling. Retrieved on January 15, 2012, from *http://www.cybervictims.org/CCVCresearchreport2010.pdf*

Halder, D., Jaishankar, K., Periyar, E. E. & Sivakumar, R.(2011). *Cyber Victimization in India: an empirical analysis.* Presentation in the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) 15-17, January, 2011, at Jaipur, India.

Halder D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of US, UK and India. *Victims and Offenders*, *6*(4), 386-398.

Halder, D., & Jaishankar. K. (2012) *Cyber crime and victimization of women: Laws, rights, and regulations*. Hershey, PA, USA: IGI Global.

Heylighen, F. (1994), *Cyberspace Principia Cybernetica web.* Retrieved on December 15, 2011, from http://pespmc1.vub.ac.be/CYBSPACE.html

House of Commons, UK (2012). *Malware and cyber crime. Twelfth report of session 2010–12*. London, UK: House of Commons, Science and Technology Committee.

IPWatchdog.com (2003). *About cyber crime*, IPWatchdog.com Web Site, Retrieved on December 15, 2011, from *http://www.ipwatchdog.com/cyberc rimes.html*

Jaishankar K., (2008). Space transition theory of cyber crimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2009a). Sexting: A new form of victimless crime. *International Journal of Cyber Criminology*, *3*(1), 21-25.

Jaishankar K., (2009b). *Sexting: How do we protect the victim turned offender?,* Presentation at the Workshop on "Victim Protection" in the International Conference on "Protecting Children from Sexual Offenders in the Information Technology Era" organized by the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC), during December 11- 13, 2009 at Courmeyeur, Mont Blanc, Italy.

Jaishankar, K. (2010). *Victims of cyber crimes - A study on developing Profile, Legal Reviews and Policy Guidelines.* Research under Commonwealth Fellowship held at Centre for Criminal Justice Studies, School of Law, University of Leeds, UK.

Jaishankar, K. (2011). Epilogue: Raising the human spirit and restoring order in the information super highway. In P. Madhava Soma Sundaram, & Syed Umarhathab. (Ed.), *Cyber crime and digital disorder* (pp. 149-153).Tirunelveli, India: Publication Division, Manonmaniam Sundaranar University.

Jennings, W. G., Higgins, G. E., Tewksbury, R., Gover, A. R., & Piquero, A. R. (2010). A Longitudinal assessment of the victim-offender overlap. *Journal of Interpersonal Violence*, 25, 2147-2174.

Jennings, W. G., Park, M., Tomsich, E. A., Gover, A. R., Akers, R. L. (2011). Assessing the overlap in dating violence perpetration and victimization among South Korean college students: the influence of social learning and self-control. *American Journal of Criminal Justice*, *36*(2), 188-206.

Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior*, *17*(1), 16-26.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: findings from three youth internet safety surveys 2000-2010. *Journal of Adolescent Health*, *50*(2), 179-86.

Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace in the internet*. London and New York: Routledge.

Klevens, J., Duque, L. F., & Ramírez, C. (2002). The victim-offender overlap and routine activities: Results from a cross-sectional study in Bogotá, Columbia. *Journal of Interpersonal Violence*, *17*, 206-216.

Kumar, A. R., & Jaishankar, K. (2007). *Cyber bullying using mobile phones: A study on victimization and perpetration among school students.*

Presentation in the Second International Conference on Victimology and Sixth Biennial Conference of the Indian Society of Victimology, Chennai, India 9-11, February, 2007.

Lastowka F. G & Hunter, D. (2004). Virtual crimes. *New York Law School Law Review, 49*, 293-316.

Lauritsen, J. L., & Laub, J. H. (2007). Understanding the link between victimization and offending: New reflections on an old idea. *Crime Prevention Studies, 22,* 55-75.

Limsamarnphun, N. (2011). Is your data safe and secure? Retrieved on 15 January 2012 from *http://www.nationmultimedia.com/new/opinion/Is-your-data-safe-and-secure-30166572.html*

Mann, D., & Sutton, M. (1999). NetCrime. More change in the organisation of thieving. *British Journal of Criminology*, *38*(2), 201–228.

Matt, S. M. 2004. Cybercrime: A comparative law analysis. Unpublished Dissertation submitted for the Degree of Magister Legum (LLM) at the University of South Africa. Retrieved 15 December, 2011, *http://uir.unisa.ac.za/dspace/bitstream/10500/2056/4/02chapter2.pdf*

McAfee. (2011). *A good decade for cybercrime: McAfee's look back at ten years of cybercrime, report*. Retrieved on 15 January 2012 from *http://www.mcafee.com/ca/resources/reports/rp-good-decade-for-cybercrime.pdf*

Mitra, A., & Schwartz, R. L. (2001). From cyberspace to cybernetic space: Rethinking the relationship between real and virtual spaces. *Journal of Computer-Mediated Communication*, *7*(1). Retrieved 15 December, 2011, from *http://jcmc.indiana.edu/vol7/issue1/mitra.html*

Mustaine, E. E., & Tewksbury, R. (2000). Comparing the lifestyles of victims, offenders, and victim-offenders: A routine activity theory assessment of similarities and differences for criminal incident participants. *Sociological Focus*, *33*, 339-362.

Nasar, J., Hecht, P., & Wener, R. (2007). 'Call if you have trouble': Mobile phones and safety among college students. *International Journal of Urban and Regional Research*, *31*(4), 863–873.

Norton (2011). *Norton Cybercrime Report: The Human Impact.* Retrieved on 15 January, 2012, from *http://us.norton.com/theme.jsp?themeid=cybercrime_report*

Parker, D. (1999). Automated crime, information security. Retrieved on December 15 2006, from *http://www.infosecuritymag.com/articles/1999/autocrime.shtml*

Parker, D. (2002). *Automated crime, windowsecurity.com web site* (Oct. 16, 2002), Retrieved on December 15 2006, from *http://secinf.net/misc/Automated_Crime_.html/.*

Parliamentary Joint Committee on the Australian Crime Commission

(PJCACC) (2004) *Cyber crime*. Parliament of the Commonwealth of Australia: Canberra

Policy, Research & Media. (January 2012). *Cutting them free: How is the UK progressing in protecting its children from sexual exploitation?* Retrieved on 1 February, 2012 from *http://www.barnardos.org.uk/cuttingthemfree.pdf*

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2011). The unintended consequences of digital technology: exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*. iFirst, DOI:10.1080/0735648X.2011.641816, Available online: 7 Dec 2011

Roberts, L. (2008). Cyber-victimisation in Australia: Extent, impact on individuals and responses. *TILES Briefing Paper No. 6*.

Roberts, L. D. (2009). Cyber-Victimization. In R. Luppicini & R. Adell (Eds.), *Handbook of research on technoethics* (pp. 575-592). Hershey, PA, USA: IGI Global.

Rumgay, J. (2010). *When victims become offenders: in search of coherence in policy and practice.* Report of the Fawcett Society. Retrieved on 15 January, 2012 from *http://www.fawcettsociety.org.uk/documents/When%20Victims%20Become%20Offenders%20Report%2014.12.04.pdf*

Schreck, C. J., Stewart, E .A., & Osgood, D. W. (2008). A reappraisal of the overlap of violent offenders and victims. *Criminology, 46,* 871-906.

Shaffer, J. N. (2003). *The victim-offender overlap: Specifying the role of peer groups.* Unpublished Doctoral thesis submitted to the Pennsylvania State University, USA.

Smith, R., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial.* Cambridge: Cambridge University Press.

Statistics Canada (2002). *Cyber-crime: issues, data sources and feasibility of collecting police-reported statistics*. Ottawa: Canadian Centre for Justice Statistics.

Suler, J. (1999). To get what you need: Healthy and pathological Internet use. *CyberPsychology and Behaviour*, *2*, 385-393.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology and Behaviour*, *7*, 321-326.

Suler, J. (2005). *The psychology of cyberspace*. Retrieved on December 15 2006, from *www.rider.edu/suler/psycyber/psycyber.html.*

Suler, J. R., & Phillips, W. (1998). The bad boys of cyberspace: Deviant behavior in multimedia chat communities. *CyberPsychology and Behavior*, *1*, 275-294.

Umarhathab, S., Rao, G. D. R., & Jaishankar, K. (2009). Cyber crimes in India: a study of emerging patterns of perpetration and victimization in Chennai city. *Pakistan Journal of Criminology, 1*(1), 51-66, April 2009.

Wall, D. S. (1999). Cybercrimes: new wine, no bottles? In P. Davies, P.

Francis & V. Jupp (eds.), *Invisible crimes: their victims and their Regulation* (pp. 105-39). London: Macmillan,

Wall, D. S. (2001). Cyber crimes and the internet. In D. Wall (ed.) *Crime and the internet* (pp. 1-17). London: Routledge.

Wall, D. S. (2004). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 78-94). Thousand Oaks, CA: Sage Publications

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information Communication and Society*, *11*(6), 861–884.

Wall, D. S. (2010). Cyber crimes. Class notes, masters course in criminology and law. School of Law, University of Leeds. On personal communication.

WHOA. (2010). Cyber stalking statistics. Retrieved on January 15, 2012 from *http://www.haltabuse.org/resources/stats/2010stats.pdf*

Wolak, J., Finkelhor, D., Mitchell, K., & Ybarra, M. (2008). Online "predators" and their victims: myths, realities, and implications for prevention and treatment. *American Psychologist*, *63*, 111-128

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth: Five years later*. Alexandria, VA: National Center for Missing & Exploited Children Bulletin - #07-06-025.

Yar, M. (2005) The novelty of 'cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427:

Yar, M. (2006). *Cybercrime and Society*. London: Sage Publications.

Yar, M. (2010). The private policing of internet crime. In Y. Jewkes & M. Yar. (Eds.), *Handbook of internet crime* (pp. 546 - 561). Cullompton: Willan Publishers.

ORGANISED CYBER CRIME: MYTH OR REALITY, MALIGNANT OR BENIGN?

ROB MCCUSKER
Director of Centre for Fraud and Financial Crime; University of Teesside Middlesbrough, UK

The very fact that the notion of a connection between organised crime and cybercrime has been considered, and continues to form the basis of inter-governmental debate, reflects the dynamic nature of, and rapidity of change within, transnational crime. By their very nature, transnational crime networks are loosely structured, motivated by profit and engage in long-term, dividend rich, enterprise criminality. They are both proactive (in terms of conceiving new crimes or committing old crimes in new ways) and reactive (in terms of their ability to respond immediately to sudden changes in law enforcement activity or legislative change).

They are no longer ethno-centric in organisational constituency and they remain ever more multi-jurisdictional, forming strategic alliances and attaining a degree of symbiosis with governments, law enforcement and the judiciary via systemic corruption. As with their legitimate business counterparts transnational crime networks have taken advantage of the globalisation process with its integration of trade, technology, transportation, communications, information and financial systems and, unlike those counterparts, have managed to actively exploit differential regulatory and legal regimes and differential State capacity to respond to their actions. It is clear that transnational crime will continue to grow in volume and impact and that it will increasingly affect the financial stability of society in addition to continuing to cause the social, political and cultural effects it has historically demonstrated. Moreover, far more than has hitherto been the case the potential for the mitigation of transnational crime lies as much in the hands of the financial and other business sectors as it does in the continued efforts of law enforcement and intelligence agencies. The difficulty however lies in convincing such sectors of this new and important reality.

Cybercrime has become an integral part of the transnational threat landscape and more recently, the concept of 'organised crime' has been attributed to cybercriminality. There has been subsequent disagreement and confusion concerning whether such crime is a derivation of traditional organised crime or an evolution of such crime within the online space. This opaque state of affairs has been exacerbated by the relative lack of clear evidence attesting to and supporting either sce-

nario. Technological advances have always been used to the advantage of the criminal fraternity. The crucial question that remains is whether those advances have merely facilitated the commission of physical crime or whether in fact they have led to the creation of a new wave of traditional, but virtual, organised crime.

In broad terms, the debate surrounding the actual and/or prospective involvement of traditional organised crime groups in cybercriminal activity is characterised by a tension between logic and pragmatism. Logic would dictate that traditional organised crime groups will engage with cybercriminal endeavours as fervently as they will with any low risk, high profit non-virtual criminal activity. Pragmatism on the other hand would suggest that it remains questionable whether such groups either need that engagement or indeed have the capacity to exploit the cyber environment to the extent that their capital investment would produce the desired and appropriate financial gains.

Wall was noted that '...when so-called cases of cybercrime come to court, they often have the familiar ring of the "traditional" rather than the "cyber" about them[1].' However, crime, like nature, abhors a vacuum. It has accordingly always seemed inevitable perhaps that traditional organised crime groups would positively rush to fill the void for illicit product placement deemed to present itself in the context of cyberspace. It might be assumed, therefore, that an evaluation of the purported involvement of traditional crime groups in cybercrime would be a relatively simple affair. Certainly, the literature, broadly defined, is replete with references to 'cybercrime' and more recently to 'organised' cybercrime. Unfortunately, the mere assertion in much of that literature that such crime exists (both in a general sense and in an organised form) has been routinely transmuted, as if by osmosis, into tangible fact. Arguably, however, in many cases those 'facts' appear to rely as much upon anecdote, hearsay, extrapolation and assumption as they do upon objectively obtained and verified evidence.

At the basic level of analysis there is no discernible control mechanism in place insofar as terminology is concerned. Thus, one might speak of 'cybercrime,' 'high tech crime,' 'computer crime,' 'technology crime,' 'digital crime' and 'IT crime' and be discussing the same and/or different concepts, respectively. Achieving any vestige of comparative analysis of the impact of cybercrime therefore is fraught with difficulties. Beyond that, the increasingly common conflation of cybercrime with the prefix 'organised' infers the involvement of traditional organised crime groups but ultimately alludes to 'ordinary' criminals who happen to operate in cyberspace in an organised manner. Equally, it seems common to refer to cybercriminal 'groups' as if they were of

---

1 Wall, D. S. (2004). The internet as a conduit for criminal activity in A. Pattavina (Ed.), *Information technology and the criminal justice system* (Chapter 4:77). Sage

equivalent size, complexity, 'stature' and duration as their traditional, non-virtual counterparts. This effectively allows cybercriminal groups to achieve the semblance of the organisational evolution actually achieved by those traditional organised crime groups they are deemed to emulate. In short, there remains a confused and confusing plethora of terminology, purported parameters and alleged participants of cybercrime as well as concerns over the provenance and quality of evidence elicited in support of such activity. These are certainly subtle differences but they are important differences nevertheless.

In consequence the term 'cybercrime' has rapidly become a generic descriptor for any malfeasant online behaviour (whatever the relative differences in complexity and seriousness) ranging from spam emails and denial of service attacks to malware and botnet infiltration. It is the very imprecision of the term which has given rise to the hyperbole and opacity that surrounds it.

Beyond the broad non-specificity of definition lies an equally amorphous conundrum, which forms the heart of this piece, namely, whether 'organised' cyber crime is crime committed by traditional organised crime groups or 'merely' that it is crime committed online in an organised manner. Even at this juncture the question is fraught with difficulty.

The term 'organised,' when applied to traditional organised crime groups, is defined (see, inter alia, the UN Convention against Transnational Crime[2]) and subsequently assessments of organised crime can gravitate to and from a fixed point. However, 'cybercrime' is seemingly deemed to be 'organised' once the perpetrator ceases to be the archetypal lonely hacker and gravitates instead towards a group of fellow lonely hackers. If acting in illegal concert were the sole arbiter of 'organised' crime then any form of criminal behaviour which necessitated any degree of planning might be deemed de facto to be organised crime.

These assertions are somewhat incongruous and consequently both sets of assertions do little to clarify the distinction between traditional organised crime involvement in cyberspace and criminals who simply operate in the online space.

In truth, fewer terms are destined to create a greater state of apoplexy within law enforcement agencies than 'cybercrime,' a fact reflected in part by their usual depiction of such crime as 'high tech' rather than 'cyber' in nature. The tension between the law enforcement perspective on the one hand, and the assertions within oft-accessed and cited literature on cybercrime on the other, may appear to be a little odd given the accepted use of technology by criminals generally. Indeed, unlike

---

2 Article 2 (a) of the UN Convention Against Transnational Organized Crime defines an 'organised criminal group' as a '...structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with [the] Convention, in order to obtain, directly or indirectly, a financial or other material benefit.'

organised crime in the twentieth century, cybercrime in the twenty-first century is arguably more akin to an adaptation of existing crime to new technology than the creation of a brand new crime type and/or structure. Equally, one might assume that in order to operate effectively within the relative complexity of the online environment one would have to be organised as a matter of course. In this sense, the debate as to whether criminality is organised or not might be deemed somewhat redundant. However, given the finite nature of law enforcement resources it remains important strategically and logistically for cybercrime efforts to be directed at the actual rather than supposed criminals. That, in turn, renders the question as to whether one is confronting traditional organised crime in an online context, or online criminals who happen to be organised, a practical and serious one.

One might argue that the potential future of cybercrime sits within the broader digital environment, an environment created primarily to facilitate social and business relationships and transactions but one which is increasingly prone to degradation, infiltration and subsequent malfeasant activity. Although the precise future characteristics of cybercrime cannot be accurately determined it remains both possible and appropriate to frame potential cybercrime activities within the context of developments in technology more broadly and of the digital environment it supports and operates within.

As suggested at the outset, logic alone would suggest that the digital environment will be increasingly targeted by traditional organised crime groups. The recognition by the business sector of the wealth of product placement opportunities available on the Internet will not have escaped the notice of traditional organised crime entities. Conversely, the extent to which there has been a major development in traditional organised criminal behaviour and activity, as a direct or indirect result of cybercrime developments per se, is starting to be questioned.

The Internet, for example, was never designed to be a highly developed or intelligent system. The basic purpose of the Internet, a vehicle for conveying packets of data between devices (the "end to end principle"), has remained unchanged and the resultant architecture, whilst embracing the original unfettered communication precept of the Internet, has facilitated an increasing vulnerability to inadvertent technical failings as well as advertent criminal and other malfeasants. It is clear that it is becoming less and less able to cope with the exponential demands, in terms of information storage and exchange, being placed upon it. In addition, globalisation requires, and will continue to necessitate, an increased connectivity of the world's computer, banking and financial systems. Globalisation has increased the free movement of capital between the world's developed and underdeveloped economies. Globalisation operates in cyberspace, which by definition is extraterritorial. This means that the regulatory practices which purport to exist and operate in the landlocked world, and which should be the *sine qua non* of the globalised economy, are missing.

Furthermore, the Internet was never designed to be secure from exploitation. The strength of the Internet in terms of its rapid communication facility has become one of its undermining weaknesses. The criminal fraternity operates online under the same free market principles and the legislative and law enforcement endeavours launched against them suffer from geographical and practical restrictions. The potential for an increase in the number of victims of economic crime, as well as cybercrime more broadly, is likely to rise.

The dissemination, storage and protection of information lie at the heart of the Internet, ecommerce and the online environment per se. Personal information about clients and customers is increasingly being lodged in digital documentation and that digital documentation is being routinely disseminated between computer networks. This distributed digital identity places confidential information in the ether with only the security processes of the organisation to prevent its exploitation. The acquisition and abuse of such information is likely to continue to form the basis of the future cybercrime threat.

Increasing dependency upon computer systems to control and operate key infrastructure may leave such control systems, and the populations who depend upon their effective operation, prone to the consequences of any subsequent breach. Importantly, the wider dissemination and availability of technology may render it a far easier task for criminals to engage fraud and fraud-related endeavours. Technology is destined to become increasingly ubiquitous. Established technologies such as mobile phones and computers will continue to widely used but there is likely to be a proliferation of auxiliary devices aimed at improving the performance and flexibility of those established products.

It is recognised that in fact, flatter, more horizontal networks, comprising cell-like 'crews,' have become the norm in much of the organised crime environment

Nisbett suggests that '[l]ogically, the first issue to consider when analysing forms criminal organization may take in cyberspace is the extent to which already-evolved forms of criminal organization are likely to migrate to the virtual frontier. Since the already evolved forms of criminal organization have proven successful in the real world, it is reasonable to expect that they will enjoy at least a measure of success in the cyberworld[3].'

The flexibility of the organisation and control of traditional crime groups has in part derived from a proactive reaction by such groups to law enforcement endeavours and operations against such groups. Whilst one might

---

3 Nisbett, C (2002). New directions in cyber-crime. White Paper, QineticQ, *http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0012.File.pdf*

argue that such structural changes have resulted more from the necessity of protection than through freedom of choice, this demonstrated ability to make such organisational changes augurs well for similar adaptations to be made by traditional organised crime groups in reaction to, and after reflection of, changes in their operating environment, namely, cyberspace. Olson maintains that '[o]rganized crime is perfectly suited to profit from the information revolution. Its existence relies on innovating, adapting strategies and operations, and evading detection. These attributes complement the ever-changing nature and unpredictability of the information revolution. The Internet offers an array of lucrative opportunities with little or no risk[4].'

There has been a degree of rumination over whether the 'organised crime in cyberspace' versus 'crime in cyberspace which is organised' debate is itself being taken over rapidly by events. Clarberg has pointed out that '...high technology crime is often not a crime in isolation, and forms part of a crime which is also occurring within the physical world. It is very difficult to find a real world crime that does not have a high technology element, even if it is as common and straightforward as the use of a mobile telephone[5].' There have also been suggestions that in fact, as with the purported convergence of organised crime and terrorism in light of perceived mutual benefits, the two sides of the 'organised' debate may in fact find greater solace, reward and operational fluidity through a combination of their efforts[6]. Olson maintains that '[e]lements of both the cybercrime and organized crime worlds have encouraged the two to merge. Hackers were traditionally antisocial loners, operating without any monetary motivation. Their motivations have now shifted from mere curiosity to more self-serving and lucrative attacks. But hackers now frequently work together in loosely knit units or cells[7].' Furthermore, she notes that '[m]any of the characteristics traditionally attributed to organized crime can also be attributed to cybercriminals and hackers. This

---

4 Olson, J. L. (2004). The threat of systematic and organized cybercrime and information warfare: 17
http://www.american.edu/tracc/resources/publications/students/olson01.pdf

5 Clarberg, B. (2003). Cyber crime, Paper presented at the conference on international cooperation on transnational crime, The Hague, 9–10 October (unpublished)

6 See, for example, McCusker, R. (2006) Organised crime and terrorism: Convergence or separation?, ECPR
Standing group on organised crime newsletter (5:2) 2–5
http://www.essex.ac.uk/ecpr/standinggroups/crime/documents/SGOC_Vol5_2.pdf

7 Olson, op.cit: 15

overlap in skill and motivation has created a natural bond between the two underground networks[8].'

More radically still is the notion that the intrinsic nature of cyberspace will in fact alter the very notion of the term 'organised' whether applied within the context of organised crime of the traditional-oriented or cyber-born complexion. Nisbett has observed a truism that '[i]n the cyberworld...one's aptitude as a cybercriminal is a function of his or her technical expertise...While there may be opportunistic reasons to affiliate with a cybercriminal group, such an affiliation is not essential for the pursuit of a criminal career, as it is for members of real-world gangs[9].' As Brenner has it,'[t]he characteristics of cyberspace, the absence of fixed, empirical constraints and a diffuse, fluid, evolving environment, indicate that hierarchical organizational structures are at once not needed in and not appropriate for activities conducted in cyberspace. What, then, will criminal organization look like in cyberspace?...will organized criminal activity in cyberspace ever actually exist[10]?'

Some authors have posited that cybercrime itself may alter the structure of traditional organised crime groups. The Council of Europe once noted, for example, that '[c]ybercrime requires less control over a geographical territory, less violence and intimidation, less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals, in short less need for formal organisations[11].' Brenner has suggested that '[o]nline criminal organization will tend to de-emphasize formal, hierarchical organizational structures. At the same time, it will emphasize a broader, lateral contextual structure. Online criminal organization has no reason to be circumscribed, in its membership or in its operations, by national, territorial boundaries or by cultural differences because cybercriminals...share a culture that transcends national borders and context. So, as opposed to the localized, rigid, and often provincial hierarchical organizations that have so far characterized criminal groups, regional, or even global, coalitions will develop[12].'

---

8 Ibid: 16

9 Nisbett, op.cit

10 Brenner, S.W, Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina, Journal of Law and Technology, Volume 4, Issue 1: Fall 2002:39

11 Council of Europe (2005). Organised crime situation report: Focus on the threat of economic crime, *http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/8_ Organised_crime/Documents/Report2005E.pdf*

12 Brenner, op.cit: 45

Such coalitions are likely to comprise a mixture of '...cybercrime entrepreneurs...' and '...diffuse, loosely-structured opportunity groups...'[13] which are, in a manner currently typical of 'Russian' organised crime groups in the physical environment, likely to collude in relation to a specific offence and thereafter disband. The ties that bind and typify traditional organised crime groups in terms of membership criteria and strategic alliances are likely to become less constricting. The '...traditional indicia of commitment, and of membership, will decline in importance. Instead of multi-generational criminal enterprises, cybercriminal organization will emphasize arm's length, instrumental associative alliances[14].'

The catalyst behind the current debate concerning traditional organised crime online, or online crime that is organised, is the nature and quality of evidence adduced in support of either and/or both camps. Given the accepted precept that opportunity, tempered by an evaluation of relative risk, provides the key incentive to criminal endeavour, logic, if not evidence, would suggest that traditional organised crime groups and/or networks are fully engaged in the exploitation of the cyber environment.

There are undoubtedly criminal elements (known colloquially as 'super-empowered criminals') operating in the online environment as obtainers and disseminators of identity and identity-related information. Panda Security[15] noted that the FBI had determined the existence of range of cybercrime professional positions which it was felt provided credence to the organised nature of such crime. These positions comprise 'programmers' (who develop malware), 'distributors' (who trade and sell stolen data), 'tech experts' (who maintain criminal enterprises' IT infrastructure), 'hackers' (who search for and exploit system vulnerability), 'fraudsters' (who create and deploy social engineering vehicles, e.g. Phishing), 'cashiers' (who control drop accounts and provide names and accounts to criminals), 'money mules' (who complete wire transfers between bank accounts), 'tellers' (who transfer and launder illicit proceeds) and 'organization leaders' (who assemble team and select targets).

It seems certain, that traditional organised crime groups are prepared to pay for such information in order to facilitate the commission of physical rather than virtual crimes. As Deloitte recently noted, '[d]ata is more valuable than money. Once spent, money is gone, but data can be used and reused to pro-

---

13 Ibid

14 Ibid: 47

15 Panda Security, 2010, The Cyber-Crime Market: Uncovered, *http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf*

duce more money. The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities'[16]. A relatively recent but growing threat vector for the dissemination, capture and abuse of information is social networking. Sophos[17] noted that 1 in 7 users on Facebook was logged into their profile all the time during office hours and using a false profile Sophos managed to obtain, inter alia, dates of birth, current email addresses or telephone numbers of other users and in some cases secured employment details, resumes and a mother's maiden name . Ofcom noted in the UK context that 44% of adults who had a social network profile allowed profile to be seen by anyone (even though they could have instituted privacy settings) and 25% of social networking users had posted personal data on their profiles including telephone number, home and/or email address[18]. Symantec observed that 65% of malicious URLs were directed specifically at users of social networks[19] and Sophos[20] noted that the majority of spam, malware and phishing attacks incurred by corporations had been routed through social network accounts of staff within those corporations[21]. The Financial Services Authority in the UK noted that 'criminals appear to be changing the way in which they commit financial crime, indicating an increasing sophistication as they require more complete data to commit such crimes' and equally that '...consumer awareness of financial crime risks and how individuals may be targeted by criminals does not appear to have kept pace with the change in criminal use of technology'[22].

---

16 Deloitte, 2010: Cyber crime: a clear and present danger:Combating the fastest growing cyber security threat, *http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf*

17 Sophos, 2011, Threat Report 2011, *http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf*

18 Ofcom, 2008, Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use, *http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf*

19 Symantec, 2011, Symantec Internet Security Threat Report, *https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf*

20 Sophos, op.cit

21 Ibid

22 Financial Services Authority, Financial Risk Outlook 2009, *http://www.fsa.gov.uk/pubs/plan/financial_risk_outlook_2009.pdf*

However, it remains unclear, and indeed doubtful, whether currently there are traditional organised crime groups operating within the cyber environment. Equally, it seems likely that traditional organised crime groups will not shy away from using the cyber environment to facilitate the operation, and / or to disguise the illicit proceeds, of physical world-based crimes. The use, for example, of denial of service attacks to pursue extortion, of online banking to transfer laundered funds and the use of malware and/or botnet operators to acquire pertinent personal information for use in identity related financial crime is likely to continue to develop. The wholesale or partial mutation of traditional organised crime groups into fully-fledged cybercriminals will ultimately be determined as much by the diminished profitability, or increased risk, of real world criminal activities as it will by the innate attractiveness and relatively low risk of virtual criminality.

Part III

NATIONAL ENFORCEMENT AND INVESTIGATION AGAINST CYBERCRIME

CHINA NEW CRIMINAL LEGISLATION ON CYBERCRIME IN THE COMMON INTERNET

PI YONG
Professor School of Law, Wuhan University, China

A. Cybercrime in China

Cybercrime is a new type of crime occurring in this information age. In China, as the development of information technology, Cybercrime has been changing along with the time. Because China moved back to the normal route in 1980s, which made the application of Computer in China later than that of the west world, so did even much more late the application of Internet. Therefore computer crimes seldom occurred in China during the beginning period, most of the crimes violate the computer system without network or use them as its tools. In 1994, Internet entered into China, thereafter the number of Chinese Internet users is increasing everyday and now we have the largest internet users all over the world. In the newly blooming internet society, the computer crimes in China have two new characteristics: The first one is Internetization of crimes. There are more crimes using Internet, more interregional or transnational computer crimes appeared. The other one is that Cybercrimes in economic field happened much more frequently. Along with the development of China network economy, Cybercrimes in China rushed into the new field and has formed an industrial chain with different divisions. Many criminals use the network resources outside China to commit Cybercrime, according to statistics of Cybercrime by China Ministry of Public Security in 2010, over 90 percent of network sites, which were used to committing fraud, phishing, pornography crimes and Internet gambling, locate their server system outside China, and over 70 percent of Botnet control sides were set up in foreign countries[1].

B. China criminal legislations against cybercrime

As Cybercrime in China has been changing, China legislations on Cybercrime were amended frequently. In 1994 the State Council issued the first

[1] See general statements of Chinese delegation in the first meeting of the Intergovernmental Group of Experts of United Nations Crime Prevention and Criminal Justice Program in January, 2011.

law on computer crime, which is Ordinance on protecting the safety of computer system. In 1997, 2000, 2009 China Criminal Law was amended to increase new Cybercrimes[2], in 2011 China Supreme People's Court and Supreme People's Procuratorate issued the judicial interpretation on Cybercrime[3].

However China Criminal Procedure Law responses to Cybercrime slowly, now there is no rules on collecting electronic evidence or admissibility rules relating to electronic evidence, until 2011 Draft of amendments to China Criminal Procedure Law began to stipulate technical detection measures that include electronic surveillance[4]. But China judicial practice already goes ahead of criminal procedure law, China Supreme People's Court and Supreme People's Procuratorate issued several judicial interpretations on electronic evidence[5].

In the field of international judicial cooperation, there is no agreement between China and foreign countries on cooperation on combating Cybercrime, China does not join any international convention or treaty on Cybercrime also.

More details are given as below:

I. Provisions on cybercrime in China criminal law

In China Criminal Law, five Cybercrimes were prescribed, which are illegal accessing, illegal obtaining computer data, illegal controlling computer system, providing computer program or tools for illegal accessing or controlling computer system, and sabotaging computer system:

(1) According to the first paragraph of Article 285 of China Penal Code, Crime of illegal accessing is, illegal invading the computer system in the

---

2 In 1997 China Penal Code was amended to add Article 285, 286 and 287, which stipulated two CIA Cybercrimes (Illegal Access and Sabotaging computer system) and other tool-type Cybercrime, in which computer systems are used as the tools of crime. In 2000 Decision on Protecting Security of Network was passed by National Council to combat 21 tool-type Cybercrime. In March 2009 the 7th Amendment of China Penal Code became effective, which stipulate three new Cybercrime to combat new types of Cybercrime in the China networked economy.

3 See Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering the Safety of Computer System, which became effective on 1th, September 2011 and interprets the application of China Penal Code to new Cybercrime in 7th Amendment of China Penal Code.

4 See *http://www.npc.gov.cn/npc/xinwen/lfgz/2011-08/30/content_1668503.htm*, 2011 Draft Amendment of China Criminal Procedure Law and its interpretation.

5 See Provisions on Problems related to Examine and Identify Evidence in the Death Penalty Cases and Provisions on the Judicial Problems related to Internet Gambling Cases, which were issued by China Supreme People's Court.

fields of State affairs, national defense construction or sophisticated science and technology;
(2) According to the second paragraph of Article 285, Crime of illegal obtaining computer data is illegal invading the computer system that is not belong to the computer system described above or using other technical method to obtain computer data in the computer system;
(3) According to the second paragraph of Article 285, Crime of illegal controlling is illegal controlling the computer system, which is described in the crime of illegal obtaining computer data;
(4) According to the third paragraph of Article 285, Crime of providing computer program or tools which is used to illegal access or control computer system is, providing computer program or tools which is especially produced for the aim to illegal invade or control computer system, and in the case of knowing the computer program and tools will be used for illegal invading or controlling computer system, deliberately providing them;
(5) According to the Article 286, Crime of sabotaging computer system is, sabotaging the functions of computer system or computer data in the computer system, which results in the failure of computer system.
In addition to the above provisions, there is a kind of Cybercrime in the field of China network economy, the criminals transfer, purchase or help to sell illegal acquired data or control of computer system, in order to seek illegal interests. In order to control the new kind of crimes, the aforementioned judicial interpretation prescribed that the criminals shall be convicted and punished according to provision in Article 312 of China Penal Code, which prescribes the crime of concealing illegally acquired goods[6]. If the ISP or advertising company willfully provide for criminals of Cybercrimes the technical support or financial help, they shall be convicted and punished as the accomplice[7].
I made a comparative research of criminal legislations between China and European community, the result is that: the aforementioned provisions reaches and goes beyond the standard set by Council of European Union Framework Decision on attacks against information systems, and reaches most of requirements of Council of Europe Convention on Cybercrime.

---

6 See Article 7 of Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering the Safety of Computer System.

7 See Article 9 of Interpretation to the Judicial Problems on Dealing with Criminal Cases related to Endangering the Safety of Computer System.

II. *China criminal procedural law on cybercrime*

There is no independent criminal evidence law in China, collecting and adopting electronic evidence shall follow the common rules on evidence in China criminal procedure law and related judicial interpretations, now there are only few judicial interpretation that prescribe the rules on electronic evidence, for example, Provisions on Problems related to Examine and Identify Evidence in the Death Penalty Cases and Provisions on the Judicial Problems related to Internet Gambling Cases, which were issued by China Supreme People's Court. Since there are not sufficient rules on electronic evidence, the rules in other law field such as civil law, administrative law and the related judicial interpretations in fact play the role of instructing the police to collect electronic evidence and influencing the decision of Judge.

1. Rules on collecting electronic evidence

On the measure of retention of electronic data, China Internet regulations prescribe that ISP should record and save electronic data and provide them to the authorities if they are required[8]. The measure is not a criminal investigative measure, but it plays key role in the process of investigation to Cybercrime, without it the investigative authority cannot efficiently find Cybercrime and collect necessary evidence. So in the view of function of regulations[9], these Internet administrative regulations do help to collect electronic evidence.

On the measure of copying and detaining electronic data, before 2010 China investigative authority treated electronic data as video and voice data, so that electronic data was detained according to the rules prescribed to video and voice data. Now new judicial interpretation in 2010 prescribed special measures to copy, collect and preserve electronic data[10].

On the measure of real time collecting electronic data, there is no measure of real time collecting electronic data in China criminal procedure law, but electronic surveillance is used in the criminal investigation of

---

8 See Article 14of Management Measures on Internet Information Services, Article 19 of Implement Measures of Interim Provisions on International Networking of Computer Information Network, Article 14 of Management Measures on Internet Surfing Service Units and Article 14 of Management Measures on E-Bulletin Board Service, etc.

9 Vgl. Ulrich Sieber, Strafrechtsvergleichung im Wandel, Strafrecht und Kriminologie unter einem Dach, Kollquium zum 90. Geburtstag von Professor Dr. Dr. h.c. mult. Hans-Heinrich Jescheck, S.78-130.

10 See Article 5 of Provisions on the Judicial Problems related to Internet Gambling Cases.

serious crimes. The electronic data that is collected by using electronic surveillance cannot be used as evidence in the court[11], because it is not the evidence prescribed in the criminal procedure law, so the electronic data can only be used to find other evidence such as oral statement. The draft of new amendment of China Criminal Procedure Law that will be passed in 2012 prescribed electronic evidence and technical investigative measures, which include the electronic surveillance. The draft prescribed its scope, implementation units, applicable object, period and its extension, security clause, aim and effect of the electronic data.[12] These provisions are similar to the related legislation of foreign countries and the Convention on Cybercrime.

On the measure of production order, Chinese legislations such as Criminal Procedure Law[13], Nation Security Law[14] and People's Police Law[15] prescribe that the units and persons should truthfully provide evidence when the judge, prosecutor or police require the evidence. These provisions are similar to the related regulations in the Convention on Cybercrime[16].

2. Rules of adopting electronic evidence

On the aspect of rules on adopting electronic evidence, now there are no rules on adopting electronic evidence, the judges adopt the electronic evidence according to the common rules on evidence, only few new judicial interpretation by China Supreme People's Court prescribed the principle and rules on the legality of the electronic evidence, these interpretation play an important role in the cases of Cybercrime. Neither is there rule of probative force of electronic evidence, judges make free decision on the probative force of electronic evidence according to all related evidences. However, the rules on probative force of electronic data in other law field affect the Chinese judges to make their decision. For example, electronic data is usually saved, transferred, processed

---

11 See Article 3 of Interpretation on Judicial Problems of Criminal Investigation implemented by Criminal Investigative Units According to China Criminal Procedure Law.

12 See Article 5,56 of 2011 Draft Amendment of China Criminal Procedure Law and its interpretation.

13 See Article 45 of China Criminal Procedure Law.

14 See Article 18 of Nation Security Law.

15 See Article 34 of People's Police Law.

16 See Convention on Cybercrime of Council of Europe of 23.11.2001 (ETS No. 185), Article 18.

electronic data through some electronic equipments, if these equipments conform to the national or industry standard, that will help judges believe the strong probative force of electronic evidence.

Generally speaking, on the aspect of criminal procedure law, China criminal procedural legislations on electronic evidence develop slowly. In the cases of Cybercrime, the special regulations in the China criminal procedural law, administrative law and judicial interpretation play the similar role as the related procedural provisions in the Convention on Cybercrime, and in majority part they are already in harmonization with Convention on Cybercrime. But on the aspect of the force, operability and balance between controlling crime and protecting civil right, China criminal legislation still should be improved.

III. Provisions on jurisdiction and international cooperation

There are no special provisions on jurisdiction of Cybercrime in China Penal Code, for which Article 6 to Article 12 of China Penal Code are applied. If the place of the act or the consequence of Cybercrime is in China, China Penal Code should be applied. If Chinese outside of China commits Cybercrime and the highest penalty of the crime is less than 3 years, China Penal Code may not be applied. China legislation is in harmonization with the Article 22 of Convention on Cybercrime and Article 10 of Council of European Union Framework Decision mentioned above, which make sure that Cybercrime in China can be ruled absolutely. Now there is not agreement between China and foreign countries or international treaty that prescribed the handling mechanism on the Cybercrime cases in which more than one country have the jurisdictions.

On the aspect of judicial cooperation on Cybercrime, there is not special judicial cooperative mechanism between China and foreign countries or international organization. But in the special transnational Cybercrime cases, China criminal investigative authorities have cooperated with foreign criminal authorities in the field of criminal investigation and help, from 2004 to 2010 China criminal investigative authority help more 40 countries investigative authorities in more than 700 Cybercrime cases[17].

---

17 See general statements of Chinese delegation in the first meeting of the Intergovernmental Group of Experts of United Nations Crime Prevention and Criminal Justice Program in January, 2011.

C. Challenge of harmonization of criminal legislation against cybercrime and role of China

In the era of Internet, Cybercrime becomes the common threat of the world, because the technical base such as computer and Internet technique on which Cybercrime relied on is same for all the countries, so Cybercrimes in all countries have the same characteristics and trends. The common challenge makes the harmonization of the relevant criminal legislation of all countries necessary. Due to the work of CoE, CoEU and UN, some country's criminal legislation on Cybercrime began to harmonize, now legislation standard set by Framework Decision mentioned above becomes the basic standard which many country's legislations have already reached, Convention on Cybercrime represents the higher legislation standard, so the countries who reached the later standard are less. On the aspect of harmonization of criminal procedure law, even the countries who already ratified the convention, for example Germany, don't totally fulfill the obligation of transplanting the provisions in the convention to domestic law yet, it is almost sure that it will be much later for the ratified countries to build a transnational judicial cooperation programs that are strictly conformed to Convention on Cybercrime. Even in the scope of European community the progress of harmonization of criminal legislation against Cybercrime cannot be quick.

Convention on Cybercrime is an open international treaty, countries outside of Europe such as USA, Japan, Canada and South Africa also become its parties, so in the past, the present and the future CoE was, is and will still be the mover and one of the important leader in the progress of harmonization of criminal legislations of countries against Cybercrime. But CoE is a regional international organization and has limited effect on the countries outside of European, in addition, Convention on Cybercrime is only a response to Cybercrimes in the countries who participated in the drafting of the convention, and conditions and programs are hard to achieve after the convention became effective, therefore now the convention is effective to some European countries and USA[18], who is a ally of European countries. Those countries, which are outside of Europe and have not the relationship of ally with European countries, for example China and Russia etc., are not the parties of the convention. It means that CoE can not solely lead the progress of harmonization of criminal legislations against Cybercrime, need work together with worldwide international organization such as UN, to

[18] See PI Yong, Comparative Research on Measures of Collecting Evidence in the Convention on Cybercrime and China Criminal Procedure Law, China Legal Science, 2003. vol. 4.

push the far-reaching project of harmonization of criminal legislation and judicial cooperation system against Cybercrime.

China is in the common Internet world and faces the same challenge from Cybercrime, China has been amending the criminal legislation on Cybercrime with the change of China Internet society and Cybercrime. Now China Penal law on Cybercrime reaches and goes beyond the standard set by CoEU Framework Decision, and in most area reaches the requirement of standard set by Convention on Cybercrime. On the aspect of criminal procedure law, in recent years China has been pushing progress of legislation on collecting and adopting electronic evidence, now besides the measure of expedited preservation of stored electronic data, the legislation of other measure on collecting electronic evidence will soon reach the requirement of Convention on Cybercrime. On the aspect of jurisdiction and international cooperation, China did not reach any agreement with foreign countries on judicial cooperation of combating Cybercrime and did not join the related international treaty, that make China criminal judicial authorities face difficulties when they handle with transnational Cybercrime cases. China stands outside of the international judicial cooperation system on combating Cybercrime, it leads to a lot of transnational Cybercrimes move from other countries into China. The situation will not only do harm to safety of China network society but also make China the springboard to attack computer systems of foreign countries, because the key technique of Internet security is not in the hand of China, and it is forbidden to export to China by U.S and European countries, so China Internet system in fact is vulnerable and weak.

Cybercrime is the common challenge of world, it cannot be efficiently controlled unless the worldwide international judicial cooperation is built up, in which China, such a great Internet country, cannot be absent. China and International organizations especially UN and COE should communicate and cooperate more closely in the field of judicial cooperation against Cybercrime. Cybercrime is the challenge of the whole world, one of choices can be a more extensive new international treaty against Cybercrime, which is more than the scope of European countries and in the scope of United Nations, and based on the research of worldwide Cybercrime, especially reflects the status of Cybercrime of main Internet countries such as USA, European countries, China and Russia.

A STUDY OF INVESTIGATION SYSTEM IN THE REPUBLIC OF KOREA FOR AN EFFECTIVE RESPONSE TO CYBERCRIME

WONSANG LEE
Associate Research Fellow, Korean Institute of Criminology, Seoul, Republic of Korea

I. Introduction

The Republic of Korea ("Korea" herein after) is very well-known for its extensive broadband infrastructure. On the other hand, the development of security system of software is too slow of a pace for the advancement of hardware. This explains the reason that Korea had been an entry point of cyber-attacks. However, with its increasing presence on international stage, Korea now becomes one of a main target of cybercrime. According to "Global Internet Security Threat Report for 2009," released by Symantec Corporation (NASDAQ: SYMC), the largest maker of security software for computers, Korea ranked fourth in terms of vulnerability to cyber attacks (7%), following the U.S. (21%), Spain(11%), and China (8%). The most alarming fact is that the figure increased at a rapid pace from 2% in 2007 to 7% in 2008, while the U.S. and China only saw 2% increase and Spain 3% decrease during the same period. It implies Korea is overlooking the fact of the simplicity to become the victim of various kinds of cyber-attacks from around the world.

Table 1. Top countries/regions for government targeted attacks

2008	2007	Country	2008	2007
1	1	United States	21%	19%
2	2	Spain	11%	14%
3	6	China	8%	6%
4	13	Korea	7%	2%
5	3	France	7%	10%
6	4	Germany	7%	9%
7	5	Italy	6%	7%
8	6	United Kingdom	4%	4%
9	8	Canada	4%	3%
10	12	Taiwan	3%	2%

The biggest threat to Internet network in Korea is malicious computer codes attacks and distributed denial-of-service (DDoS) attack. Korea suffered a cyber-turmoil caused by 'the 7.7 massive DDoS attacks' which happened on July 7, 2009. The attack hit more than 115,000 IP addresses, which paralyzed all web sites of government agencies, financial institutions, media outlets, etc. Estimated damage was over 50 billion Korean currency. After the attack, government agencies drew up countermeasures against any possible attacks for the future. Nonetheless, according to an analysis of cyber attacks in Korea by AhnLab, antivirus software and security solutions provider, DDoS attacks top the list in terms of threat against network security with 35.4% in 2010. It is widely concerned that growing number of smart phones could be a new target of means of DDoS attacks.

As social network services like *Twitter* and *Facebook* have been rapidly increasing its number of the service users along with smart mobile phone users have increased. As a hardware platform, the paradigm of cybercrime is also changing by this phenomenon. To put it simple, cybercrimes maliciously take advantages of social networks such as easy access to the other networks and rapid dissemination of information results in increased number of loopholes of possible threat and victims. Social network and smart mobile phones become channels to spread malicious codes by disguising themselves as vaccines or false information. They are able to expose personal information or trace locations of others. The major problem is that all the activities on the internet are directly or indirectly related to possible crimes. Cybercrimes are more sophisticated and may pose greater threat than previous ones, meaning, the next DDoS attack may result in greater loss and victimization than the attack in 2009.

Earlier in the year, the Stuxnet computer worm proved that a computer virus can be used as a weapon to target real-world infrastructure such as industrial facilities. The world was shocked by the news that nuclear plants in Iran were attacked by Stuxnet. Fortunately, no case regarding Stuxnet attacks has been reported in Korea.

One of characteristics of cybercrime is that it does not dwell on specific borders. With the expansion of cyber space along with increased number of computer users, the entire world became a body threat against cybercrime. It is generally known that cybercrimes are almost impossible to deal within a country alone. This paper is an overview of the investigation system against cybercrime in Korea. Then it will suggest international cooperation strategies for a further effective investigation tactics.

II Current status of cybercrime in Korea

One of a useful index to learn about the current trends of cybercrime in the year 2010 is statistics published by Cyber Terror Response Center. The center classifies cybercrimes into two categories; 'Cyber Terror Type Crime' and 'General Cybercrime.' 'Cyber Terror Type Crime' defines attacks against the information network, for instance, hacking, mal-ware distribution, and Denial-of-Service attacks. On the other hand, 'General Cybercrime' refers to a crime that uses cyber space as a tool for committing crime, for example, Internet auction fraud or online child pornography distribution. It includes 'malicious and criminal activities' such as security intrusion, ID theft, file altering, data theft, spam mailing and DDoS attack. The most common general cybercrimes are auction fraud, piracy, service of illegal contents, defamation, ID theft, cyber stalking, cyber gambling, exchange of prohibited product, and so on. The table below shows trends of cybercrimes in Korea over 5 years. The table is made based on the classification of the Cyber Terror Response Center.

Table 2. Number of occurence of Cybercrime

Classification	Total	hacking-virus	Internet Fraud	cyber violence	illegal web site	illegal copies	Others
2006	70,545	15,979	26,711	9,436	7,322	2,284	8,813
2007	78,890	14,037	28,081	12,905	5,505	8,167	10,195
2008	122,227	16,953	29,290	13,819	8,056	32,084	22,025
2009	147,069	13,152	31,814	10,936	31,101	34,575	25,491
2010	103,809	14,874	35,104	8,638	8,611	17,885	18,697

Source: Cyber Terror Response Center

According to the statistics above, the total number of cybercrime has sharply increased and almost doubled over the past 5 years. The number of cyber terror type crime dropped in 2007 and 2009 while that of general cybercrime gradually went up.

In terms of the number of arrests, it is notable that since 2008, the number of offenders who were arrested for running illegal websites or violating copyrights has increased. Rapid increase in the number of arrests for selling illegal copies could be explained with lesser tolerance on infringement of copyright and massive law enforcement actions.

The trends in cybercrime have shifted. In the past, most of offenders were teenagers plus those in their 20's who are more accustomed to cyberspace than the older generation. With the continuing growth of the internet use, offender's age was also a factor to be observed since more 30's and 40's use internet as well. As a result, the ratio of them in cybercrime has gone up gradually.

Table 3. Age of offenders

Classification	Teenagers	in 20's	in 30's	over 40	Others
2006	13,4%	33,6%	29,5%	22,1%	1,4%
2007	15,1%	39,2%	26,3%	17,7%	1,7%
2008	26,6%	39,0%	21,8%	11,8%	0,8%
2009	19,4%	34%	29,6%	16,5%	0,5%
2010	19,5%	39,5%	25,4%	14,4%	1,2%

Source: Cyber Terror Response Center

III. Investigation system to respond to cybercrime in Korea

(1) Measures to handle cyber terror type crimes

Investigation system to deal with cybercrimes was established in 1996 when Korea Information Protection Center (currently Korea Information Security Agency, KISA), under the Ministry of Information and Communication and Korea Internet Security Center (KrCERT), was founded.

Year Classification	Total		Cyber Terror Type Crime		General Cybercrime	
	Occurence	Arrest	Occurence	Arrest	Occurence	Arrest
2006	82,186	70,545	20,186	15,979	62,000	54,566
2007	88,847	78,890	17,671	14,037	71,176	64,853
2008	136,819	122,227	20,077	16,953	116,742	105,274
2009	164,536	147,069	16,601	13,152	147,935	133,917
2010	122,902	103,809	18,287	14,874	104,615	88,935

KrCERT is a sub-branch of KISA. In 2001, Act on the Protection of Information and Communication Infrastructure was enacted. The purpose of the act is not only to protect key national information and communication infrastructures, but also to provide countermeasures against cy-

bercrime. After Korea experienced so-called '1.25 massive internet disruption' by worm virus in 2003, the Korean government took measures to prevent and respond to cybercrimes in the private, public and military sectors all together. Korea's response system to cybercrimes consists of KrCERT, which mainly deals with crimes in the private sector, National Cyber Security Center (the public sector) and Response Center to Information Warfare under the ministry of defense. In 2005, 'National Cyber Security Management Regulation' was brought to attention. It provided the grounds for setting up and administrating "National Cyber Security Strategy Meeting" and "National Cyber Security Center." In addition, National Cyber Security Management System and National Crisis and Disaster Management System were established and operated by National Cyber Security Center and the National Security Council respectively.

It is National Cyber Security Center (NCSC) that came up with both comprehensive and systematic measures that is able to respond to cybercrime at a national level. It also enhanced security of information and communication network by checking and identifying any problems or risks of network that each institution uses. Above all, it has a system that collects and analyzes information about inter-traffic, hacking, and efficiency of network. Another important role of NSCS is to monitor any risks 24/7 and protect them from attacks. To effectively respond to cyber attacks, NCSC introduced cyber threat warnings. Warning grades range from Green (normal), Blue (moderate), Yellow (substantial), Orange (severe) to Red (Critical). Furthermore, its activities include: keep attacks from spreading by conducting inspection to identify origin of the attack; support to restore damaged network as soon as possible; and prevent reoccurrence of attacks by performing safety inspection.

However, the current cyber attack response system in Korea has certain lack of efficiency due to it is diversity. For example, National Crisis & Disaster Management System being under control of the National Security Council (NSC), and National Cyber Security Management System being under the head of National Intelligence Service (Cyber Security Council), and Key Information and Communication Infrastructure Protection System being under the head of Office of the Prime Minister (head of Information and Communication Infrastructure Protection Committee). Given the fact that risks of cyber-attacks are increasing even as we speak, political discussion has been brought to attention over introducing 'National Cyber Security Assistant System,' which plays a role of control tower, and enacting 'Act on Cyber Crisis Management,' unifying laws and regulations related to cyber security.

(2) Organizational structure of cybercrime investigation agencies

It is required to examine the organizational structures of the Korean prosecution service and the Korean police in order to understand how cybercrime investigations are performed in Korea. The Cyber Terror Response Center (CTRC, also called NETAN) is the cyber investigative division of the Korean National Police Agency (KNPA), operated within the Agency's Investigation Bureau. Furthermore, a cybercrime investigation team is located at each local police station. However, most cybercrime investigation cases are conducted by the CTRC. The CTRC is divided into the Management & Cooperation Team and Investigation Strategy Team, the Investigation Team, the Research Team and the Technical Assistance Team. Besides the CTRC, cybercrime investigation teams and units, which are located under local police agencies or stations, are also in charge of investigating cybercrime.

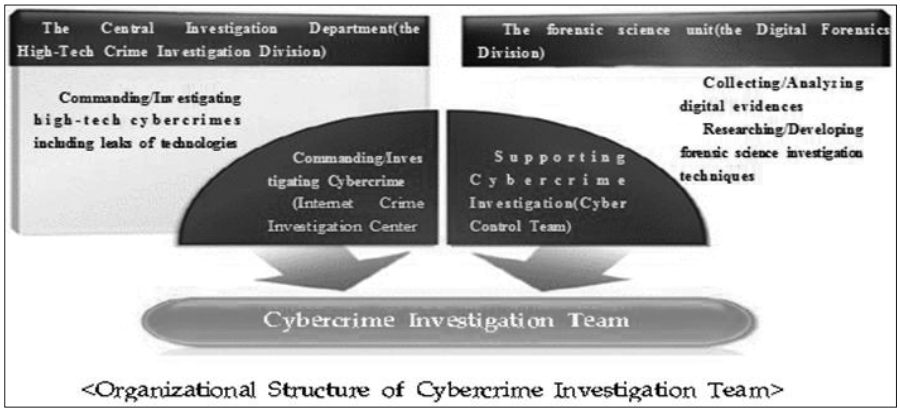
The Korean National Police Agency is currently operating an integrated cybercrime response system. The CTRC is taking a pivotal role and is linked to other cybercrime investigation departments installed in the 16 provincial police agencies and 236 local police agencies. With the experience of establishing and operating the cybercrime response system, the KNPA has strengthen its high-tech facilities including software for analyzing digital evidence to lead trends in technology and has been closely cooperating with public institutions, the private sector, research institutions as well as member states of the International Criminal Police Organization.

In case of the Korean prosecution service, cybercrime has been mostly handled by the Internet Crime Investigation Center, operated within the High-Tech Crime Division. Major duties of the center are, by large, researching trends in internet-based crime, receiving internet-based crime reports, developing investigation techniques, reforming legislation and policies, establishing cooperative investigation systems at the international level and etc.

The center has been focusing its resources to crackdown on cyber terrorism targeting national infrastructures related to telecommunication, energy and natural resources and e-commerce fraud, infringement of private information and distribution of unwholesome idea, which can directly impact of people's daily lives. The Center handles various Internet crimes, including hacking, virus distribution, privacy infringement, and unlawful information distribution. The center is making the utmost effort to develop new investigation techniques and countermeasures against crime on the Internet, and has built close networks with concerned private organizations and companies as well as national institu-

tions. The center also serves a contact point of the "24/7 Network for High Tech Crime," which has 48 member states including the U.S., the U.K., and Japan.

However, the Korean prosecution service realized that there is a need to build a system more specializing in cybercrime by centralizing the capacity of the prosecutorial service in order to respond effectively to cybercrime. There was also a call for establishing a division in charge of recruiting and training investigation agents specializing in information technology and representing the national investigation agencies to strengthen cooperative investigations promptly at international level. Due to these reasons, a division with more specialization in cybercrime investigation in the prosecution service, the High-Tech Crime Investigation Division in the Central Investigation Department, was founded.



<Organizational Structure of Cybercrime Investigation Team>

(3) Current status of cybercrime investigation

Korea has been generally successful in the fields of digital forensics and international cooperation for cybercrime investigation. Digital Forensics is of pivotal importance in cybercrime investigations. The importance of Digital Forensics was enhanced since digital information which is not just found in cybercrime is being considered as important evidence at in court proceedings. Due to this significance, the Digital Forensics Center (DFC) of the Public Prosecutor´s Office, the Cyber Terror Response Center (CTRC) of the National Police Agency, the National Scientific, Criminal & Investigation Laboratory (NCIL) of the Ministry of Public Administration and Security and others have all been conducting digital forensic related tasks in Korea.

The importance of Mobile Device Forensics has increased as the number of people using smartphones has skyrocketed. The National Police Agency's CTRC, has accumulated a vast amount of experience and knowledge. They have recently signed an MOU with the Netherlands Forensic Institute and both institutions have been cooperating closely in advancing Mobile Device Digital Forensics.

Furthermore, investigation agencies in Korea have dedicated great amount of effort to enhance international cooperation in investigating cybercrime as well. The Korean prosecution service recently conducted an investigation with other countries to investigate hacking that targeted the Korean National Agricultural Cooperative Federation. Due to a cooperative investigation, the Korean Prosecutorial Office found out that the hacking attempt originated from North Korea. Besides the cooperative investigations, Korea has been continuously pursuing cooperative investigations with individual nations at a bilateral level. The Prosecutor General of Korea visited China lately to discuss strengthening cooperative investigations between two nations in order to counteract cybercrime, especially targeting on voice-phishing. As a matter of fact, a large scale operation of voice phishing targeting Korean public was detected and arrested through a cooperative investigation between the two nations.

(4) Legal measures relative to cybercrime

Legal provisions that can be applied to prosecute cybercrime are stipulated in multiple acts of Korean law. "The Korean Penal Code" does criminalize some types of cybercrime, however the "Act on Promotion of Information and Communication Network Utilization and Information Protection, etc." serves as the fundamental law when for punishing cybercrime in Korea. The act was legislated with a view to improving the Korean people`s quality of life and public welfare by promoting the utilization of the information and communication networks and protecting personal information of people using information and communication services so that a wholesome environment for people using information and communication networks is ensured. In Korea's case, amending the Korean Penal Code is not an easy task, thus new types of cybercrime are regulated according to the specialized law from the aforementioned act. Traditional types of cybercrime such as computer fraud, computer sabotage, forgery and falsification of electronic data are regulated by the penal code, while new types of cybercrime such as distributing viruses, hacking, cyber stalking and cyber defamation are punished according to the act.

However, Korea has not yet signed 'the Convention on Cybercrime', which infers that Korea's existing laws related to cybercrime do not fully reflect the current trends of global cybercrime laws and legislations. Regarding child pornography issues, for instance, while the global standard against child pornography is getting tougher and tougher, Korea unfortunately has not met the global standards. Of course, this can be understood from the perspective that Korea has not had any big social problems generated by child pornography.

V. Perspective of cybercrime in Korea

Until now, the greatest occurrence of cybercrime in Korea is on portal websites in the forms of defamation, insult, infringement of copyright, hacking and etc. However, the number of Distributed Denial of Service attacks (DDoS) reported in Korea has increased since Korea became an easy target for hackers. Furthermore, the number of cybercrimes related to smartphones and social network services (SNS) has increased as the number of people using smartphones has surpassed over 20 million and social network services are getting extremely popular.

There are some hypothetical future trends of cybercrime in Korea. First, the various types of cyber attacks utilizing SNSs are likely to increase in numbers. SNSs started getting popular since 2010 and the number of people using SNSs rapidly increased in 2011. In 2012, however, cybercrime committed through SNSs is likely to be an extensive threat.

Second, DDoS attacks are expected to become more sophisticated. Since the massive 7.7 DDoS attack occurred in 2009, more sophisticated DDoS attacks than the 7.7 DDoS attack have been continuously reported. Fortunately, the damage from those sophisticated DDoS attacks has been relatively minor, but new types of attacks using mutated viruses combined with SNSs are likely to be observed in 2012.

Third, utilities or social infrastructure is expected to become the target of cyber attacks. In Korea, until today there has been no reported cyber attack targeting social infrastructure such as the 'Stuxnet' attack. However, since Korea has many atomic power plant sites and computerized social infrastructures, it is highly plausible those facilities can also be targets of cyber attack. In particular, considering the circumstance of confrontation between two Koreas, North Korea might attack social infrastructure of South Korea as a form of terror tactics.

Fourth, it is expected that there will be increased threat posed to smartphone users by hackers seeking financial gains. For instance, hackers might lure

smartphone users to download applications that can overcharge mobile phone bills or cause damage by ushering smartphone users to connect to phishing sites.

Fifth, there will be cyber attacks targeting wireless internet vulnerabilities. While the number of free Wireless Access Points (WAP) has expanded throughout Korea to provide better Wi-Fi service, those Wi-Fi Access Points might be prone to sniffing attacks. This is because the security of Wi-Fi access points is still unstable compared to wired internet access points.

Sixth, there will be threats caused by manipulating virtualization and cloud computing technologies. Establishing several command and control (C&C) servers by using virtualization and cloud computing technologies allow criminals to manage botnets efficiently and to hack cloud computing systems to use their resources.

Seventh, there will be increased numbers of targeted cyber attacks. Recently hacker groups such as "Anonymous" frequently attacked national institutions or organizations with a specific aim. In other cases, hacker groups committed cybercrime in order to make financial gains. In Korea, there have been many attacks by foreign hacker groups targeting online game servers located in Korea. Online games are very popular and the virtual items in those games are very often traded for large amounts. These types of targeted attacks, whether idealistically or financial motivated are set to continue. All in all, there will be more attacks seeking to achieve specific aims or to make profits in cyberspace.

VI. Efforts of the international community to respond to cybercrime

Based on experiences of Korea, some recommendations can be made to the international community in its efforts to respond to cybercrime. First, it is necessary for each nation to establish and define the investigation system designated to respond to cybercrime. In case of Korea, we first built an organizational structure designed to respond cybercrime. The established organizational structure is extensive that includes not only government agencies such as the National Intelligence Service, the prosecution service, the police and Korea Internet & Security Agency (KISA), but also the private sector; including internet companies and the like, and coordinating with the military. Hackers circumvent judicial institutions by possessing a technological edge in cyberspace. In this regard, unilateral investigations conducted by government investigation agencies without any support from the private sector are in essence very difficult. Moreover, cybercrime incidents can escalate to acts of cyber war in certain circumstances. Therefore, an extensive organization, which consists of the private and public sector as well as the military, is required to handle cybercrime issues properly.

Second, cybercrime is not confined by national borders. Therefore, cooperative investigations among countries are essential. Obviously, cooperative investigations at the multilateral level are required, but also strengthening cooperative investigations at the bilateral level is necessary to deal certain types of cybercrime; such as the case of voice-phishing in Korea and China. Furthermore, nations with a vast amount of experience and know-how in investigating cybercrime should support those nations that have yet to do so. A good example of this is the 'Virtual Forum against Cybercrime (VFAC)' managed by KIC with an aim to providing technical support to nations developing capacity to combat cybercrime. Through this forum, KIC has been trying to share cybercrime experts' knowledge in the theory and practice of preventing cybercrime with the participants of the forum.

Third, there is a need that domestic legal provisions related to cybercrime, including investigation rules and procedures, among countries be legislated and amended based on global standards. The "Council of Europe convention on cybercrime" has been already entered into force at European level and some other countries outside of Europe also ratified the convention. Furthermore, UNODC has been trying to establish a global cybercrime prevention convention. As a part of UNODC's endeavor, there was a expert group meeting held in January 2010 in Vienna. Every nation should support the UNODC in this matter, so that its efforts can be realized with the outcome of establishing a global cybercrime prevention convention. In addition, once the convention is implemented and ready to be signed by countries, countries should swiftly ratify the convention and enact or amend their domestic laws based on the convention.

Lastly, research on cybercrime should be conducted continuously. Information and Communication Technology (ICT) has progressed inexorably. Cybercrime has also been on the rise coinciding with the progress of the ICT. In this light, research on cybercrime must be conducted constantly. Until now, most cybercrime related researches have been focused on domestic issues; however, it is necessary to conduct research at a global scale by cooperating with other nations. Therefore, research institutions specialized in crime throughout the world should closely cooperate with each other to conduct cybercrime and digital forensics related research.

CYBERCRIMES IN IRAN: PERSPECTIVES, POLICIES AND LEGISLATIONS

BATOUL PAKZAD
Assistant Professor of Criminal Law and Criminology, Azad University, North Branch Tehran, Iran.

GHASSEM GHASSEMI
Assistant Professor of Criminal Law and Criminology Azad University, North Branch Tehran, Iran

Introduction

Computer and telecommunication technology has spread into nearly all areas of life including the administration of important social infrastructures. The same is true for computer-related crime.

In Iran information technology is being used in various part of social life and the government supports the expansion of this technology. One of the main goals of development programs in Iran is declared to be the development of electronic infrastructures and services and in Iran. In the meantime offences in cyberspace and abuses of this technology have increased during recent years. Some years ago the justice system was not able to combat and react to this problem effectively because of the lack of pertinent legislation. This in turn impeded the development of information technology in country. Therefore, the Parliament launched several legislative projects to fill the gap and some drafts of laws such as, electronic commerce, and cyber crime, were prepared which protect the emerging interests and values in cyberspace, values like, personal and private data and computer systems.

This paper intends to introduce policies and legislations which have been adopted by Iranian Parliament during the last decade, especially those related to the cyber crime. It discusses the cyber criminal law in Iran and focuses mainly on the Cyber Crime Act passed in 2009. This through and comprehensive illustration of cyber criminal law in Iran may be useful for comparative studies especially between Islamic and non-Islamic systems.

I. General overview of cybercrime background and its state of the art in Iran

1. *Historical background of cyber crime*

Theoretical physics research center was the first institution that used internet connection in Iran. It used internet connection through satellite in 1992. It started providing services to universities in 1993. In 1993 Iran joined the World Wide Web. To regulate the cyber state judiciary power established a committee for drafting the laws regarding Cyber Crimes in 2002 which was composed of legal and IT experts. This committee prepared the draft of the Cyber Crime Act (CCA) in 2004. Having been approved by the head of the judiciary with some modifications the draft was sent to the board of ministers and finally in July 2009 was passed by Parliament with some other modifications.

2. *Sources of inspiration of the Draft*

CCA is composed of 56 Articles and is divided into two main parts and one miscellaneous part; first part is on crimes and punishments and the second part is on prosecution of cyber crimes. To prepare the draft the committee conduct a comparative study on cyber crimes in different countries however, it is mainly inspired by European Convention on Cyber Crimes.

3. *Challenges:*

Since the rules and regulations referred to in the draft were mostly novel and unprecedented then, the committee had great difficulty with the explanation of the concepts to high rank judges and legislative bodies that had little knowledge of the cyber space and its nature. As a result, in many places committee had to simplify the draft and make it understandable for authorities which in turn led to some ambiguities.

Other challenge was related to definition of some concepts like obscenity and indecency was one of most challenging issues. The law obliges ISPs to filter and restrict user's access to obscene and indecent materials. The draft established no restriction based on Islamic morals. The restriction was only on pornographic content. However, later the parliament in article 22 established a committee to enlist the materials which should be restricted and filtered. This committee and the list of banned materials will be discussed in next parts.

4. *Policies, institutions and legislations*

The necessity for differentiated policy and practice in prevention and prosecution of different types of crimes has been acknowledged in

Iranian legal system in recent years. This is especially true in cyber space law. Evidently, cyber crimes may not be prosecuted like real crimes. This has led to the formation of new set of policies, laws and institutions in justice system which may be referred to as cyber justice. In this part first the policies regarding to cyber space are reviewed and then related laws and institutions will be discussed.

4.1 Policies; Guidelines for cyber space security

General policy Deed which defines the main guidelines of the country development for 20-year period and was introduced in 2003 the Supreme Leader, requires the governmental organs to secure the production and transmission of the data in cyber space (7^{th} part, General policy regarding computer information systems).

In line with the Deed, Fourth Development program in introduced in 2007, insists on the qualitative and quantitative improvement of computer information system and development of information society, e-commerce and instructs the necessary legislations for securing cyber space and confronting cyber organized crimes (such as guidelines for cyber space security). It also encourages the cooperation with regional and international institutions and unions of information and communication technology.

Fifth Development Program passed in 2010 requires the development of national information network, electronic state, etc…so as to provide 60% of Iranians with internet access by 2016.

This program instructs the development of IT in various sections like, administration of the state, economy, commerce, justice, national defense and security and etc.

Comprehensive Statute of security in production and exchanging data (AFTA) passed in 2009 declares that the Main goals of establishing information transfer system are as follows:

- Protecting the national and religious identity and human values of the society
- Respecting privacy and legal liberties
- Securing confidential documents and national integrity
- Securing vital infrastructures of the country against electronic attack
- Protecting material and intellectual properties
- Developing prevention system
- Collecting information relating to threats and attacks
- Eliminating threats and damages caused by attacks
- Combating crimes against security of information transfer

- Creating a system for confidential documents
- Creating related legal instruments
- Cyber Crimes

4.2 Institutions

4.2.1 Police

Cyber police is called FATA (Persian: Polis-e Faza-ye Towlid va Tabadol-e Ettela'at; Iran Cyber Police) belongs to NAJA (Niru-ye Entezami-ye Jomhuri-ye Eslami; Law Enforcement Force) and has provincial branches.

Iran Cyber Police has been set up in 2011 to fight phishing, forgery, internet theft, hacking, organized internet crime, pornography, and violation of privacy and to fulfill following aims in cyber space:

to secure and preserve order, defend religious and national identity, protect private sphere and legal liberties, protect national interests, secrets, and authority, secure the fundamental infrastructures against electronic attacks, maintenance of public peace.

Committee for determining the criminal contents

The Committee for Determining the Instances of Criminal Content[1], was establish by The Iranian Judicial Administration. It is located at the Office of the *State Prosecutor General. Members of this committee are ministers (or their representatives) of the Education,* Information and Communication Technology (ICT), intelligence, Justice, Science, Research and Technology, Culture and Islamic Guidance, the president of *the Islamic Propagation Organization, and the head of the Islamic Republic of Iran Broadcasting, the Commander*-in-*Chief of the Police, an expert in* information and communication technology chosen by the *Commission* of *Industries* and *Mines* of the *Iranian parliament and one of the members of the Legal and Judicial Commission* of the the *Islamic* Consultive Assembly chosen by the *Legal and Judicial Commission* and confirmed by the parliament. The *State Prosecutor General shall be the chairman of the committee* (Art 22).

[1] It is noteworthy of mention that there was no trace of the above committee in the bill approved by both judicial and executive branches and and submitted by them to the Parliament. It was inserted in the bill by the judicial commission of the parliament at the end of their internal debate.

The instances of criminal content determined by the above committee constitute a wide range of subjects.
However for the sake of brevity we only refer to five different titles under which the instances are categorized as follows:

- Obscene content which is against public morale and decency
- Content against Islamic sacrosanct
- Content against public peace and security
- Content against public and governmental institutions and authorities.

4.2.3 Prosecutorial Office

CCA requires the judiciary power to establish enough prosecutorial office all around Iran whose competence are solely prosecution of cybercrimes. Prosecutors and judges should have enough knowledge and skills in cyber space. At the moment there is only one special prosecutorial office for cyber crimes in Tehran. Since 2005 regular training courses and workshops have been held for judicial staff.

4.3 Legislations

Addressing these policies, Iranian Parliament passed following laws and regulations. These laws constitute computer and electronic legal system in Iran at the moment:

Audio-video Crimes Act in 2008
Protection of Software Copy Right Act in 2000
E-Commerce Act in 2003
Military criminal Act in 2003
Cyber Crimes Act in 2009
Free Access to Information Act 2007

These laws and regulations require their own modality of enforcement and hence professional law enforcement agencies. Iranian lawmakers recognizing this reality have established professional divisions within justice system for investigation and prosecution of cyber criminality. In following part these institutions are introduced.
Computer Crime Act (hereinafter refer to as CCA) adapted in 2009 is the most important enactments on cybercrimes. The law is consisted of 56 Articles divided into two main parts. The fist part deals with cybercrimes and punishments (substantive part) and the second part is concerned with criminal procedure of cyber crimes (procedural part). E commerce Act of 2007 (hereafter referred to as ECA) is another

important enactment in regard with cybercrimes which is out of the scope of this paper. In following parts first cybercrime and its categories will be introduced and then general rules governing the prosecution of cybercrimes will be discussed. At the end procedural rules governing the prosecution of cybercrimes in Iran will be reviewed.

II. The substantive law

According to CCA and ECA cybercrimes may be categorized into following seven types: Offences against the confidentiality of data and systems, Offences against the authenticity of data and system, Cyber terrorism, Offences related to the availability of data and systems, Computer related crimes, Accessory crimes, Ecommerce Crimes. Each of these types of crime is comprised of several criminal conducts to which special punishment is attached.

1. Crime and Its categories

In accordance and on the basis of the above mentioned laws cybercrimes can be categorized in seven groups.

1.1 Offences against the Confidentiality of Data and Systems

This group is sub divided into three different crimes:

1.1.1 Illegal accesses:
CCA defines this crime as any access, wholly or partially, to a computer or communication systems without right. It is committed by infringing security measures, (ART. 1 CCA.) The punishment is imprisonment from 91 days to 1 year, or fine from 5,000,000 to 20,000,000 Rials, or both.
In case the intention is gaining access to secret data, subject of Art. 3 of CCA then the offender will be punished by 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both.

1.1.2 Illegal interception:
Illegal interception is another crime against data confidentiality. It is defined as interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer

system including electromagnetic emissions from a computer system carrying such computer data. It is punished by a prison term of 6 months to 2 years, or by a fine of 10,000,000 to 40,000,000 Rials, or by both (ART. 2 CCA).

1.1.3 Espionage:

Cyber espionage, according to CCA, is a set of behaviors dealing with secret data which is transmitted by or stored at computer or telecommunication systems or data carriers. It includes following criminal behavior:

Violating security measures of computer and communication systems containing secret data. offender will be punished by 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both.(Art.4 CCA)

Gaining access to secret data, obtaining them or intercepting the secret content while in transmit ion. Punishment: 1 - 3 years of imprisonment, or a fine of 20,000,000 - 60,000,000 Rials, or both (Art.3.a ACC).

Providing access to the people, who lack legal competence, with the secret data. The criminal is Punishable with 2 to 10 years of imprisonment.(Art.3.bCCA)

Disclosure of or providing access to secret data for, foreign state, organization, company or group or their agents. Punishment of this crime is 5 to 15 years prison (Art.3.c CCA.).

Disclosing secret data, to those who lack any proper competence, out of carelessness, negligence or infringement of the security measures by officials trained to preserve the confidentiality of the data and are duty-bound to preserve the secrecy of data. Punishment of such a crime is 91 days to 2 years prison, or fine from 5,000,000 to 40,000,000 Rials, or both, in addition to a term of 6 months to 2 years during which the offender will be dismissed from governmental service (Art.5 CCA).

Note: Secret data is any data the disclosure of which disturbs national security or interests[2].

---

[2] In accordance with Art.3 (Note 2) the executive by-laws pertaining to the norms of determination and identification of the confidential data, and the method of classification and protection thereof shall be drafted by the Ministry of intelligence with the cooperation of ministries of Justice, Interior Affairs, Information and Communication Technology (ICT), and Defense, and approved by the Board of Ministers within 3 months from the date the present Act is ratified. However such by-laws are not as yet prepared.

1.2 Offences against the authenticity of data and system

This Category Consists of Two Crimes:

1.2.1 Computer related forgery

Computer-related forgery includes following behaviors:

a) Input or alteration of reliable data or fraudulent creation or input of such data,

b) Alteration of data or signals of memory or process able cards in computer or telecommunication systems or chipsets, or deceitful creation or import of data or their signals to them.

These forms of forgery are punishable by a term of 1 to 5 years of imprisonment, or by fine of 20,000,000 to 100,000,000 Rials, or by both (Art. 6-CCA).

1.2.2 Use of false data

However, knowingly uses the forged data, cards or chip, is punishable with punishment of forgery. (Art. 7- CCA)

1.3 Offences against the integrity of data and systems

This category is consisted of four forms of crime:

1.3.1 Data interference

This crime includes four behaviors, namely, deletion, destruction, disturbance of other's data or making them unprocessable without right. These crimes are punished by a term of 6 months to 2 years of imprisonment, or by fine from 10,000,000 to 40,000,000 Rials, or by the imprisonment and fine both (Art. 8CCA)

1.3.2 System interference:

This crime is composed of following behaviors without right:

Damaging or disturbing the functioning of computer or telecommunication systems by inputting, transmitting, distributing, deleting, interrupting, manipulating and deteriorating data or electromagnetic or optical emissions.

The relative punishment is 6 months to 2 years of imprisonment, or a fine of 10,000,000 - 40,000,000 Rials, or by both of them (Art. 9 CCA).

1.3.3 Cyber terrorism:

Generally, cyber terrorism is the use of internet based attacks in terrorist activities (cyber as target or means of crime), specifically it is actions against networks, data, information and computers via internet with political motives[3].

Art. 11 of CCA, though, dose not expressly mentioned the term "cyber terrorism ", is the relevant article addressing this crime in its strict sense by referring to any act of deletion, destruction , disturbance of other's data or making them unprocessable and Damaging or disturbing the functioning of or Denial of access to data or system:

Computer or communication systems that are necessary for delivering services such as, medical, water, electricity, gas, telecommunications, transportation, and banking services to the public, with the intention of disturbing public security and peace. This crime shall be punished by a term of 3 to 10 years of imprisonment.

1.4 Offences related to the availability of data and systems

This category consists of two different types of crime. The first type includes crimes whereby the principle of accessibility of data and system is violated by someone.

The second type, quiet in contrast of the first type, is committed where the data of which the accessibility is prohibited by law becomes accessible out of omission of a internet service provider.

1.4.1 Denial of access to data or system:

Denial of access to both data and systems, in its wide sense consists of any behavior which hinders or denies the access of an authorized user to data or system. Denial of access is the violation of the principle of accessibility of data and system which is one of the fundamental tenets of data and information security[4]. This crime is not addressed by a separate article at

---

[3] For further reading re: Sieber, Ulrich; Cyber terrorism- the use of the Internet for terrorist purposes; Council of Europe Publishing, 2007, and Brenner, Susan. W. and Goodman, Mark D; In defense of Cyber terrorism: An argument for anticipating cyber-attacks, Journal of law, technology and policy, 2002.

[4] The information security is founded upon three main pillars: Confidentiality, Integrity and Integrity, known as CIA model. These criteria are taken from D. Gollmann's suggesting as well as Information Technology Security valuation criteria)ITSEC).

See: Janczewski, Lech J and Colarik, Andrew M; Managerial guide for handling cyber – terrorism and information warfare, Idea group publishing, 2005, pp.2 – 3.

the EU cyber crime convention although at the said European convention the crime against availability is alluded to alongside the Offences against the confidentiality, integrity and availability of computer data and systems[5]. It has been addressed by Art.4 and 5 through the behavior of suppression of computer data. Which is a behavior that interferes with data or system? In the ACC there is a separate article dealing with the said offence. According to Art.10 of this Act:

"Every person who, without authority, denies authorized persons access to data, or computer or telecommunication system by actions including hiding data, changing passwords, and encrypting data shall be punished by a term of 91 days to 1 year of imprisonment, or by fine from 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine."

1.4.2 Failing to prevent access to criminal content

This crime happens mostly by Internet service providers (access or hosting). Providers have to filter any content which have been declared as criminal by the committee set up for to this purpose (committee of determining the instances of criminal content) , including criminal content or content which is used for committing computer crime. If a service provider fails, deliberately, to filter such content he will be banned to continue their work. If they fail,out of negligence or recklessness to filter they will be fined for the first and second times and to a business closure of one to three years at the third time.(Art.21&23 CCA)

Service providers should block the access to criminal content as soon as they receive the pertinent order of the committee established to define criminal contents, intentional failure will lead to their ban from this profession. Furthermore negligent failure makes them punishable by fine.

1.4.3 Illegal use of bandwidth

State has the exclusive right to use the international bandwidth for telecommunication. Whoever uses this band without prior permission for telecommunications from Iran to abroad or vise versa is criminal and punishable with 1 to 3 years of imprisonment, or by fine from 100,000,000 to 1,000,000,000 Rials, or by both of them (Art.24 CCA).

---

5 The EU cyber crime convention, Section 1 - *Title* 1.

1.5 Computer-related Crimes

These offences are related to a number of behaviors whereby the computer or internet is used as means of committing traditional crime. In a wide sense:" computer-related crime not only comprises attacks against new computer-specific interests, such as the aforementioned crimes against the confidentiality, integrity and availability of computer systems, it also includes attacks against traditional interests committed by new, computer-specific means"[6].

In the CCA crimes of theft and fraud are only addressed under the title of computer related crimes. However, chapters four and five of the Act deal with offences such as offences against public decency and morals, libel and defamation wherein the computer or telecommunication systems are the tool by which the crime is committed.

Here we shall focus only on those crimes addressed by the CCA.

1.5.1 Cyber fraud

This crime covers a wide range of financial misuses in cyber space meaning obtaining property or financial privileges through misuse of data or computer systems. Behaviors like, creation, deletion, alteration of data and disturbance in computer systems.

Cyber fraud is to be punished by 1 to 5 years of imprisonment, or fine of 20,000,000 to 100,000,000 Rials, or both of them , in addition to restitution of the property (Art. 13 CCA).

1.5.2 Computer-related theft:

This crime occurs where other's data is stolen whether or not the original data remain there. In case where the data is completely taken away the punishment will be harsher. Punishment of this crime is for the first time, fine from 1,000,000 to 20,000,000 Rails and for the second time, 91 days to 1 year of imprisonment, or fine from 5,000,000 to 20,000,000 Rails, or by both of them (Art. 12 CCA).

1.5.3 Offences against public decency and morals:

They include three types of crimes that are committed by means of computer or telecommunication systems or data carriers:

---

6 Organized Crime In Europe: The Threat Of Cybercrime; Situation Report 2004, Octopus Program, Council Of Europe Publishing, 2005, pp.114- 86. For further references see: Sieber, U. (1992), *The international emergence of criminal information law*, Cologne, Berlin, Bonn and Munich.

a) Dissemination, distribution or exchanging pornographic contents and production or preservation of such contents, with the intention of financial gain or corruption of public moral.

Pornographic contents in CCA are divided into two types: content which is gravely obscene[7] and the content which is indecent[8].

The punishment for the first type is 91 days to 2 years of imprisonment, or fine from 5,000,000 to 40,000,000 Rials, or both of them. For the second type of crimes the punishment is the minimum amount of one of the above punishments.

Legislature has aggravated the punishment of these crimes under special circumstances. In the case that the offender has made the acts in his routine occupation or commits them in an organized way, if not being found guilty of corruption on earth (punishable with death penalty), he shall be punished by the maximum amount of the both punishments.

In departure from the norms of the EU convention[9], at the CCA there is no distinction between pornographic content relating to adults and those relating to children[10].

b) Encouragement, provoking, threatening, or convincing and deceiving people to access pornographic contents ,or facilitating or training the methods of gaining access to them,

Punishment for the content which is gravely obscene is to be 91 days to 1 year of imprisonment or fine from 5,000,000 to 20,000,000 Rials, or by both of them and for the content which is indecent is fine from 2,000,000 to 5,000,000 Rials (Art.15.a CCA).

c) If someone encourages, provokes, facilitates, invites or threatens others to commit crime against decency, abuse drugs, or commit suicide or sexual deviations or violent crimes. facilitating orTraining others for committing such crimes is also punishable by a term of 91 days to 1 year of imprisonment, or by fine from 5,000,000 to 20,000,000 Rials, or by both them (Art.15.b ACC)

---

7 Refers to real or unreal image, audio, or text, or a text indicating the whole nakedness [nudity] of a man or woman, or sexual intercourse.

8 Refers to those materials which contain lewd scenes and images.

9 Art.9 of The EU cyber crime convention

10 At the bill submitted to the parliament the distinction was there, with a harsher punishment for child pornography. But the ACC deals with child pornography at the same footing as the adult pornography.

1.5.4 Offences against dignity

These crimes includes following behaviors:

a) Fabricating, distorting or alteringthe video, voice, or picture of a person and its distribution, by means of computer or telecommunication systems, in a way that offends that person. These forms of crime are punishable by a term of 91 days to 2 years of imprisonment, or by fine from 5,000,000 to 40,000,000 Rials, or by both.
In case the alteration or distortion is in a pornographic manner, the offender shall be punished by the maximum amount of the both provided punishments (Art.16 CCA).

b) Distributing or making available voice, picture, private or family video, or others' secrets of another person without permission in a way that it disturb their dignity or causes loss, unless law provides so. Punishment of this crime is the same as the punishment of the crime mentioned in number one (Art.17CCA)

c) Disseminating of false news through computer and telecommunication systems, with the intention to harm others or disturb public peace, whether it cause such harm or not. This crime has also the same punishment imposed to the perpetrator of the crime mentioned in number one, in addition to re- instating the dignity of the victim, if possible (Art.18CCA).

1.6 Accessory crimes

This group of crimes consists of behaviors which are actually preparatory to other cybercrimes or they are considered as contributory for committing those crimes. CCA recognizes three categories of such behaviors as crime and their punishment is a term of 91 days to one year of imprisonment, or fine from 5,000,000 to 20,000,000 Rials, or both.
In the event that the offender has made the below acts as his routine occupation, he shall be punished by the maximum amount of both punishments (Art.25 CCA).
The production, distribution , making accessible, or trading data, software, malware or any other electronic devices, which are exclusively used to commit computer crimes;
Distribution or making accessible of the training materials and contents that showing how to commit cybercrimes includes cyber espionage, data or system interference , illegal access or interception.

Sale and distribution of passwords or providing access to them or any data that provides unauthorized people with the access to data or computer or telecommunication systems belonging to others;

1.7 E-Commerce crimes

The crimes pertaining to E-commerce or electronic financial exchanges are dealt with in ECA of 2003. Some crimes such as forgery and fraud are replaced by the provision of the CCA. They are categorized, on the base of violated values and interests, into two main groups; crimes violating rights related to data message and crimes violating individual rights.

1.7.1 Crimes violating the declared rights of author related to data message,

This crime encompasses two types of crimes:

1.7.1.1 Crimes violating intellectual property rights

According to Art.74 of ECA, violation of intellectual property rights, works and computer software by copying, offering and dissemination in electronic exchange procedure is a crime and will be punished by a term of 3 months to one year imprisonment and fine of 50 million Rials.

The legal protection covers not only intellectual property rights of the author, previously known as incidental intellectual property rights, but also covers the right of people rather than the authors, such as the actors and the producer of audio–visual Disks and those of recording and distribution companies.

1.7.1.2 Crimes against commercial secretes and signs

In order to protect fair and legitimate competitions in the field of electronic exchanges, to get held of trade and economic secrets of entities and companies for own benefit or disclosed to third party, electronically, is considered as a crime and the perpetrator shall get a prison sentence of six months to two and half years and fine of 50 million Rials (Art.75 ECA).

It is unlawful to use trade marks as a domain name or any online display of trade mark which causes deceive or makes a party mistake about originality of a commodity or a service. The wrongdoer shall get a prison sentence from one to three years and a fine from 20 to 100 million Rials (Art.76 ECA).

1.7.2 Crimes violating individual rights

This category may also be divided into two distinct groups of crime:

1.7.2.1 Violating consumer rights

Aiming to protect the consumer in the field of electronic exchanges the E-Commerce Act has envisaged a number of duties for sellers and service providers (Arts 33-43) the violation of which in some cases, including the following cases, will carry penal sanction of fine from 10

million to 50 million Rials (Art.69ECA).
Failing to deliver effective information,
Violating laws in giving information,
Right to canceling the deal ,
Failing to return the money to consumer;

1.7.2.2 False commercial advertisement

Those providing the advertisement of commodities and services must carry out the advertisement in such away that the consumer can get, correctly and clearly, the information pertaining the commodity, the service and the identity of person or the entity for whose benefit the advertisement is made.

According to Art.70 of the e-commerce Act, any act or omission violating advertisement rules, such as;

Fraudulent advertisement;
Unhealthy advertisement;
Ambiguous advertisement;
Anonymous advertisement;
Hiding the identity or brand.

Is a crime and subject to fine from 20 million to 100 million Rials (Art.70 ECA).

1.7.2.3 Violating the protection of personal data

Saving, processing, and /or disseminating personal data message relating to ethnic or racial origins, ideological and religious view point, moral particulars and data messages relating to physical, moral or sexual condition of people without their explicit consent in whatever manner is unlawful and a crime. Furthermore in case of explicit consent, too, any saving, processing, and /or disseminating personal data message in the field of electronic exchanges shall be subject to the provisions of the law. Any conduct contrary to those legal provisions, is a crime and according to Art.71 ECA is punishable by a one to three years imprisonment.

General Rules

Cybercrimes covered by the Iranian penal law are mostly deliberate crimes unintentional, careless or reckless behaviors are consider as crime only exceptionally. Attempt in cybercrimes is not considered as crime and is not punishable.

Only with regard to aggravating circumstances and legal persons' penal liability special rules are provided for, which will be discussed in following parts.

2.1 Aggravating and mitigating circumstances

In following instances punishment is aggravated, as the case may be, the offender shall be punished by more than two third of the maximum amount of one or both the punishments (Art.26CCA):

When crime is committed in an organized way

When crime is committed widely

When the perpetrator is an state or public employees or staff and commits the crime through misusing his position

Perpetrator possesses or manages legal computer or communication system and commits crime by abusing this position

When data or computer and telecommunication system belongs to the state or public institutions or centers providing public services.

It is to be noted that in addition to the above mentioned special aggravating circumstances in case of recidivism in a cyber crime the punishment will be heavier as well.

If criminal commits crime for more than two times the judge may deprive the criminal from pubic electronic services such as, internet access, cell phone subscription, obtaining domain name registrations in national (or country code) Top-Level Domain, and electronic banking. Depending on the extent of the punishment for the original crime, the length of the period of deprivation from such rights is from 1 month to 5 years (Art 27cca).

Despite setting special rules concerning aggravating the punishment no special mitigating circumstances is prescribed for cybercrimes. Their punishment may be mitigated based on general criminal code.

2.2 Corporate liability

In cyber crime Act the criminal responsibility of legal entities is established for the first time (Art.19 CCA) when:

- The crime is committed by the name of legal entity;
- The crime is committed for the benefit of legal entity;
- Crime is committed by the" director"[11] of the legal entity or the director orders the computer crime and the crime has been committed

[11] The term "Director" refers to the person who has the authority of representativeness, decision making, or supervision of the legal entity.

or any of the employees of the legal entity commits the computer crime with the director's awareness or due to his lack of supervision;

The activities of the legal entity are entirely or partly allocated to computer crime.

We have to mention that the criminal liability of the legal person shall not exempt the offender from punishment, and in case of lack of terms and conditions provided in the proceeding, or impossibility of attributing the crime to the legal entity, the sole real person shall be regarded responsible.

2.3 Criminal responses and sentences

Since the excusing and justifying circumstances and factors are not specifically addressed in the CCA, the general penal rules are applicable to the case of cybercrimes.

The main punishments for cybercrimes are imprisonment and fines. Prison sentence is imposed between minimum 91 days and Maximum 15 years and fine is fixed between 5.000.000 and 100.000.000 Rials.

The amounts of fines provided in the CCA are to be changed every three years, based on the official annual inflation rate declared by Central Bank, with the suggestion of the chief justice, and ratification of the Board of Ministers.

It can be seen, also that due to the anti-imprisonment approach, at the time of drafting the CCA, in most cases, along with the prison sentences, a monetary fine is set as an alternative and the judge can choose each of those two sentences. In most of the crimes two sentences of imprisonment and fine is imposed and the court may choose one of them. All kinds of punishments may be suspended and prisoners may be released early on parole.

Procedural law

In dealing with cybercrime, the traditional rules of penal procedural law are facing fundamental challenges. Therefore, part 2 of CCA, under the title of "Procedural Rules" has adopted special rules with regard to cybercrimes and any crime and in which electronically evidence is relied upon. In this section some important points of procedure, briefly under two general titles of jurisdiction and electronically evidence, will be addressed.

3.1 Criminal jurisdiction

Cybercrimes know no boarder and determining the place where the crime is committed is one of the main challenges of criminal jurisdiction in cyber space. Second section of the convention on cybercrimes defines the general principles on jurisdiction of state parties. However, this convention introduces the traditional forms of jurisdiction and creates no special form of jurisdiction in cyber space. In ACC, in addition to conventional forms of jurisdiction, legislator recognizes new forms of criminal jurisdiction in cyber space.

It has thus extended the criminal jurisdiction. When a cybercrime is committed via abuse of a child under 18 years old, the perpetrator may be prosecuted in Iran whether the child has Iranian nationality of not. Other special forms of jurisdictions are as follows:

Criminal data or data used in committing crimes is anyhow stored in computer or telecommunication systems or data carries existing in Islamic Republic of Iran's land, air, and maritime territory;

The crime is committed by means of the websites with national Top-Level Domains of Iran;

The crime is committed by any Iranian or non-Iranian person, outside Iran's borders, against computer or telecommunication systems, and websites used by or under control of the three branches of the government, Supreme Leader office, official governmental agents, or any institution or entity providing public services, or against websites with national *Top-Level domains of Iran* (Art. 28. ACC).

In spite of the existence of the above mentioned provisions, it seems that there are challenges in following areas.

On the basis of the rules of territorial jurisdiction, to determine the locus of commission of crime, recourse is made to the doctrine of ubiquity. If one of the elements of the crime or its final effect is situated inside the borders of a country, that jurisdiction is comer tent to decide the related case. However, in cyber crimes, on the one hand to determine the locus of the crime or the occurrence of the effect is not always easily possible (the prescribed criteria are not sufficient for determining the locus of the cybercrime and recognizing the physical place of a source or internet users is often impossible. In the other hand, the elements and the effect of a crime might take place in more than one country and this leads to positive conflicts. The most

important issue therefore is the application of the rule of prohibition of double trial.

Another legal lacuna is jurisdiction over crimes of legal entities; criminal jurisdiction over cybercrimes committed by legal persons is not clearly determined by laws.

3.2 Collection of e-evidence

The information technology, not only is challenging the penal jurisdiction through eliminating physical borders, but it has set a new chapter in the evidentiary system, whereby to acknowledge there unique characteristics requires new rule and measures.

3.2.1 Maintaining data

Maintenance of computer is an important tool for pursuing cyber crimes. These crimes are often committed through computer and communication networks. This communication might include criminal content such as pornography, computer viruses, malwares or evidence of commission of other crimes. Furthered, to find out the origin and the destination of these information and communications might help to identify the wrong doers. For the purpose of having access to E-Evidence, on the one hand there is a duty upon internet service providers and on the other hand, for immediate protection of saved computer data and their supply legal provision are set as follows:

3.2.1.1 Data retention

The Access service providers are obligated to retain "the traffic data" at least until 6 month after the creation. They must preserver" the users' information" at least 6 months after termination of the subscription (Art.32 CCA).

The domestic host service providers have to retain their users' information at least until 6 months, and preserve stored content and traffic data resulted from the occurred changes at least until 15 days (Art.33cca).

3.2.1.2 Expedited preservation of stored computer data

Whenever the preservation of stored computer data is necessary for criminal prosecution and trial, the judicial authority is empowered to issue the protection order addressed to any person who has control or possession over them. When the data is at risk law enforcement officers are empowered to issue the protection order, and ask for judicial authorization within 24 hours. The data should be preserved up to

maximum 3 months. For longer preservation judicial order is needed (Art.34CCA). Reservation of data does not mean that they are disclosed to the public.

3.2.1.3 Production of data order

The judicial authority may order the production of data which is retained or preserved in order to be delivered to law enforcement officers (Art.35 CCA).

In the case of violation of the above orders or disclosure of the preserved data, or informing the persons to whom the aforesaid data is concerned of such preservation, the perpetrator is punishable.

3.2.2 Data and computer systems' search and seizure

The conventional criminal procedure does not address Search and seizure of computer system and data, this and special requirements of prosecution of crime in cyber space, such as necessity of rapid Search, let to enactment of a new procedural regulation for cyber space.

Where as in the search and seizure of data and computer system .there is a need for speedy and expeditious action so as the crime evidence is not destroyed and on the other hand the said measure must be taken such a way that the harm to the privacy and interests of people be kept to a minimum, therefore, precise and accurate provisions are necessary in this regard. In the CCA attempt is made to secure the balance between those two concerns.

It can be seen that a part from prescribing special condition and methods for search and seizure, special provisions are adopted for the protection of personal rights as follow:

- In cases in which during the implementation of search and seizure order, the search of data, related to the crime committed, in other computer or communication system which are under the control or possession of the accused becomes necessary , the law officers can not extend their search and seizure to the said systems without judicial warrant (Art.43 CCA).
- Seizure of data or communication or computer system is prohibited where it leads to physical injury, or financial damages to individuals or disruption in the provision of public services (Art-44 CCA).
- Also article 45 provides for the conditional right of the beneficiary to get a copy of the original data which is seized.
- Article 46 is about the judges' duty to determine the fate of the data or computer and communication systems (art 46).

- Finally the party affected by the seizure of data and systems have the right of objection which can be submitted to the relevant judicial forum as provided for in art-47.

3.2.2.1 Conditions and requirements of search and seizure

Search and seizure of data or computer and communication systems is ordered by judicial authority and this order is given when there is a reasonable doubt that they contain criminal evidences or may help to discovering the crime, or identifying the criminal or crime evidences. The search and seizure should be performed at the presence of the legal possessors or persons, anyhow, have them under their control, including system operators. Otherwise, the judge shall issue the order of search and seizure without the presence of the mentioned persons

The search and seizure order must contain the information which aids the accurate execution thereof, including order execution in/out of the location, the qualifications and scopes of search and seizure, type and extent of the considered data, type and number of the hardware and software, the method of accessing the encrypted or deleted data, and the approximate time needed for accomplishment of search and seizure (Arts.36-38 CCA).

3.2.2.2 Methods of search and seizure

Data or computer and telecommunication systems' search includes the gaining access to computer and telecommunication systems, in whole or in part; to data carriers including diskettes, compact discs, or memory discs; and to encrypted or deleted data (Art.39CCA).

Methods of seizure systems or data are different. Seizure of the computer or telecommunication system is made through changing the password or forfeiting the system in place. Seizure is performed proportionately considering their type, importance, and role in committing crime. In any of the following cases, the computer or telecommunication systems shall be seized:

- The stored data is not conveniently accessible, or is a large volume one (there is a large amount of data);
- Search and analysis of data is not possible without having access to hardware system;
- The legal possessor of data has given his/her consent;
- Copying data is not technically possible;
- In-place search causes damage to data (Arts.41-42 CCA).

Seizure of data is made through data printing, copying, imaging, and making data inaccessible by means of techniques including changing passwords or encoding or encryption them and confiscation of data carriers are practiced (Art.40 CCA).

3.3 Attributability of e-evidences

One of the challenges faced by penal law is the admission of computer data as a proof of crime. In those systems, which are based on the method of intellectual (or subjective) evidence there is less difficulty and the problem is related to the process of reliability of E-Evidence.

Due to the wide discretion of the judge in evaluation of evidence it seems that in Islamic penal law the subjective method of evidence is the prevailing one[12].

In Iranian penal law although for proof of crimes falling under the title Hodud (the limits) Qissas (retaliation) special evidence is required , in judicial by-laws and directives it is emphasized that even in this sort of crimes the judge's own knowledge and conviction is very important and instrumental in attributing the crime[13]. Therefore, in criminal proceedings it is advisable to utilize scientific methods and tools of crime discovery brought about by human knowledge[14].

For the purpose of reliability and admission of E-Evidence, Iranian law, includes special rules which will be dealt with in following section.

3.3.1 Admissibility of data

In Iran legal system, electronic data have the same power of proof as the paper data. They are deemed as paper deeds and E signature is deemed as a paper signature. For the first time, reliability of E-Evidence was recognized by ECA.

By virtue of article 12 of ECA, evidence can be in the form of data-message and its probative value can not be denied by any court of law or governmental office. Furthermore, in accordance with article 7 of the CCA, the electronic signature is as valid as a hand written signature. On the basis of the CCA, a data- message is as valid as a written document saved for the followings:

- Ownership deed of immovable property
- The sale of medicines to end-users

---

12 Husseini Nejad, Husseingholi, Evidence Law, p. 13

13 Akhundi, Mahmoud, Criminal Procedure Law, P. 85

14 Judicial Directive issued by High Judicial Council, No. 1363/12/6-1/56313.

The warning or notices containing special orders for the use of some items or precluding certain methods of their use (art. 6 .ECA.)
Section 3 of CCA is about admissibility and reliability of E-Evidence where by Art. 50 expressly provides:

"In the event that the computer data is created, processed, stored, or transferred by the party to the suit or the third party unaware of (the existence of) the suit, while the relevant computer or telecommunication system operates so properly that the validity, integrity, reliability, Non-

Repudiation *of data are not affected, (the data) shall be admissible."*
The law concerning the fifth program of five-yearly-development of Islamic republic of Iran admits, an E-document as a paper document provided that its authenticity and integrity are established (Art.48).

Legal requirements for accepting e-evidences

For the purpose of reliability and admissibility, an E-Evidence must possess the realities integrity, reliability and non – repudiation.

The E-Evidences are vulnerable because of their nature. Therefore, they carry the risk of being damaged or destroyed while they are being collected. Consequently there must be caution in saving, depositing, collecting, preserving and evaluating these kinds of evidences. In documentation a series of measures are taken in order to show the attributability of the crime to the accused and to prevent any damage or alteration while the E-Evidence is at the disposal of the law office or other authorities. Therefore, the chain of protection of data must be envisaged in the rules and be observed by the officials.

Generally, the probative value of E-Evidence is determined with due regard to security measures, including the proportionality of the methods in relation to the case at hand. Art.49 of the CCA provides:

"For the purpose of protection of accuracy, integrity, reliability, Non-Repudiation of the collected digital evidence, collected E-evidences should be protected and preserved pursuant to the relevant executive by-laws".

Also, Art.54 of the said act requires that the by-law concerning the collection and admissibility of E-Evidence, has to be prepared by the justice ministry and be signed by the head of judiciary. The by-law is prepared, but it is yet to be signed by the head of judiciary.

Conclusion

Criminal justice has made some important progress in tackling cybercrimes in Iran. Legislator has addressed regulatory needs of cyberspace both in general policies and ordinary legislations, most important of which is Cyber Crime Act passed in 2009. Electronic Commerce Act is another important enactment. However, the legal infrastructures of cyberspace are still in progress in Iran and several projects are being conducted under the supervision of FAVA.

Cyber Crime Act is inspired mainly by Cyber Crime Convention of European Council 2001. Notwithstanding, criminal laws related to the criminal contents are based upon Islamic criminal laws. The Act has listed main cybercrimes and provided differentiated and special criminal procedure for prosecution of these crimes. The law has also established special criminal justice institutions such as cyber police, cyber prosecutorial office and courts for cyber crimes. However, in spite of all these progresses there are still some deficiencies which need to be addressed in future. Some of these deficiencies are as follows:

- Some forms of harmful conducts are not criminalized, conducts like: identity theft, spam and cyber money laundering…
- Vagueness in cyber evidence rules and investigation procedures,
- Unclear rules of jurisdiction,
- Some deficiencies in amputability of the evidences and documentation of electronic evidences,
- Cyber Crime Act has delegated the power of law making to state in some respects for which the Parliament is the only competent authority according to the Constitution.

The lack of a system for international cooperation in combating cyber crimes, this problem is not however special to this Act. In international level the question of cooperation in cyber criminality is also a challenging matter and remains on United Nation and other international organizations to set up a global system for preventing and combating this form of criminality.

References:

Akhundi, Mahmoud, Criminal Procedure Law, Second Volume, Islamic Propagation and Guidance Ministry, Fifth Edition, 1998 (In Faesi).

Alipour, Hassan, Criminal Law of Information Technology, Khorsandi Publication, 2009, Iran (InFarsi).

Brenner, Susan W, Cybercrime, Cyber terrorism and Cyber Warfare, International Review of Penal Law: Cybercrime, AIDP, Volume 77, 2006

Brenner, Susan, Toward a Criminal Law for Cyberspace: Distributed Security, University of Dayton School of Law, at: *http://law.bepress.com/expresso/eps*

Council of Europe, Organised Crime In Europe: The Threat Of Cybercrime; Situation Report 2004, Octopus Program, Council Of Europe Publishing, 2005, pp.114- 86

Ghanad, Fatemeh, Criminal Matters in E-Commerce, PhD Dissertation, Shahid Beheshti University, Faculty of Law, 2005, Iran (In Farsi).

Ghassem, Ghassemi, Pending Book, Criminal Sentencing in Iran after Revolution of 1978, A Comparative Study of Sentencing in Iran and Germany", Max Plank Institute for Foreign and International Criminal Law, Freiburg im Br., Germany.

Husseini Nejad, Husseingholi, Evidence Law, Daneshnegar Publication, Second Edition, 2002 (IN Farsi).

Janczewski, Lech J and Colarik, Andrew M; Managerial guide for handling cyber – terrorism and information warfare, Idea group publishing, 2005,

Pakzad, Batoul, Cyber Terrorism; A Threat against National Security, Azad University, Science Development Office, 2010 (In Farsi).

Research Center of Islamic Consultative Assembly (Parliament), Communication and new Technology Office, Evaluation of Internet Users Condition in Iran and the World, Research Center of Islamic Consultative Assembly (Parliament), No, P 53, 2006.

Sieber,Ulrich, Cyber terrorism- the Use of the Internet for Terrorist Purposes; Council of Europe Publishing, 2007

Sieber, U. (1992), The International Emergence of Criminal Information Law, Cologne, Berlin, Bonn and Munich.

Documents:

Convention on Cybercrime, Budapest, 23 November 2001. On the website of the Council of Europe

Part IV

NEW NATIONAL AND INTERNATIONAL LEGAL RESPONSES TO CYBERCRIME

THE BUDAPEST CONVENTION 10 YEARS ON: LESSONS LEARNT

ALEXANDER SEGER
Secretary Cybercrime Convention Committee, Head of Data Protection and Cybercrime Division, Council of Europe, Strasbourg, France

The 10th anniversary of the Budapest Convention on Cybercrime was the focus of the Council of Europe's annual Octopus Conference on Cooperation against Cybercrime in Strasbourg from 21 to 23 November 2011[1].

The presentations and debates during that event and the lessons learnt since this treaty was opened for signature in Budapest on 23 November 2001 provide valuable insights not only with respect to the functioning of this specific Convention, but with regard to international cooperation against cybercrime in general.

Having been involved in the promotion and implementation of this treaty from 2002 onwards, I am offering here my views on what the Budapest Convention is all about, on key achievements ten years on, on lessons learnt and on the need to weave a web of responses to challenges on the web[2].

About the Budapest Convention

The Budapest Convention basically requires state parties to this treaty to do the following:

To establish specific types of conduct as criminal offences in domestic legislation. This includes offences against computer data and systems, that is, the so-called offences against the "confidentiality, integrity and availability" of computers, such as illegal access, data and system interference and others. In addition to these "c-i-a" offences, it includes offences by means of computers. However, as any crime these days may involve computer systems, the Budapest Convention focuses on the criminalization of specific conduct that acquires a new quality or scope when committed through computers. Thus, it stipulates

1 For presentations, videos and other materials see *www.coe.octopus*

2 As an interested party, I do not claim my views to be "scientific".

the criminalization of computer-related forgery and fraud, of child pornography and of intellectual property related offences.

To provide criminal justice authorities with effective means for investigations through procedural law tools such as search and seizure, expedited preservation of volatile data, interception of communications and others. It is important to note that these investigative means are to apply to the evidence on computer systems related to any criminal offence and not only for offences against and by means of computers. This gives the Convention a very broad scope. Article 15 requires Parties to establish conditions and safeguards to limit and prevent abuse of law enforcement powers and to protect human rights[3].

To engage in efficient international cooperation through a combination of urgent provisional measures (such as expedited preservation), and police and judicial cooperation.

Cybercrime is thus understood as offences against and by means of computers. It is also understood that any crime may involve electronic evidence and that this needs to be addressed in procedural law[4].

The Budapest Convention is a criminal justice treaty that establishes criminal law measures based on rule of law and human rights principles. While measures against cybercrime certainly contribute to national security and to cybersecurity, and while international cooperation against cybercrime based on this treaty can contribute to confidence and trust between states and de-escalate incidents of cross-border cyberattacks, the Budapest Convention is not an agreement aimed at the politico-military dimension of international relations and it is not a cybersecurity treaty[5].

The Budapest Convention does serve as a guideline and many countries have used it as a "model law" when preparing domestic legislation. Unlike other

---

3 For a discussion on article 15 see:
http://www.coe.int/t/dghl/cooperation/ economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_SafeguardsRep_v16_8nov11.pdf
For an overview of Internet case-law of the European Court of Human Rights see:
http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf

4 This has practical consequences for crime prevention and criminal justice policies and strategies: all law enforcement, prosecutors and judges need to have at least basic training in matters related to cybercrime and electronic evidence.

5 For a distinction between cybercrime and cybersecurity strategies see:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

"model laws", however, it is a negotiated and formally adopted international agreement and thus also a legal framework for cooperation between state parties.

The Convention is scalable in terms of membership. It is true that it has been prepared by the member states of the Council of Europe[6]. However, Canada, Japan, South Africa and the USA participated in it negotiations. The treaty is open for accession by any country that is prepared to fully implement it and cooperate with other parties. Eight states have been invited to accede so far[7].

It is also scalable in terms of content. In 2003, a Protocol on Xenophobia and Racism committed through computer systems was adopted. In February 2012, the Cybercrime Convention Committee (T-CY) began work on a solution to transborder access to data within the context of cloud computing. This may result in another protocol to the Convention or a soft-law guideline. Implementation of the Budapest Convention in conjunction with other instruments allows addressing challenges such as the sexual exploitation and abuse of children on the Internet, the terrorist use of the Internet, criminal money flows and money laundering on the Internet[8], the need to protect privacy and personal data, and others.

The Budapest Convention can be backed up or complemented by additional tools, guidelines and good practices. In recent years, the Council of Europe began to weave a web of tools around the Convention, such as on law enforcement/service provider cooperation[9], on judicial training[10], on law enforcement training strategies[11], on cybercrime strategies[12], on criminal money flows, and on specialized services.[13] In fact, training and materials developed by other organizations often take the Budapest Convention as the starting point as well.

---

6 Currently the Council of Europe has 47 member states (*www.coe.int*).

7 By February 2012, Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

8 For example, on 16 February 2012, the Financial Action Task Force (FATF) published the revised consolidated 40 Recommendations. Recommendation 36 encourages accession to the Budapest Convention.

9 *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf*

10 *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf*

11 *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf*

12 *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf*

13 *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf*

The Budapest Convention is a mature treaty. By the time it was opened for signature in November 2001 it had been preceded by more than twelve years of preparatory work and precursors in the form of soft-law recommendations. The ten years that followed its adoption showed that it has proven to work, that due to its technology-neutral language it is still most relevant, and that with each new party it is becoming more effective.

November 2001 – November 2011: Key achievements

The adoption of the Budapest Convention is a major achievement in itself. Cybercrime has been around from the late 1970s, and from the late 1980s onwards work on computer crime and information security had been underway at the level of the OECD[14] and the Council of Europe[15]. However, until 2001 there had not been sufficient experience and pressure to negotiate a binding international agreement. I would argue that in 2001 the Council of Europe exploited a window of opportunity when finalizing and adopting a treaty as comprehensive as the Budapest Convention on Cybercrime. I also believe that that window closed soon afterwards. Ten years later, information and communication technology have become far too important for governments and societies and involve such a large number of stakeholders that it would seem very difficult to bring all interests under an international agreement of the scope and depth of the Budapest Convention[16].

---

14 Leading in 1992 to the first version of the Guidelines for the Security of Information Systems
http://www.oecd.org/dataoecd/16/22/15582260.pdf

15 Leading in 1989 to Recommendation R(89)9 on Computer-related Crime *https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2*
And in 1995 to Recommendation R(95)13 on Problems of Criminal Procedure Law connected with Information Technology
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2

16 Considering not only the interests of different governments (some want to control content and the internet infrastructure, others promote a free and open Internet and fundamental rights, some want to address not only cybercrime but also cyberwarfare and cyberterrorism, others want to address cybersecurity, etc.) but also the "Internet street" (see the mobilization of protest against the SOPA and PIPA proposals in the US

The approach of the Council of Europe and of the current state parties to the Budapest Convention of building on this treaty and gradually rolling it out across the globe seems to be more promising than trying to negotiate a new agreement.

Key achievements since it adoption in November 2001, can be summarized as follows:

The Budapest Convention reinforced a process of legislative reform worldwide. This is particularly true since around 2006[17]. An inventory would suggest that such reforms have been carried out or are underway in at least 120 states. The Budapest Convention has served as a guideline to most of these countries[18]. The Convention thus facilitated a minimum of harmonization of legislation around the world[19]. The United Nations General Assembly[20] recommended that UN member states use the Budapest Convention to "Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime". This may further support harmonization.

The treaty had a reach beyond Europe. 55 countries had ratified or signed it or been invited to accede, including 14 non-European countries. The Council of Europe engaged with at least another 55 countries in technical cooperation on the basis of the Budapest Convention.

The Convention served as a catalyst for technical cooperation. Not only the Council of Europe, but also major donors such as the European Union now

---

Congress in January 2012 or against the Anti-Counterfeit Trade Agreement in many countries of Europe in February 2012 or against the law on blocking access to child abuse materials in Germany in 2010 which led to the abolishment of that law in 2011). Governments and politicians are likely to be reluctant to be seen promoting a new meaningful treaty on cybercrime.

17 In 2006, the Council of Europe launched its Global Project on Cybercrime that assists countries in the implementation of the Budapest Convention.

18 Which does not mean that all of them have implemented it in full.

19 See for example the country profiles prepared under the Council of Europe's Global Project on Cybercrime
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
Presentations at the Courmayeur Conference showed that also countries such as Iran based much of their law on the Budapest Convention or that China is using it as benchmark to identify gaps in domestic legislation.

20 UN General Assembly Resolution 64/2011 of 17 March 2010 on Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical infrastructures.

recognize that measures against cybercrime contribute to the rule of law and help countries make use of the development opportunities of information and communication technologies.

In countries that have implemented the Budapest Convention an increase in criminal justice measures against cybercrime is noted[21].

Police-to-police and judicial cooperation increased considerably between many of the parties to the Budapest Convention. Ratification of this treaty by the United States of America in 2006 was essential in this respect. All parties now have functioning 24/7 points of contact in line with Article 35.

The Budapest Convention has been one of the Council of Europe's main contributions to multi-stakeholder cooperation for Internet governance. This has been most visible during the Internet Governance Fora since 2006[22], the European Dialogue on Internet Governance[23] or the Octopus Conferences since 2004[24]. Multi-stakeholder cooperation includes in particular public-private cooperation. The private sector has supported the implementation of the Budapest Convention[25]. Practical results included the guidelines on law enforcement/service provider cooperation in the investigation of cybercrime of 2008[26].

Governments have a positive obligation to protect people through effective laws and law enforcement measures, for example, by implementing the Budapest Convention as noted by the European Court of Human Rights[27]. Article

---

21 In Germany, for example, changes in legislation in line with Article 8 (computer-related fraud) of the Budapest Convention closed a gap in legislation. Computer-related fraud now accounts for the largest number of cases recorded by the police (27,292 in 2010).
http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

22 *http://www.intgovforum.org/cms/*

23 *http://www.eurodig.org/*

24 *www.coe.int/cybercrime*

25 Microsoft in particular, but also McAfee and Visa Europe have been partners in project activities.

26 *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf*

27 See the case K.U. v.Finland
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA39864919
Regarding Article 15 see
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_SafeguardsRep_v16_8nov11.pdf

15 helps strike a fair balance between the need for effective law enforcement and procedural safeguards. The Convention is thus about "protecting you and your rights[28]".

In short, during the first ten years of its existence, the Budapest Convention became an essential element of norms of behaviour for cyberspace.

Leasons learnt

Standards, norms and good practices to meet the challenge of cybercrime have been and are being developed by public and private sector and international organizations. The main problem is that while they are available they are not sufficiently implemented in all regions of the world. Widest possible implementation of existing standards such as the Budapest Convention and other tools would seem the most effective way ahead. Discussions at the 2010 United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil) clearly underlined the need for technical assistance for capacity building against cybercrime[29].

The Budapest Convention de facto serves as the guideline or reference for cybercrime legislation worldwide, even in countries that for political reasons may not want to become parties.

In most countries, those responsible for legislation (ministries of justice, parliaments) and those responsible for criminal law measures (law enforcement, prosecutors, judges) see the benefits of this treaty. In some countries ministries of foreign affairs sometimes oppose it. The reasons brought forward concern less the substance of the treaty but the fact that their respective country did not participate in the negotiation of the Convention[30]. The historical fact that this

---

28 See Octopus conference 2011 – Outlook Panel 1 *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/Presentations/default_en.asp*

29 *http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress-documents.html*

While there was full consensus on the need for technical assistance, there was much disagreement on the need for a new treaty on cybercrime.

30 An anecdote for illustration: at the UN Crime Congress in Salvador I mentioned to the head of delegation from a G77 country strongly opposed to the Budapest Convention, that the legislation of his country had been guided by this treaty. His reply was: "What do you mean guided? We copied it word by word!" To my question why then he opposed it, he answered: "you don't understand: it's political!"

treaty was prepared by the Council of Europe and not by the United Nations is difficult to correct retroactively. For some, this problem is that serious that it prevails over the benefits of urgent international cooperation against cybercrime and the practical and legal value of the treaty.

For many other countries, this is not a major obstacle. They consider it in their national interest to cooperate against cybercrime, and consider that the Budapest Convention offers an existing and functioning framework to that effect. They also recognize that once they are parties they will participate in the operation of the treaty and, as members of the Cybercrime Convention Committee, will participate in its further development, for example, through protocols. They acknowledge that the treaty has the support of a significant number of countries and organizations gathering a very large share of Internet users, of the Internet industry and of the ICT infrastructure worldwide. For them, these advantages outweigh the fact that they had not been involved in negotiating it.

The effectiveness of the treaty increases with each new party. However, ratification or accession to the Budapest Convention has been slower than expected. There are several explanations. The expectation is that by the time of ratification or accession, all provisions are reflected in domestic legislation. The treaty comprises a range of procedural law measures, which means that states not only need to amend their criminal codes but also their criminal procedure codes. It is legitimate that governments and parliaments take time to make such amendments. But this is not the only cause for slow implementation. Within the European Union, member states often attempt to combine the ratification of the Budapest Convention with implementation of European Union instruments, such as the 2005 Framework Decision on Attacks against Information Systems[31], the Data Retention Directive of 2006[32] or the Directive on Attacks against Information Systems which is expected to be adopted in mid-2012[33]. This causes delays. There is a further important reason: for many decision-makers in governments and parliaments the question of cybercrime has simply not been high enough on their agenda. The 2007 attacks against Estonia and subsequent attacks against other states started to change this. It is expected that

---

31 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML*

32 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML*

33 *http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463*
This Directive will bring EU law more in line with the Budapest Convention.

by the end of 2012 the number of parties will have increased significantly[34]. This will enhance the Budapest Convention as a framework for trusted international cooperation against cybercrime.

Measures against cybercrime must be designed to protect rule of law and human rights principles. This means full implementation of Article 15 Budapest Convention on safeguards and conditions for law enforcement powers but also effective measures to protect privacy and personal data. The protection of personal data has become a key challenge of information societies. It is noteworthy that in many countries data protection legislation is adopted in conjunction with cybercrime legislation. The Council of Europe's Data Protection Convention 108[35] is open for accession to third countries, and in 2011 Uruguay was the first non-member state invited to accede.

While the Budapest Convention in its present form meets most needs, new challenges have emerged in recent years. These include issues related to cloud computing and the question as to how law enforcement can access data not stored on a specific computer system of a suspect but stored "somewhere" in the clouds, that is, possibly in foreign jurisdictions. As indicated above, in January 2012, the Cybercrime Convention Committee started its work on transborder access and jurisdiction in view of proposing a solution in the form of a protocol to the Budapest Convention or soft-law instrument providing guidance.

Governments around the world expect international organizations to provide support and coherent solutions. International organizations should therefore cooperate closely with each other to serve societies and help them meet the challenge of cybercrime. The experience of recent years suggests that there is much room for improvement. The main issue seems to have been the question of whether or not there should be another international treaty on cybercrime or cybersecurity or information security. While reflections on this are likely to continue in the foreseeable future, different international organizations could start engaging in closer cooperation in an area where there already is full international consensus, namely that of capacity building.

---

34 The EU's "Stockholm Programme – An open and secure Europe serving and protecting citizens" foresees that all EU member states will be have ratified by the end of 2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:EN:HTML

35 *http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=12/02/2012&CL=ENG*

The controversy about future "cyber treaties" is partly due a confusion of the concepts of cybercrime as a crime prevention and criminal justice concept and that of cybersecurity with critical information infrastructure and national security as primary rationale. Given the difficulty in coming to international agreements in such sensitive areas, a clarification of these two complementary but different concepts may help separate the issues into more manageable portions. For cybercrime prevention and criminal justice a solution already exists with the Budapest Convention. For the politico-military dimension of cybersecurity a different solution may need to be negotiated in the coming years, possibly in the form of principles of state behaviour in cyberspace as discussed for example by the OSCE[36] or in fora such as the London Conference on Cyberspace[37].

In any case, a major lesson learnt during the past ten years, is that while international treaties are essential to helping societies meet the challenge of cybercrime, they are only one element in a web of responses.

Conclusion: the web is a web

The World Wide Web, or more broadly the cyberspace of interconnected computer systems, is a web linking up a huge number of stakeholders, billions of users and increasingly every "thing[38]". It is a web with many nodes that changes day by day.

It offers unique opportunities and at the same time poses huge challenges; cybercrime and threats to cybersecurity are among them. It is a web of innovation, and this includes innovative responses to threats and challenges by public and private sector stakeholders and individuals.

As stated above, international treaties provide important frameworks. However, where cyberspace is dynamic and organic, international treaty making is usually slow, static and mechanical. A single, stand-alone international agreement cannot represent the sole regulatory response to security challenges in cyberspace.

An organic approach combining a range of measures is needed. Soft-law instruments or good practices may be more responsive to needs and be equally if not more influential than formal treaties. In short, we need to weave a web of responses to threats in cyberspace – a web with many nodes.

---

36 *http://www.osce.org/cio/77317*

37 *http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/*

38 See the "Internet of Things"

In such a web, the Budapest Convention is a node linked to crime prevention and criminal justice in general, to law enforcement capabilities and to many other rule of law as well as human rights issues. It is linked to regulations on data protection, child protection, terrorism prevention, anti-money laundering measures, organized crime treaties, telecom regulations, domestic legislation, consumer protection, codes of conduct, self-regulation, guidelines, good practices and many others. It is connected to cybersecurity which in turn is connected to national security but also social and economic development opportunities. And, importantly, it is connected to the many measures taken by the private sector, by governments and by other international organizations.

The strength and effectiveness of the Budapest Convention – and of all other responses for that matter – depends on the strengths of its connections with other nodes. I would maintain that the Budapest Convention has made an impact because it is part of an organic multi-stakeholder approach.

From such a perspective it would seem futile to focus on re-negotiating the same node again and again.

It would seem much more productive to build on what already exists, to engage in capacity building worldwide and to reinforce the links and synergies between multiple stakeholders and initiatives. In short: we should all cooperate in the weaving of a web of responses to cybercrime.

POTENTIAL NEW GLOBAL LEGAL MECHANISMS ON COMBATING CYBERCRIME AND GLOBAL CYBERATTACKS

STEIN SCHJOLBERG
Judge, Co-chair of the EastWest Institute (EWI); Cybercrime Legal Working Group, Oslo, Norway

I'd like to open with the following quotation, by prosecutor Benjamin Ferencz, the United States. He was a prosecutor at the Nürnberg War Crimes Tribunal, and the quotation as you will read:

"There can be no peace without justice, no justice without law, and no meaningful law without a court to decide what is just and lawful under any given circumstance."

Let me also open with a quotation from the former United Nations Secretary General Kofi Annan:

"In the prospect of an international criminal court lies the promise of universal justice."

Without an international court or tribunal for dealing with the most serious cybercrimes of global concern, many serious cybercrime attacks will go unpunished. The most serious, global cyber attacks in the recent years have revealed that almost nobody is investigated and prosecuted and nobody has been sentenced for those acts.

Such acts need to be included in a global treaty or a set of treaties and investigated and prosecuted before an international criminal court or tribunal.

Cyberspace, as the fifth common space after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations.

It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyber-threats.

Peace, justice and security in cyberspace should be protected by international law through a treaty, or a set of treaties, under the United Nations.

Critical infrastructure of many governments and private industry has been targeted by global cyber attacks in the recent years. The cyber attacks on sensitive national information infrastructures are rapidly emerging as one of the

most alarming international security threats and could be considered as most serious cybercrime of global concern. Such attacks may have a great potential impact on the global economy, international security and the critical information infrastructure of all nations.

A treaty, or a set of treaties, at the United Nations level, on cyber security and cybercrime, should be a global proposal based on potential for consensus.

The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda, for a framework for the international response to how global challenges to the international cyber security could be coordinated.

In order to assist the ITU in developing a strategic proposal, a global, high-level expert group was established in October 2007. I was the chairman for this group. This global expert group of almost 100 persons from around the world delivered the chairman's report and the global strategic report in 2008 with recommendations on cyber security and cybercrime legislations.

Global working groups

The United Nations office on Drugs and Crime in Vienna, Austria, organised the 12th United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010, and the congress made a recommendation in the Salvador Declaration –Article 42.

United Nations institutions made a follow-up and the recommendation was adapted by the United Nations General Assembly in its resolution 65/230.

3 main working groups have been established in 2010 in order to make recommendations for potential new, international legal responses to cybercrime. The United Nations has initiated a comprehensive study of the problem of cybercrime recommended in the Salvador Declaration, Article 42, to establish *"an open-ended, intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by member states, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime."*

This expert group –or study group- had its first meeting in Vienna in January, 2011.

The United States and the European Union have established a working group on cyber security and cybercrime at an EU-US summit in November

2010. the group is tasked with developing collaborative approaches to a wide range of cyber security and cybercrime issues. Among the efforts is *"advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties."*

The group had its first meeting in February 2011. EU has made additional remarks that large-scale attacks, which is an emerging trend, are not fully covered in the Convention.

The EastWest Institute (EWI) established in June 2010 a Cybercrime Legal Working Group, in order to advance consideration of a treaty or a set of treaties on cyber security and cybercrime. The members are independent non-governmental global experts on cyber security and cybercrime. The Working Group shall develop recommendations for potential new legal mechanisms on combating cybercrime and cyber attacks, and *"develop a consensus-building set of proposals related to international law."* The group had its first workshop in Brussels in March, 2011, the second workshop was held just recently in Lausanne, and the next workshop will be held in March 2012. I am the co-chair of this group.

The EWI Cybercrime Legal Working Group Recommendations, where I am the co-chair, will make proposals for non-partisan, objective, non-political solutions that may promote collaboration and serve as a compromise for the global inter-governmental organizations, and develop a consensus-building set of proposals related to an international criminal law for cyberspace.

Recommendations will include five main pillars.

The first pillar: recommendations for international laws on: substantive criminal law, procedural instruments, jurisdiction and international cooperation.

The recommendations may use existing regional agreements and convention as guidelines or as reference.

The second pillar: establishing A Global Virtual Task Force for the investigation and Prosecution. A Global Virtual Task Force should be established, including law enforcements, INTERPOL, non-governmental organizations, key stakeholders in the global ICT industry and sector, financial service industry, academia, working in a partnership.

A task force will be necessary for the prevention, detection, and responses to the global cybercrimes and global cyber attacks in fast and effective investigative measures and arrests, having real-time access to global information in cyberspace.

The third pillar: establishing an International Criminal Court or Tribunal for Cyberspace (ICTC).

Criminal prosecution based on international law need an international criminal court or tribunal for any proceedings. The most serious cybercrimes of

global concern, could be considered in the list of crimes within the jurisdiction of the International Criminal Court. An alternative solution could be to establish an International Criminal Court or Tribunal for Cyberspace.

The fourth pillar: recommendations for a global treaty on cyber security issues. Security models for the Information and Communication Technology (ICT) in cyberspace must be developed on a global level, defining a global and national cyber security strategy. Technical and procedural measures, organizational structures, capacity building, and international cooperation are the most important issues that should be included in a global treaty.

And the fifth and last pillar: blocking of child pornography websites.

Additional recommendations for a treaty or a framework on blocking of child pornography websites will be included. Blocking child pornography websites must be based on global and national solutions.

The International Criminal Court (ICC)

The International Criminal Court (ICC) was established at a conference in Rome in 1998 by 120 States. The Rome Statute of the International Criminal Court was adopted and it entered into force in July 2002.

The Court is independent from the United Nations, but has historical, legal and operational ties with the institution. The relationship is governed by the Rome Statute and by other relationship agreements.

The International Criminal Court (ICC) is the first ever permanent, treaty-based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.

The International Criminal Court may have a role to play in the fight of massive and coordinated cyber attacks against critical information infrastructures even today, under the current jurisdiction in force. According to article 93, paragraph 10, the Court may upon request *" cooperate with and provide assistance to, a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court, or which constitutes a serious crime under the national law of the requesting State."*

Massive and coordinated cyber attacks against critical information infrastructures may qualify as a "serious crime".

If massive and co-ordinated global attacks in cyberspace are included in

the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings. And the Prosecutor, which is an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on an exceptional basis. In accordance with Article 18 on preliminary rulings regarding admissibility, the Prosecutor may *"seek authority from the Pre-Trial Chamber to pursue necessary investigative steps for the purpose of preserving evidence where there is a unique opportunity to obtain important evidence or there is a significant risk that such evidence may not be subsequently available."*

Such an exceptional proceeding may very well be needed in investigations of massive and coordinated cyber attacks against critical information infrastructures in cyberspace. It is also the Pre-Trial Chamber that later on eventually issues an arrest warrant.

An International Criminal Court or Tribunal is necessary

Criminal investigation and prosecution based on international law, needs an international criminal court for any proceedings.

An international criminal court have been called a missing link in the international legal system. Many most serious global attacks will go unpunished without a criminal court or tribunal in action. When an International Criminal Court or Tribunal is established, then the principle of individual criminal accountability may globally be enforced.

Anyone who commits any of the cybercrimes included in the international cybercrime law can be prosecuted by the court.

This possibility may also be a cornerstone for the global cybercrime deterrence. An effective deterrence may be one of the primary goals for establishing a permanent court or tribunal. It will be a signal from the United Nations and the global community that global cyber attacks are no longer tolerated.

Provisions may be included in the list of crimes within the jurisdiction of the International Criminal Court (ICC) in The Hague. An alternative solution may be to establish a special International Criminal Court for Cyberspace as a subdivision of ICC in The Hague, since it may be a natural choice with all international courts inside, or in the urban area of this city.

But as an alternative subdivision in Singapore, where the INTERPOL Global Complex (IGC) will be established and operational in 2013/14 especially on enhancing preparedness to effectively counter cybercrime.

An International Criminal Tribunal for Cyberspace must be a United Nations court of law, established through a Resolution by the Security Council

in accordance with Chapter VII of the United Nations Charter.

The Tribunals authority could be prosecuting and sentencing the most serious cybercrimes and global cyber attacks of global concern, and should have jurisdiction on issues as follows:

- Violations of a global treaty or set of treaties on cybercrime;
- Massive and coordinated global cyber attacks against critical information infrastructures.

The Tribunal must have concurrent jurisdiction in relation to national courts, but may claim primacy over national courts and take over investigations and proceeding at any stage.

The Office of the Prosecutor should be operating independently of the Security Council, of any State, or any international organization, or of other organs of the Tribunal. Investigations are initiated by the Prosecutor at his/her own discretion on the basis of information received. Indictments must be confirmed by judges prior to becoming effective.

The Rules of Procedure and Evidence must be based on, and in consistent with, the Statute of the Tribunal. It should be guided by the Rules of Procedure and Evidence of other international criminal tribunals and courts, such as the ICC, the Tribunal for the former Yugoslavia and the Tribunal for Rwanda.

An International Criminal Tribunal for Cyberspace could be established in The Hague as the natural choice in 2013-2014.

A possible International Criminal Tribunal for Cybercrime, could, as an alternative, also be established in Singapore. The tribunal could be operational in time for the opening of Interpol Global Complex (IGC) in Singapore in 2013-14. It would open up a possibility of assistance and cooperation with an outstanding investigation institution.

The Prosecutor may then be assisted very efficiently in the determination if a case is of sufficient gravity in order to justify further action by the Tribunal. That would enable the global justice to promote the rule of law and ensure that the gravest international cybercrimes do not go unpunished.

A global virtual taskforce for the investigation and prosecution of the most serious cybercrimes of global concern

A Global Virtual Taskforce established in operational partnership with key stakeholders in the global information and communications technology industry, financial service industry, non-governmental organizations, academia, and the global law enforcement through INTERPOL, will be necessary for the

prevention and effectively combat global cybercrimes, especially for delivering fast-time responses to cyber attacks.

A basic platform must be the coordination and open sharing of knowledge, information and expertise between members of the taskforce, that may result in fast and effective investigative measures, arrests, convictions, and securing and preserving evidence in a way that ensures legal compliance across many jurisdictions.

The main task for a Global Virtual Taskforce on cybercrime should therefore be to prevent, detect, and respond to cybercrime, by investigation and prosecution of the most serious cybercrimes and cyber attacks of global concern.

A Taskforce could be overseen by a joint global Strategic Working Group.

Establishing an INTERPOL Global Complex (IGC) in Singapore is a very important effort and development for the international law enforcement to effectively counter cybercrime. A Global Virtual Taskforce for Cyberspace may also be seated in Singapore. Together, this cooperation may create the most efficient law enforcement support for all global cybercrimes.

The Prosecutor and the office of the Prosecutor shall be responsible for the investigation and prosecution of the most serious cybercrimes of global concern.

The Prosecutors Office should have the power to seek the most efficient assistance in the investigation of cybercrimes.

The Prosecutors Office may be assisted in the global investigation by two pillars.

INTERPOL has since the 1980s been the leading international police organization on knowledge about and global cooperation on computer crime and cybercrime investigation.

The INTERPOL network enables police to share information on cybercrime, and to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections. It is very important that the investigators of cybercrimes may swiftly seize digital evidence while most of the evidence is still intact.

It is vital that the police have an efficient cross-border cooperation when cyber attacks involve multiple jurisdiction.

The INTERPOL Global Complex based in Singapore may go into full operation in 2013/14, and employ a staff of about 300 people.

The Global Complex is an integral part of the INTERPOL efforts to reinforce its operational platform and will focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime.

Models for a Virtual Taskforce may be, but not limited to, the Metro-

politan Police Central e-crime Unit (PCeU), that was established in United Kingdom in 2008, in partnership with the taskforce in the United Kingdom.

The International Cyber Security Protection Alliance (ICSPA) is a business-led global organisation. It is a not-for-profit organisation, established in 2011 to channel funding, expertise and assistance to law enforcement cybercrime units in both domestic and international markets.

And another model may be the National Cyber Investigative Joint Task Force (NCIJTF) chaired by the FBI in the United States.

The text of a potential draft Statute

The text of a potential draft Statute; may be as follows:

The United Nations Security Council, acting under Chapter VII of the Charter of the United Nations, has established the International Tribunal for the prosecution of the most serious violations of International Cybercrime Law, (hereinafter referred to as "the International Tribunal") and shall function in accordance with the provisions of the present Statute.

I should only mention the draft Article 1, Competence of the International Tribunal.

The International Tribunal shall have the power to prosecute persons responsible for the most serious violations of international cybercrime law, in accordance with the provisions of the present Statute.

I will end my presentation also with a quote from my good friend, Professor Peter Grabosky, Australia:

"Those who fail to anticipate the future are in for a rude shock when it arrives."

HARD AND SOFT LAW OPTIONS IN RESPONSE TO CYBERCRIME, HOW TO WEAVE A MORE EFFECTIVE NET OF GLOBAL RESPONSES[1]

MARCO GERCKE
Director, Cybercrime Research Institute,
Köln University, Germany

Cybercrime is a typical transnational crime that – despite legal advancements made in various states – cannot simply be solved on a national level but requires international cooperation. When discussing the need to develop a legal response to the global challenge of Cybercrime the discussion in the past quickly focussed on the question whether there is need for a "Global Convention on Cybercrime" (I.) without first differentiating between the various elements that need to be addressed and without discussing which instruments are available to introduce them. This article provides an overview over key areas that require a legal response (II.), explains the various legal options in introducing suitable regulation (III.) and shows that the international community has a variety of choices.

I. Introduction

Computer-related crimes are not new phenomena. Since the 1960's the emerging use of transistor-based computer systems led to a debate about related crimes[2]. Even more recent trends and methods in Cybercrime such as "phishing", "botnet attacks", the rapid development of technology that is more difficult for law enforcement agencies to handle (such as "voice-over-IP (VoIP) communication"[3] and "cloud computing"[4]) have been live issues for years. It is

---

1 First publication in the February issue of Computer Law Review International (Cri) Cri 2012, 78-87, *http:// www.cr-international.com*

2 See for example: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq; Miller*, The Assault on Privacy-Computers, 1971; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq; Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 2.3.

3 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

4 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

therefore impossible to posit that sudden technical changes took states and international organizations by surprise. Nevertheless, despite half a century of debate many states and international organizations are still in the process of developing strategies, policies and legislation to address the challenges of Cybercrime.

More than one – especially during the eleventh[5] and twelfth[6] UN Crime Congress – the international community discussed the need for global response – but did not come to an agreement. Taking into account that Cybercrime is widely recognized as global challenge, the lack of agreement was most likely not due to a lack of common understanding that something needs to be done but because the debate neither differentiated between different components that need to be addressed (harmonisation of legislation, introduction of tools for a better cooperation in criminal law matters, harmonization of standards and procedures for the collection of evidence, …) nor between the different instruments that are applicable.

II. The Current situation and the consequences for an effective legal approach

1. Status Quo

a) Cross-border crime

Prior to the advent of the Internet, computer-related crimes were in general local or domestically based crimes. However the global dimension of the Internet facilitated the metamorphosis of computer-related crimes into a truly transnational crime. Via the medium Internet, offenders can act globally and commit crimes without ever having physically been at the location of the victim[7]. With the on-going globalization of services this trend has even increased. Services offered by Google Facebook and

---

5 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

6 Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

7 Regarding the independence of location and presence at the crime site see: *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 3.2.7.

Twitter, to name a few, are accessed by millions of Internet users worldwide. Consequently, any crime involving such global services almost automatically leads to a cross-border dimension.

b) Significant number of victims and significant losses

The growing number of victims of Cybercrime and the related losses are significant although it is difficult to quantify this trend. The underlying reason is that precise and available data in this area are insufficient, as such, one of the most important sources for measuring the number of crimes are crime statistics[8]. But most statistics only list crimes that are detected and reported[9]. In the area of Cybercrime there are serious concerns that the number of unreported cases is significant[10]. Many businesses fear that negative publicity could potentially damage their corporate identity and reputation[11] and private users may not believe that law-enforcement agencies will be able to identify offenders[12]. A comparison of the large number of offences committed with the classi-

---

8 *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf*.

9 Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: *www.mekabay.com/methodology/crime_stats_methods.pdf*.

10 The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, - available at: *http://www.heise-security.co.uk/news/80152*. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

11 See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: *http://www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm*; *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf*.

12 See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf*; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: *http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf*.

cally few successful investigations, instils very little faith in the exercise of reporting Cybercrime[13].

c) *State involvement*

Cyber attacks are not anymore the exclusive domain of criminals. With the growing dependence of information societies as well as critical infrastructure[14] on the availability of communication technology the risks of state-led attacks has risen incrementally. While it is uncertain as to the extent to which states are already involved in attacks, the fact that various countries[15] have developed defence strategies related to Cyberspace is clear evidence of the fact that the threat is not virtual at all.

d) *Summary*

Computer crime and Cybercrime are undoubtedly serious threats. The fact that the majority of crimes have assumed a transnational dimension not only makes it particularly difficult to investigate Cybercrime but also limits the ability of states to develop solutions on the national level.

2. *Consequences of the cross-border nature of cybercrime*

a) *Need for international cooperation and the availability of specific instruments*

Investigating crimes with a cross-border dimension requires cooperation between law-enforcement agencies in all the countries af-

---

13 In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: *http://www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin*; as well as the information provided on the Interpol website, available at: *http://www.interpol.int/Public/THB/vico/Default.asp*.

14 Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: *http://media.hoover.org/documents/0817999825_1.pdf*.

15 See for example the US Strategy: Department of Defense Strategy for Operating in Cyberspace, 2011.

fected[16]. Cross border investigations undertaken without the consent of the competent authorities of other countries affected are difficult due to the principle of national sovereignty. This principle prohibits countries to carry out investigations within the territory of another country without the permission of the local authorities[17]. Investigations need to be carried out with the collaborative support of the authorities in all the countries involved.

Cybercrime is not the first and is unlikely to be the last category of crime with a trans-border dimension. Nation states have in the past developed various tools to develop a framework for international cooperation. Bilateral agreements as well as multilateral agreements such as the United Nations Convention against Transnational Organized Crime (UNTOC)[18] and its three protocols,[19] the Inter-American Convention on Mutual Assistance in Criminal Matters[20] and the European Convention on Mutual Assistance in Criminal Matters[21] provide solutions for key issues. In addition to providing a basis for cooperation these agreements

---

16 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: *http://media.hoover.org/documents/0817999825_1.pdf*.

17 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: *http://www.law.uga.edu/intl/roth.pdf*.

18 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: *http://www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF*.

19 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

20 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: *http://www.oas.org/juridico/english/sigs/a-55.html*.

21 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

contain solutions for practical cross border issues such as definition of formal requirements of a request and the channels through which requests need to be transmitted. Despite the fact that such instruments are highly relevant not only in relation to traditional forms of trans-border crime (such as drug trafficking and environmental crime) but also in relation to Cybercrime it is necessary to underline that international cooperation is accompanied by specific needs that are not fully reflected in all traditional instruments[22]. One example is the need for expedited cooperation. The traditional procedures for submitting request for cooperation and the related formal requirements lead to handling times that pose a serious challenge to any Cybercrime investigation[23]. Short handling times and the availability of expedited means of communication and cooperation are vital for fighting Cybercrime as data required for tracing offences are often automatically deleted within a short period of time[24]. Consequently, contact points for cooperation requests that are available 24 hours a day ("24/7 points of contact"[25]) and the ability of the receiving party to immediately take measures to ensure that electronic evidence relevant for the requesting parting is not deleted ("Quick Freeze") are widely recognized as essential instruments of international cooperation in Cybercrime but are not standard aspects that are necessary contained in all traditional bilateral and multilateral agreements.

---

22 For an overview about the applicability of traditional instruments addressing international cooperation to Cybercrime see: *; Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 6.6.

23 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: *http://media.hoover.org/documents/0817999825_1.pdf*.

24 *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 3.2.10.

25 *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484; Such 24/7 networks is for example maintained by the G8 and contained in the Council of Europe Convention on Cybercrime. Regarding the functioning of the Council of Europe network see: The Functioning of 24/7 points of contact for cybercrime, 2009, available at: *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf*.

b) Need for harmonization of legislation and limited impact of national solutions

For centuries the ambit of criminal law has fallen within the primary domain of national legislation. In many respects criminal law is influenced by history and culture[26]. And despite inherent similarities criminal law and crime-related policies vary from country to country. Even in regions where countries have agreed to cooperate closely and have adopted a harmonized legislative approach – such as the members of the European Union – criminal law was until recently seen as falling within the sole competence of each member state[27].

However, unlike prior inventions like electricity (where we see different voltage and different plugs) the Internet is based on single technical standards[28]. Any country that ignores fundamental protocols would de-facto risk to be disconnected from global services. The need to respect the global standards in order to act globally is not limited to technology but relevant for legislation as well. While it is theoretically possible for a country to develop Cybercrime legislation based on dogmatic concepts

---

26 See: *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 et seq; *Hecker*, Sind die nationalen Grenzen des Strafrechts ueberwindbar? Die Harmonisierung des materiellen Strafrechts in der Europaeischen Union, JA 2007, page 561 et seq; *Herlin-Karnell,* Recent developements in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 et seq; *Rosenau*, Zur Europaeisierung des Strafrecht, ZIS 2008, page 9 et seq; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some prliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 et seq; *Nuotio*, Criminal Law and Cultural Sensitivity, Refaerd Argang 31, 2008, Nr. 1/120, page 18; *Johnstone/Jones*, History of Criminal Justice, 2011, page 6; Siegel von Wadsworth, Criminology: Theories, Patterns, and Typologies, 2012, page 7.

27 See in this regard: The Criminal Law Competence of the European Union, House of Lords, London, HL Paper 227, 2006; *Yakut*, Post-Lisbon Criminal Law Competences of the European Union, Marmara Journal of European Studies, Vol. 17, No. , 2009, page 1; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 et seq.

28 Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: *http://www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf*. Regarding the importance of single technical as well as single legal standards, see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

that significantly differ from global trends and best practices, such approach would limit a country's ability to participate in the global fight against crime. The reason is that a number of countries base their mutual legal assistance regime on the principle of "dual criminality". Dual criminality exists if the offence is a crime under both the requested and requesting party's law[29]. Investigations on a global level are, in this case, limited to those crimes that are criminalized in all cooperating countries. If countries – based on the premise that criminal law is national domain - develop standards that differ from international best practices this can effectively preclude the ability to cooperate on an international level and ultimately lead to the development and enshrinement of safe havens[30]. Harmonization of legislation is, therefore, identified as a key priority by several regional and international organizations[31].

III. Possible instruments to enhance the legal framework and the ability to cooperate internationally

Based on the status quo and this analysis (see II. above), two key requirements can be identified as the fundamental building blocks for an effec-

---

29 The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at *http://www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: *http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf*; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: *http://www.unafei.or.jp/english/pdf/ PDF_rms/no57/57-08.pdf*.

30 The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: *http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf*. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

31 Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: *http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf*.

tive legal approach: The global harmonization of legislation and the development and adoption of instruments that enable effective international cooperation. The harmonization of legislation is an essential component and critical conduit for the facilitation of transnational cooperation as it supersedes the challenges arising from the principle of dual criminality that ordinarily limits the ability of cooperation if the requested country does not criminalize certain conduct. It is to be underscored that in the development of applicable legal instruments, it is essential to incorporate Cybercrime specific procedures (such as "quick freeze").

1. Possible instruments for a harmonization of legislation

a) Binding international legal instrument

aa) Current Status

Taking into account the truly global dimension of Cybercrime the development of an international instrument to harmonize legislation would seem to be a universal panacea. However, to date no such international binding instrument exists. The United Nations have addressed the issue of Cybersecurity and Cybercrime in various resolutions[32] but have not yet – apart from the right of the child[33] and from transnational organized crime[34] - initiated the movement toward the establishment and promulgation of an international convention. Calls for such an instrument were raised both during the preparatory meetings of the 11th UN Congress on Crime Prevention and Criminal Justice in 2005 (when some member countries and the Western Asian regional preparatory meeting called for the negotiation of such convention[35]) and the 12th UN Congress on Crime Prevention and Criminal Justice in 2010 (when during all four regional preparatory meetings for

---

32 A/RES/45/121; A/RES/55/63; A/RES/56/121; A/RES/57/239; A/RES/64/211.

33 United Nations Convention on the Rights of the Child, A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

34 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: *http://www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF*.

35 Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

the congress, for Latin America and Caribbean[36], Western Asia[37], Asia and the Pacific[38] and Africa[39], countries called for the development of an international convention on cybercrime). However the Member States decided to postpone the decision and, instead, first recommended to invite the Commission on Crime Prevention and Criminal Justice to conduct a comprehensive study, which should, *inter alia*, examine options for strengthening existing and proposing new national and international legal or other responses to Cybercrime. This study is currently being undertaken and first results are expected at the end of 2012.

One other instrument that is sometimes referred to as an "international instrument" is the Council of Europe Convention on Cybercrime. Although the Convention on Cybercrime is supported by various international organizations, the fact that ten years after it has been opened for signature the United States is the only non-European country that has ratified the Convention underlines its de jure status as a regional vis-à-vis international instrument[40].

---

36 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

37 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

38 „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

39 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

40 For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

bb) Potential

An international instrument can play an important role in facilitating a global harmonization of legislation on Cybercrime. The negotiation of an instrument by an international organization such as the United Nations can ensure that the document reflects the needs of both developed and developing countries and respects differences in legal systems and traditions. In addition, such broad participation would ensure that the topics included are relevant for all countries and assume a more all-encompassing globalized approach in undertaking an international instrument to harmonize legislation.

One clear example is the approach to the aspect of illegal content such as xenophobic material. Some European and African countries prefer a broad criminalization, while countries with a strong protection for freedom of expression[41] have in the past expressed that they would be unable to sign any agreement containing such broad criminalization[42]. The negotiation process would, therefore, ensure that the final document identifies those areas that are widely accepted. This does and should,

---

41 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: *http://www.fas.org/sgp/crs/misc/95-815.pdf*.

42 This was for example discussed during the negotiation of the Council of Europe Convention on Cybercrime. See: Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

however, not prevent regions or groups of countries sharing similar views from going beyond those standards and agree upon additional areas of harmonization.

b) Utilising an existing regional instrument

aa) Current Status

In the past, different countries and organizations[43] have discussed the possibility of promoting the existing Council of Europe Convention on Cybercrime from 2001 (CoE Convention on Cybercrime) as a tool to harmonize Cybercrime legislation globally. In this regard, several countries such as Argentina[44], Pakistan[45], Philippines[46], Egypt[47], Botswana[48] and Nigeria[49] have used the CoE Convention on Cybercrime as a model without formally acceding to it.

bb) Potential

It is integral to point out that the biggest obstacle to such an approach

---

43 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: *http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp.* The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: *http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.*

44 Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

45 Draft Electronic Crime Act 2006.

46 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

47 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

48 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

49 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

would be the fact that the Convention on Cybercrime has been - despite the aim of developing international standards – developed by European experts based on European standards. This is clearly visible when analysing the terms of reference for the committee that developed the Convention on Cybercrime. Their mandate was to "examine, in the light of Recommendations No R (89) 9 on computer-related crime and No R (95) 13 concerning problems of criminal procedural law connected with information technology, in particular the following subjects. [...]". Both were recommendations from the Council of Europe that were based on the situation in the member states. Given the nature of its remit the composition of the committee shows the European dominance and the missing representation of developing countries. At it's 583rd meeting of Ministers' Deputies, it was decided that out of the 47 member states only 14[50] would be allowed to appoint one expert each. In addition a decision was taken that three non-members were allowed to participate (United States of America, Canada and Japan) – but without right to vote. Afterwards South Africa applied to attend as an observer and was authorized[51]. The underrepresentation of developing countries has attracted criticism[52] and the influence of mandate and composition of the working group – in addition to the fact that since its promulgation in 2001, the CoE Convention on Cybercrime has neither been updated nor provides cogent legal solutions for various serious offences – make it unlikely that this European approach can become a globally accepted standard.

c) Regional harmonization through binding instruments

aa) Current Status

In the last years, different regional organizations have developed instruments that are designed to harmonize Cybercrime legislation. One example is the CoE Convention on Cybercrime that aims to harmonize substantive criminal law, procedural law and means for international

---

50 Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden and The Former Yugoslav Republic of Macedonia.

51 Ministers' Deputies, 664/10.3, 17.03.1999).

52 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: *http://www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.*

cooperation. The CoE Convention on Cybercrime has during the last ten years been ratified by 32 out of 47 member-states[53].

Another regional organization that very actively develops legal standards is the European Union[54]. In the last ten years the European Union has developed several instruments such as the Framework Decision on Attacks Against Information Systems (2005)[55] , Data Retention Directive (2005)[56] and the Directive on Child Pornography (2011)[57].

---

53 *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: *http://media.hoover.org/documents/0817999825_221.pdf*; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; G*ercke*, 10 years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: *http://elr.lls.edu/issues/v23-issue1/aldesco.pdf*; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: *http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf*; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

54 For an overview about EU legal instruments see: *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 et seq.

55 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

56 Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

57 Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

In early 2011 the African Union presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa[58]. This Convention, that has not yet adopted, aims to harmonize the substantive criminal law, procedural law and international cooperation[59].

bb) Potential

The harmonization of legislation region by region does not necessarily contradict the idea of a global harmonization of legislation. A critical comparison of how different regional approaches such as the CoE Convention on Cybercrime[60], the EU Framework Decision on Attacks against Information Systems[61] and the Draft African Union Convention on Cyber Security[62] address illegal access shows a large degree of consistency in the prescribed approach and methodology. As long as regional organizations draft legal frameworks that are in alignment with international best practices they can have a major impact on global harmonization of legislation.

d) Model legislation

aa) Current Status

One significant factor in harmonizing Cybercrime legislation is the development of Model Laws, a practice which has experienced a crescendo over recent years.

One of the first instruments was the Stanford Draft International Convention[63]. This was developed as a follow-up to a conference hosted by

---

58 The Draft Convention is available for download at: *http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf*

59 *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 5.2.6.

60 Art. 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

61 Art. 2 (1) :Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

62 Art. III-2: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

63 *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: *http://media.hoover.org/documents/0817999825_221.pdf*.

Stanford University in 1999[64] and aims to harmonize substantive criminal law and procedural law provisions. Though quite a laudable initiative, it has not been determined whether this Model was widely used by countries to bring their legislation in line with best practices.

More impact has been generated by the Commonwealth Model Law on Computer and Computer Related Crime. The Commonwealth Model Law was developed by an expert group based upon a mandate of the Law Ministers of the Commonwealth[65]. In March 2002 the Expert Group presented its report and recommendations[66] and later in 2002 the draft was produced[67].

In 2008 the International Telecommunication Union and the European Union launched the project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR) to promote the ICT sector in the Caribbean re-

---

64 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: *http://media.hoover.org/documents/0817999825_249.pdf.* For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: *http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf*; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: *http://media.hoover.org/documents/0817999825_221.pdf*. ABA International Guide to Combating Cybercrime, 2002, page 78.

65 See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

66 See: *http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_ Computer%20Crime.pdf* (Annex 1).

67 Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: *http://www.thecommonwealth.org/shared_asp_files/ uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20 Crime.pdf*. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: *http://www.cpsu.org.uk/downloads/2002CLMM.pdf*; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: *http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.*

gion[68]. One of the outputs was an assessment of Cybercrime legislation in the Caribbean region and a comparison with applicable international best practices[69]. Based on the assessment, a model policy and a model legislation was developed that is currently implemented by beneficiary countries. The Model Law not only reflects the demands of the region but is in line with international best practices[70]. Similar approaches have been undertaken in the Pacific[71] and Sub Sahara Region[72] with a total number of more than 70 countries in all three projects.

bb) Potential

Model laws by its very nature differ from international and regional agreements[73]. The primary difference is that a model law is not binding[74]. The focus is shifted from ensuring that each country criminalizes the same acts following the same methodology and approach to the aim of ensuring that countries wishing to criminalize a certain conduct have access to workable sample legislation that may also be used by other countries. While this may appear as a disadvantage when it comes to the harmonization of legislation, a closer analysis of the practical effect of Model Laws shows that this is not necessarily the case. There are actually two main advantages of a Model Law:

The fact that a Model Law is not binding allows to include provisions that only some but not all countries agree to. This for example enables those countries wishing criminalize a certain behaviour to do this by using the provision provided by the model law, while countries that do not wish to criminalize such conduct or require additional restrictions

---

68 For more information about the project, see: *http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.*

69 The assessment report is available on the project website: *http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.*

70 For an overview about the project and the comparison with other instruments see: *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 5.2.9 and chapter 6.

71 ICB4PAC. For further information about the project see: *http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.*

72 HIPSSA. For more information see: *http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/.*

73 *MacLeod*, Global Governance and the Quest for Justice, Vol. 2, 2006, page 124.

74 See *Viljoen/Precious,* Introduction, in Viljoen & Precious (eds), Human Rights Under Threat, 2007, page 13; American Intellectual Property Law Association Bulletin, 1989, page 895.

can simply ignore or modify the model provision. Consequently, it is possible to include provisions on controversial topics (such as the criminalization of xenophobic material) that would otherwise be left to other institutions to deal with. This flexibility can also theoretically be achieved through restrictions and reservations but it is unusual that all provisions in a convention include such restrictions and reservations.
In addition, its non-binding nature makes a Model Law easier to amend and update, if necessary, to facilitate development in technology and global trends. The fact that the CoE Convention on Cybercrime has not been substantively updated within the past 10 years (though several gaps have been identified and the sophistication in the type and level of crimes has led to new developments that were not known at the time the CoE Convention on Cybercrime was drafted) underlines the degree of difficultly that is attached to the amendment of a regional instrument. By comparison a Model Law comes with a greater degree of flexibility. What remains is the question whether a Model Law is less effectively harmonizing legislation because it is non-binding in nature and countries may see it more as a suggestion while implementing something else. There are two main arguments in this regard: Firstly, even binding instruments may not be implemented completely by the signatory states. For example, Germany has signed and ratified the CoE Convention on Cybercrime but subsequently has never proceeded to introduce domestic legislation that deals with expediting the preservation of computer data as required by Art. 16[75]. Apart from this, experiences with the implementation of Model Laws in the Caribbean and Pacific show that despite the non-binding nature of Model Law the countries implement the Model Law by incorporating into the domestic legal framework and simultaneously adapt the provisions of the Model Law to complement their domestic legal system and circumstances.

e) Code of Conduct

aa) Current Status

The development of a Code of Conduct is akin to Model Laws as it also falls within the genre of soft law instruments that are general in nature in and non binding[76]. They are widely used – especially within the pri-

---

75 For more examples where countries like Germany and the US failed to implement the standards of the Convention on Cybercrime see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

76 Regarding the nature of Code of Conducts see*: Gersen/Posner*, Soft Law: Lessons from Congressional Practice, Stanford Law Review, Vol. 61, Issue 3, page 573 et seq.

vate sector. One example is the Code of Conduct of the Internet Service Providers' Association of South Africa[77]. It addresses issues relevant for providers such as protection of consumers against SPAM.
Such soft law instruments are not only useful when it comes to the private sector but also in relation to criminal law and state behavior. One example of use of a Code of Conduct in the sphere of criminal law is the UN Code of Conduct for Law Enforcement Officials[78]. Art. 1 of this Code of Conduct underlines that law enforcement officials shall at all time fulfil the duty imposed upon them by law. This example clearly underlines one main difference to a model law that in general provides more precise language. While a Model Law would for example be an adequate basis for the provision of sample language for criminal law provisions a Code of Conduct can address more general aspects and may be used as an effective tool in regulating such areas of law states agree to harmonize. A clear example of its proposed utility is the instance where the representatives of China, the Russian Federation, Tajikistan and Uzbekistan proposed to the UN to define state responsibility regard to Internet security by submitting the proposal of an International Code of Conduct for Information Security[79] (and not a Model Law).

bb) Potential

Non binding instruments such as Model Laws or Codes of Conduct are instruments that may especially be used in areas requiring a non-binding basis as well as transparency and clarity with regard to certain standards. As it will never be possible to create binding responsibilities by means of a Code of Conduct such instrument is especially useful where a binding nature is either not necessary or already exists through other means. The adoption of a Code of Conduct also provides greater autonomy and self-regulatory powers in dealing with specific issues that may be particular to certain states.
Concerning Cybercrime[80] the use and development of a Code of Con-

---

77 The Code of Conduct is available at: *http://ispa.org.za/code-of-conduct/*

78 Code of Conduct for Law Enforcement Officials. A/RES/24/169.

79 Letter dated 12 September 2011 from the Permanent Representative of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359.

80 Other areas addressed in a Code of Conduct related to the broader topic of Cyber Security could be state involement and the related question of self defence, protection of fundamental rights such as freedom of speech and access to information, net-neutrality and more general aspects of security such as the need to implement protection measure.

duct could underline the willingness of states to develop Cybercrime legislation, define benchmarks or subject matters (definitions, substantive criminal law, procedural law, jurisdiction, electronic evidence, liability of Internet Service Provider and international cooperation). While theoretically a Code of Conduct could even define in an abstract way which conduct should be criminalized ("illegal access") it is unlikely that a Code of Conduct includes sample language ("Who, intentionally and without right, access […]"). It is therefore suggested that such Code may serve as a preliminary step and, if desired or deemed necessary, such details can provide a base which may effectively be transferred to a Model Law that the Code of Conduct refers to.

f) Standards and Norms (FSC/ISO)

aa) Current Status

Standards are widely considered as agreed and periodically updated norms[81]. Examples are performance-based FSC standards or procedure-based ISO norms[82]. They are normally associated with technical processes. However, despite the existence of many such standards which address various aspects of technology, there are currently none which specifically deal with the to technical aspects of Cybercrime because there is a great concentration on issues such as services (e.g. ISO 9001) and security (e.g. ISO 27001).

bb) Potential

The close nexus between security, that is already addressed by ISO norms, and crime explains why certain aspects of Cybercrime legislation as well as crime prevention are identified as possible areas where Standards could be introduced[83]. While the discussions thus far greatly focus on the application of existing norms (such as the definition of incidents) the topic can potentially be discussed on a broader basis. The development of globally applicable technical Standards is especially applied to the area of criminal procedural law (forensics) and the entire process of collecting and analysing electronic evidence. Such Standards can contribute significantly to ensuring that the same procedures and technical standards are universally applied – for example

---

81 *Darbyshire*, Mechanical Engineering, 2008, page 290.

82 *Smouth*, Tropical Forests, 2003, page 206.

83 *Almeida*, Legal rules and Information Security technical standards: possible approach for fillin in the blanks of cybercrime legislation, 2011.

while collecting electronic evidence or maintaining the integrity of electronic evidence. The further endorcement of such Standards through legislation or judicial decisions can significantly enhance the ability of countries to conduct cross border exchange of electronic evidence.

2. Possible instruments international cooperation

a) Binding international legal instrument

aa) Current Status

For the time being, the instrument containing important regulations related to international cooperation with the broadest reach is currently the United Nations Convention against Transnational Organized Crime (UNTOC)[84]. However, this Convention is only applicable with regard to offences involving organized crime and does not contain Cybercrime-specific instruments such as procedure to request expedited preservation of computer data[85].

Such Cybercrime-specific instruments are contained in the CoE Convention on Cybercrime. But with only one ratification from a jurisdiction outside of Europe, the CoE Convention on Cybercrime may not be characterized as essentially international in its global reach. One of the advantages of the CoE Convention on Cybercrime is its Art. 27 that deals with procedures pertaining to a mutual legal assistance request in the absence of applicable international agreements[86]. However, these procedures are only applicable if both states are party to the Convention and given the limited extent of assent and ratification, this inherently defeats the intended global span of the CoE Convention on Cybercrime which, based on its constitution, is a fundamental requirement for its workability and success.

---

84 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: *http://www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.*

85 *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 6.6.4.

86 For more details see: *Gercke,* Understanding Cybercrime, 2nd Edition, ITU, 2011, chapter 6.6.9.

bb) Potential

An effective fight against Cybercrime requires international cooperation. As offenders can perpetrate a crime from any place in the world, each country should be able to effectively cooperate with any other country in order to deal with security infractions. While the harmonization of legislation can be carried out through regional and soft law approaches the development of reliable instruments for effective international cooperation depends on either bilateral or multilateral agreements. If two countries wish to cooperate with regard to Cybercrime investigation and these countries have neither signed a bilateral agreement nor are part of a multilateral agreement requests needs to be based on international courtesy, based on reciprocity[87]. The need for a truly international and widely accepted instrument for international cooperation is far more urgent than the need for an international tool to harmonize legislation.

b) Using an existing regional instrument to globally harmonize legislation

The possibility of promoting the existing CoE Convention on Cybercrime on a global level has been raised in discussions in the past. However, it is essential to bear in mind that instruments related to international cooperation are only fully effective if both countries that wish to participate are parties to the convention. This would, therefore, require that as many countries as possible accede to the Convention. Given the fact that in the last ten years only 33 countries have ratified the CoE Convention on Cybercrime and despite several invitations to accede submitted to non-members of the Council of Europe, this has not shown the desired measure of success.

Given recent developments in the international sphere and the desire to foster greater integration and cooperation on an international level in treating Cybercrime it evolve into the development of a harmonized Global Convention on Cybercrime. In addition to the introduction of a new international instrument, an amendment of existing instruments (such as UNTOC) may also be considered as a viable option pending such development.

---

87 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; *Recueil Des Cours*, Collected Courses, Hague Academy of International Law, 1976, page 119.

c) Bilateral Agreements

aa) Current Status

International cooperation can be based on bilateral agreements that define procedures and rights and obligations of both the requesting and requested party[88]. Various countries have signed bilateral agreements. By way of example, Australia has signed more than 30 bilateral agreements with other countries regulating aspects of extradition[89]. While it is also known that specific aspects related to Cybercrime investigations have been addressed during the negotiations of some agreements, it is uncertain whether the existing agreements adequately govern Cybercrime-specific aspects such as requests for expedited preservation[90].

bb) Potential

The addition of Cybercrime-specific clauses to existing bilateral agreements at the time of their re-negotiation as well as negotiating new agreements is certainly an avenue that may be taken into consideration. However, it is highly unlikely that bilateral agreements will ever provide a comprehensive basis for effective global international cooperation in the fight against Cybercrime because it would be logistically onerous and near impossible to negotiate such a large number of agreements. This matter was highlighted within the context of the development of the Commonwealth Model Law. It was pointed out that just for the members of the Commonwealth it would require not less than 1,272 bilateral agreements to deal with international cooperation in this matter[91].

---

88 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: *http://www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.*

89 A full list of agreements is available at: *http://www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.*

90 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: *http://www.oas.org/juridico/english/cybGE_IIIrep3.pdf.*

91 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: *http://www.cpsu.org.uk/ downloads/2002CLMM.pdf.*

d) Regional harmonization through binding instruments

aa) Current Status

International Cooperation based on regional instruments is a more commonly adopted procedure. The Inter-American Convention on Mutual Assistance in Criminal Matters[92], the European Convention on Mutual Assistance in Criminal Matters[93] and the CoE Convention on Cybercrime[94] are just three examples for such instruments.

bb) Potential

Taking into account the global nature of Cybercrime it is unlikely that regional instruments can provide the broadly based spectrum needed to effectively facilitate the requirements of cooperation on a global scale.

e) Model Legislation, Code of Conduct and Standards/Norms

In light of the the fact that Model Laws are non-binding[95] and unlike international agreements do not require a formal adoption and incorporation into domestic law[96] they cannot effectively serve as a substitute for bilateral or multilateral agreements. While Model Laws are useful as a tool to harmonize legislation they may not provide the most appropriate basis for international cooperation but serve as an instrumental tool in harmonization of laws. This hypothesis seems also true for the impact of a Code of Conduct which has as one of its advantages the ability to strengthen the idea of international cooperation. Standards and Norms can be seen as driving forces which can facilitate the development of technical processes of submitting requests, automatic authentication and encryption and procedures in dealing with requests for international cooperation.

---

92 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: *http://www.oas.org/juridico/english/sigs/a-55.html*.

93 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

94 Council of Europe Convention on Cybercrime, ETS 185.

95 See *Viljoen/Precious,* Introduction, in Viljoen & Precious (eds), Human Rights Under Threat, 2007, page 13; American Intellectual Property Law Association Bulletin, 1989, page 895.

96 *MacLeod*, Global Governance and the Quest for Justice, Vol. 2, 2006, page 124.

IV. Conclusion

An effective fight against the transnational phenomena of Cybercrime requires various measures that range from technical solutions to legislation. Considering the harmonization of legislation and the global availability of Cybercrime-specific means for international cooperation, the crucial question is not whether there should be an international convention on Cybercrime.

When it comes to the harmonization of legislation the international community, with the support of international and regional organizations, states have various options. However, an analysis of the hard and soft law instruments available for international cooperation reveals rather limited options because without a widely accepted international instrument that specifically addresses Cybercrime-specific issues, international cooperation will hardly ever be effective.

All things being equal, however, this still leaves quite a variety of combinations. States can, for example, develop a Code of Conduct that deals with state related issues (like state involvement and self defence) and general commitments, amend the existing basis for cooperation in criminal law matters through UNTOC, negotiate model legislation and develop Norms and Standards for technical process. Alternatively, they may opt to develop a more comprehensive international agreement that combines the harmonization of legislation with international cooperation and add standards that deal with technical processes.

Ultimately it is up to the members of the international community to determine, on both international and national level the destination and the route for the global response evolving in the future.

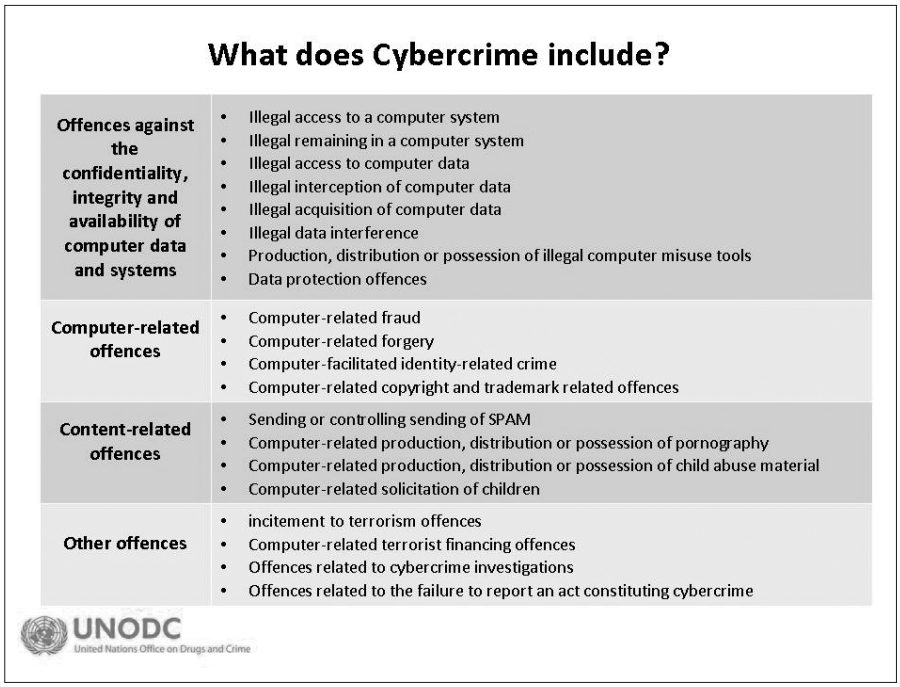
Part V

INSTITUTIONAL AND CIVIL SOCIETY APPROACH TO CYBERCRIME

UNITED AGAINST CYBERCRIME: THE UNODC/ITU CYBERCRIME CAPACITY BUILDING INITIATIVE

GILLIAN MURRAY
Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC

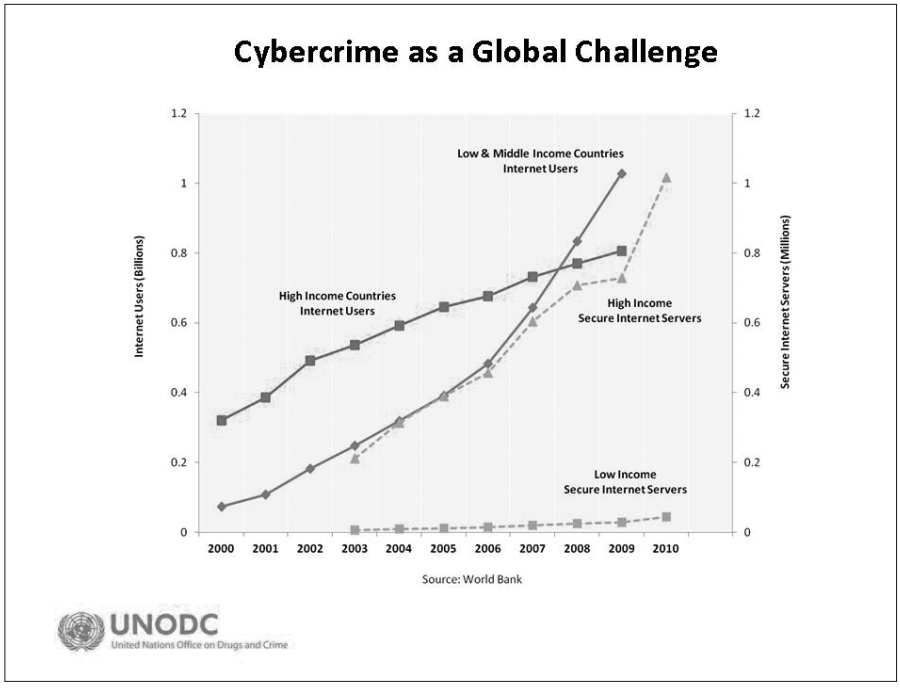
UNODC's response to cybercrime is from the crime prevention and criminal justice angle, with a focus on developing countries.



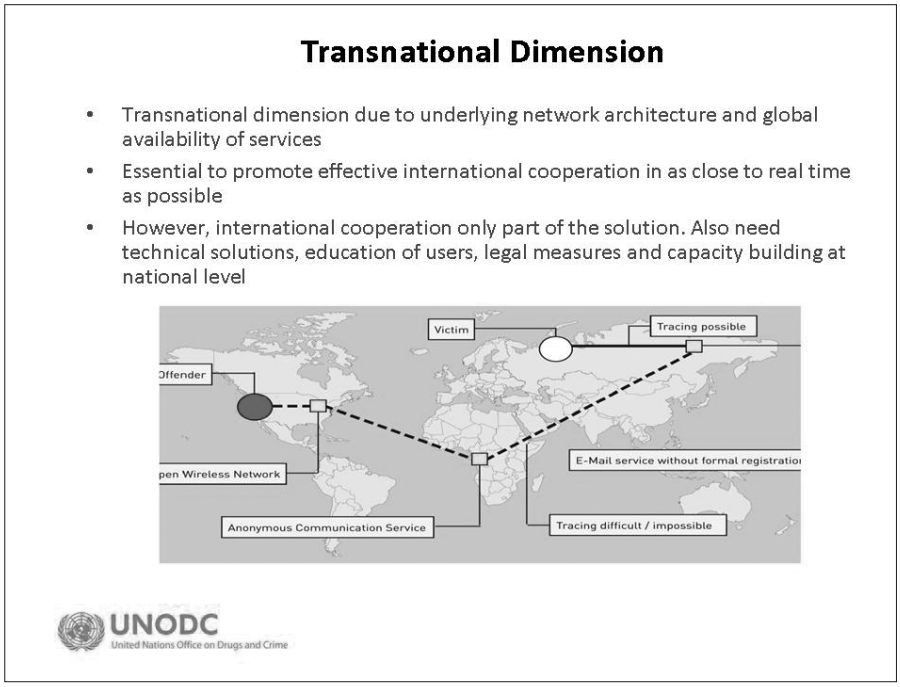
In 2008, the number of internet users (defined by the World Bank as people with access to the internet) in low and middle income countries surpassed that in high income countries. At the same time, as the number of secure internet servers (defined by the World Bank as servers using encryption technology in internet transactions) in high income countries increased to over one million, the number of secure servers in low and middle income countries has

stayed below 50,000. This illustrates the vulnerability of a significant number of global internet users.

These users may perform – for example – financial transactions using insecure resources on local servers.



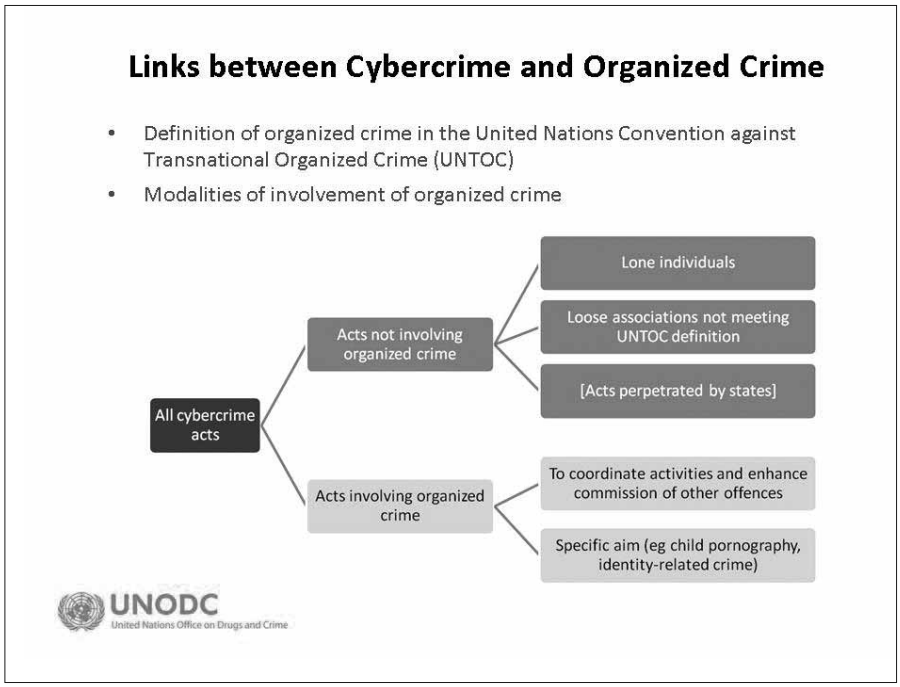
International cooperation mechanisms for rapid contact between law enforcement (for the purposes eg of preserving data that can be used in evidence) are also less developed. For example, in the G8 24/7 points of contact group, low and middle income members do include Botswana, India, Indonesia, Mauritius, and Namibia, but by far the majority are high income economies. It is evident therefore that less developed countries require assistance to counter cybercrime. The transnational nature of cybercrime, the established involvement of organized criminal groups, as well as the governance failures which often sustain these forms of criminality, make them highly relevant to UNODC mandates. International cooperation in real time is therefore vital to counter cybercrime. Equally important, however, is collaboration within countries between the various involved departments/ministries etc. How can international cooperation with low and middle income countries in cybercrime matters be improved? Possible steps could include: Recruitment to existing 24/7 points of contact



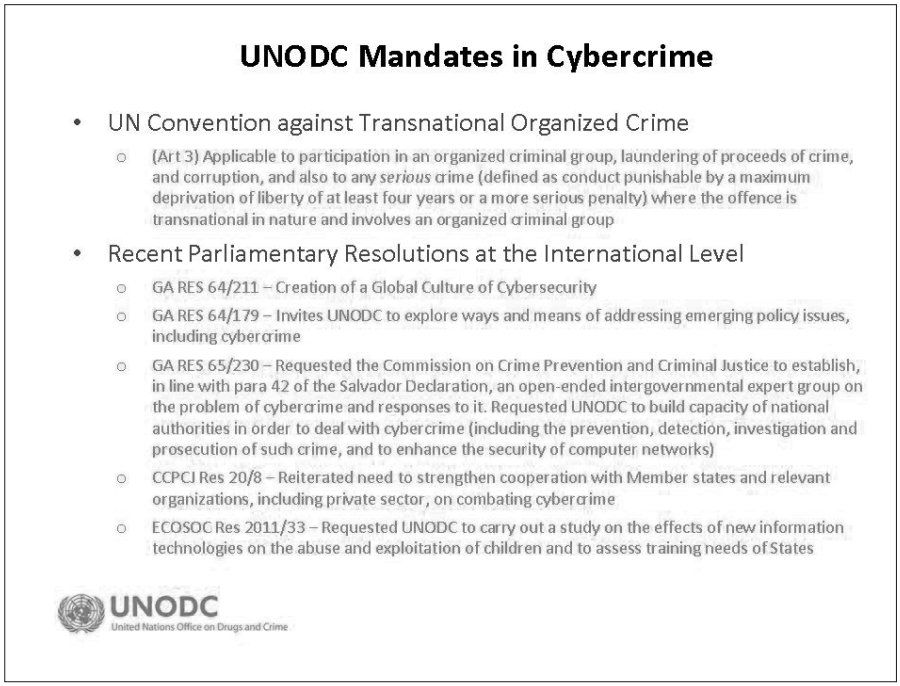
groups (membership does not necessarily require a 'high-tech' crime unit); development of simple methods of communication and information sharing between law enforcement authorities, such as online platforms; encouraging international service provider companies or subsidiaries present in low and middle income countries to develop strong working relationships with law enforcement even in absence of legal requirements – eg data retention and access policies (subject to necessary privacy rights protections)

In discussing cybercrime and organized crime, it is necessary to distinguish between two main categories of involvement by organized criminal groups: (1) the use of information technology by traditional organized criminal groups and (2) organized crime groups focusing on committing cybercrime. Traditional organized criminal groups without a background in Internet-related criminal activities use information technology to coordinate activities and enhance the commission of crimes. In such cases, information technology is used to improve the efficiency of the organized criminal group in its traditional field of activity. This includes the shift to electronic communications, which for example enables the organized criminal groups to make use of encryption technology and to communicate anonymously. Reports also point to a trend of traditional organized criminal groups becoming active in new forms of criminal activities in the area of high-tech crimes. This includes

software piracy and other forms of copyright infringement. Other areas of cybercrime, such as child pornography and identity-related crime, are also often linked to organized crime.



UNODC has received many mandates from over the years related to cybercrime, including: UN Convention Against Transnational Organized Crime; and Resolutions of the General Assembly, ECOSOC, Crime Commission, and Crime Congresses. These invite UNODC to explore the feasibility of providing assistance to address computer-related crime under the aegis of the United Nations and in partnership with other similarly focused organizations. UNTOC, can also be utilized, where applicable, with a view to fostering international cooperation in the field of cybercrime. Many common forms of computer-related crimes do fall within the definition of UNTOC as they are transnational in nature, involve an organized criminal group, and are committed with the aim of achieving material or financial benefit. But, for UNTOC to be relevant it must meet all three criteria. This means that UNTOC cannot always be used such as in cases of individual involvement.



In presenting UNODC objectives on cybercrime, I would like to highlight in particular, that the nature of the challenge requires working together at the international and national level. We need capacity building and training and prevention/education activities etc – all of which contribute to a long term and sustainable holistic approach. At the international level, a number of organizations are active in the area of cybercrime and we need to work together in line with our respective mandates. Developing countries need assistance, and here there is a clear role/niche for UNODC just as there is for the CoE, ITU, OSCE and other players.

UNODC is a technical hands-on agency and brings expertise in the area of crime prevention, criminal justice and the rule of law which complements other necessary approaches, including the cybersecurity mandate of ITU. There is a very clear role for the UN with regard to capacity building in developing countries and UNODC in particular as the only global institution with a clear crime prevention and criminal justice mandate.

GA Res 65/230 also mandated an intergovernmental expert working group to conduct a comprehensive study on the problem of and response to cybercrime. The intergovernmental expert working group established first met in January 2011 to define a methodology for the study. Topics defined in the methodology for the study include: Phenomenon of cybercrime; Statistical information; Challenges of cybercrime; Common approaches to legislation; Criminalization; Procedural powers; International cooperation; Electronic evidence; Roles and responsibilities of service providers and the private sector; Crime prevention and criminal justice capabilities and other responses to cybercrime; Role of international organizations and Technical assistance.

UNODC Activities to Date

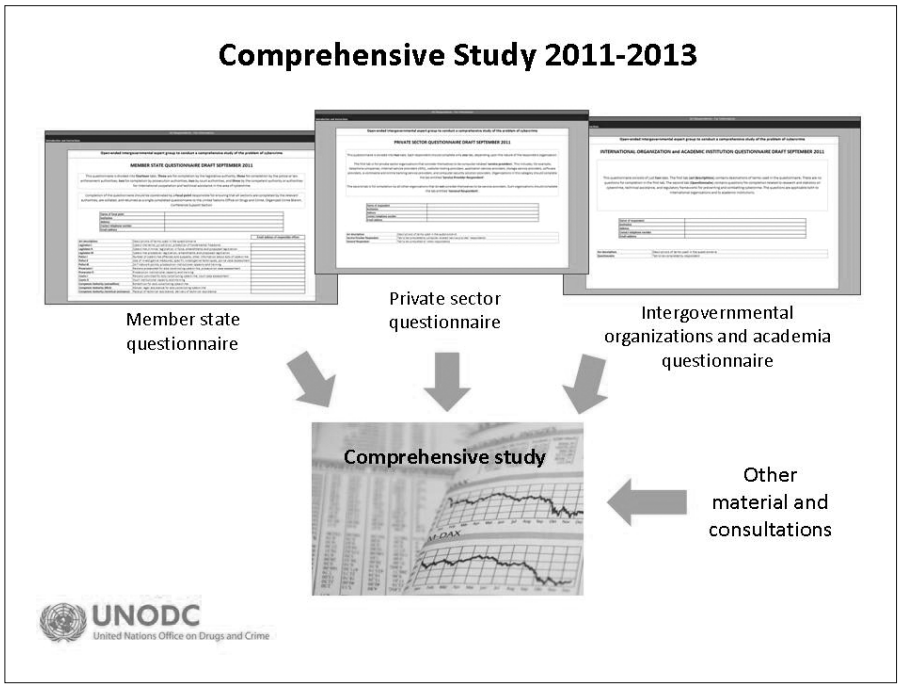
Development of training workshops on live data forensics (2009)	• Organized in cooperation with Irish Police Service and University College, Dublin
Development of handbook on identity-related crime (2009)	• Designed for use by legislators, policy-makers, prosecution and law enforcement authorities
Analysis of global cybercrime threat included in Transnational Organized Crime Threat Assessment (2010)	• Examined global threat of identity theft and child pornography
Establishment of joint activities with ITU (2011)	• Framework for UN response in areas of cybersecurity and cybercrime
Development of methodology for comprehensive cybercrime assessment (2011)	• Covering policy, legislation, regulation, investigation, prosecution, court, prevention and public-private partnerships
Pilot assessment mission (2011-2012)	• Cross-sectoral assessment mission
Development of questionnaire and desk research for comprehensive study (2011-2012)	• Questionnaire developed for Member states, private sector, intergovernmental organizations and academia

UNODC
United Nations Office on Drugs and Crime

Cross-National Legal Frameworks

- To date, cybercrime primarily addressed through national legislation and cross-national frameworks (binding and non-binding), including Arab League Model Cyber Law, Commonwealth Model Law on Computer and Computer-related Crime, ECOWAS Directive, cooperation agreement between CIS countries on computer crimes, Council of Europe Convention on Cybercrime, EU Legislation
- Within preparatory meetings for the 11th Crime Congress in 2005 a number of Member States called for a UN Convention on Cybercrime but no decision to initiate such a process
- All four regional preparatory meetings of the 12th Crime Congress in 2010 called for the development of an international instrument. Member States decided to undertake a comprehensive study of the problem of cybercrime and responses to it

UNODC
United Nations Office on Drugs and Crime



Data gathering for the comprehensive study will commence in February 2012 through the sending of a questionnaire to all Member states, to private sector organizations, academic organizations and intergovernmental organizations. Respondents will have three months to complete the questionnaire and a first draft of the study is envisaged by November 2012. Thereafter, the study will inform Member States in their deliberations as they examine options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

FOSTERING INTERNATIONAL COOPERATION ON CYBERSECURITY A GLOBAL RESPONSE TO A GLOBAL CHALLENGE

CARLA LICCIARDELLO
Project Officer on Cybersecurity, International Telecommunication Union - ITU

In the last few years there has been a dramatic increase in sophistication, in volume and in the occurrence of cybercrimes. Today the impact of cyber threats can be felt in most of national infrastructures, such as education, health, financial sector, etc. Cyber threats are not subject to national borders and the current level of the technology allows the launch of cyber-attacks on any national critical infrastructures from anywhere and everywhere.

Countries are responding to cyber threats in a number of ways. Although some states are just beginning to address the issue of Cybersecurity, most governments at the very least now recognize the need for allocation of resources and development of Cybersecurity strategies. But with cyber threats presenting a growing risk to not just to governments but to the business community and individuals at large, there is a need for greater international collaboration that includes all stakeholders. In the arena of Cybersecurity, everyone is a combatant. The responsibility for keeping networks safe must be a joint effort of governments, the private sector, civil society and international organizations.

As the UN specialized agency for ICTs, ITU plays a leading role in terms of infrastructure, the creation of an enabling environment, and building capacity worldwide. Our mission is to connect the world – and with over five billion mobile cellular subscriptions, and more than two billion people online, we are doing a good job in that regard (even if very much more still needs to be done, especially in terms of broadband access). But with increased connectivity, of course, comes the growing issue of global public confidence and security in the use of ICTs – or, in short, Cybersecurity.

ITU's concrete response was to launch the Global Cybersecurity Agenda, known as the CGA in 2007, as a global framework for international cooperation. In 2008, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) formally entered into a Memorandum of Understanding, after which IMPACT's state-of-the-art headquarters in Cyberjaya, Malaysia, became the physical home of the GCA. ITU IMPACT is the first truly global multi-stakeholder and public–private alliance against cyber threats and provides ITU's 193 Member States and others with the expertise, facilities and

resources to effectively enhance the global community's capability and capacity to prevent, defend against and respond to cyber threats.

At the same time, as the threats children face online become more complex and multifaceted, the legal, technical and institutional challenges related to the protection of minors in cyberspace are becoming even more global and far-reaching. Building on ITU's Child Online Protection initiative launched in 2008, we urgently need to address the creation of a better and safer Internet world for our children so that they can fully enjoy the benefits of the online experience.

ITU joined forces with the United Nations Offices on Drugs and Crime (UNODC) to collaborate globally on assisting Member States in mitigating the risks posed by cybercrime. The MoU enables the two bodies to work together on providing technical assistance to Member States on cybercrime and Cybersecurity, making available the necessary expertise and resources to facilitate the establishment of legal measures and legislative frameworks at the national level within the principle of international cooperation available for all countries.

In addition, the HIPCAR project — "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" — is one of three regional projects under a broader global initiative being implemented by ITU in partnership with the European Commission. HIPCAR project responds to requests from the Caribbean Community (CARICOM) and individual Caribbean countries for assistance in harmonizing their policies, legislation, regulatory processes and procedures in information and communication technologies (ICT) in order to create an enabling environment that promotes competition and fosters investment and socio-economic development in the region. As a top priority of the project, countries, since 2007, are receiving assistance in ICT policy and legislative framework on information society issues: electronic commerce (transactions), electronic commerce (evidence), privacy and data protection, interception of communications, cybercrime, and access to public information (freedom of information).

ITU, as the sole Facilitator of WSIS Action Line C5 *Building Confidence and Security in the use of ICTs*, is in a unique position to promote international cooperation through the GCA, in collaboration with the UN and industry partners. ITU is already working towards this goal in a number of ways, and it wields the resources and influence required to foster the necessary multilateral support and participation. To continue as well as expand our efforts on cybersecurity, ITU will persistently work to build confidence and trust to ensure a safe, peaceful, and secure cyber environment for all.

THE PERSPECTIVE OF EUROPOL ON CYBERCRIME

ROBERTO FERNANDEZ ALONSO
Europol Cybercrime Centre, The Netherlands.

Europol

Europol is the European law enforcement agency. More than 700 staff at Europol headquarters in The Hague, the Netherlands work closely with law enforcement agencies in the 27 European Union member states and in other non-EU partner states such as Australia, Canada, the USA and Norway.

Europol is a multi–disciplinary agency, comprising not only regular police officers but staff members from the various law enforcement agencies of the Member States and covering specialist areas such as customs, immigration services, intelligence services, border and financial police. One exceptional added value is that Europol helps to overcome the language barriers in international law enforcement cooperation. In practice this means that any law enforcement officer from a Member State can address a request to their Europol National Unit (ENU) in their native language.

Europol supports the law enforcement activities of the Member States mainly against illicit drug trafficking, illicit immigration networks, terrorism, forgery of money (counterfeiting of the euro) and other means of payment, trafficking in human beings (including child pornography), illicit vehicle trafficking and money laundering. In addition, other main priorities for Europol include combating crimes against persons, financial crime and cybercrime.

As Europol officers have no direct powers of arrest, we support law enforcement colleagues by gathering, analysing and disseminating information and coordinating operations. Europol serves as an EU centre of expertise, providing a central platform for law enforcement experts from the European Union countries.

Cybercrime: a growing global problem

With so much of our everyday communication and commercial activity now taking place via the Internet, the threat from cybercrime is increasing, targeting citizens, businesses and governments at a rapidly growing rate. The EU in particular is a key target because of its advanced Internet infrastructure and increasingly Internet-based economies and payment systems.

The scale of cybercriminal activity represents a considerable challenge to law enforcement agencies and the total cost of cybercrime to society is significant. A recent report suggests that victims lose around €290 billion each year worldwide as a result of cybercrime, making it more profitable than the global trade in marijuana, cocaine and heroin combined.

Investigations into online fraud, child abuse and other crimes regularly involve hundreds of victims at a time, and suspects in many different parts of the world. Operations of this magnitude cannot be successfully concluded by national police forces alone. No crime is as borderless as cybercrime, requiring law enforcement authorities to adopt a coordinated and collaborative approach across borders, together with public and private stakeholders alike. It is here that the European Cybercrime Centre will add significant value.

Establishing a European Cybercrime Centre

In response to the European Commission's communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre", the Council of the EU has endorsed the establishment of a new European Cybercrime Centre (EC3) at Europol in The Hague.

The Centre will become the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of cyber attacks. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

The European Cybercrime Centre will be part of the existing Europol structure to facilitate cross working with other crime areas. The Centre, which will be operational by 1 January 2013, will pool expertise and information, support criminal investigations and promote EU-wide solutions.

In addition to the analytical and operational support already provided by Europol, the European Cybercrime Centre will serve as the European information hub on cybercrime, developing cutting edge digital forensic capabilities to support investigations in the EU and building capacity to combat cybercrime through training, awareness raising and delivering best practice on cybercrime. In addition, the Centre will build a community of experts from all sectors of society to combat and prevent cybercrime and online child sexual abuse.

The Analytical Work File AWF CYBORG

The purpose of the file is to support the competent authorities of the Member States, as mentioned in Article 2 (4) of the Europol Convention, in preventing or combating the forms of criminality within Europol's mandate associated with internet and ICT (Information and Communication Technology) related Organised Crime.

More specifically the focus is on the crimes defined in the Cybercrime Convention[1] (Art. 2-8), including but not limited to botnet and malware driven cyber crime, ID theft, e-banking attacks, e-commerce fraud and e-laundering.

The outcome is concrete analysis products and forensic services to:

Add value to existing investigations;
Reflect the current priorities of the members of the Analysis Group;
Provide access to knowledge, data and information.

The new AWF concept foresees the existence of two analysis work files (AWFs) instead of twenty three different files. One focuses on 'serious and organised crime' (AWF SOC) while the other one deals with 'counterterrorism' (AWF CT). Focal Points and Target Groups within these two files provide means to further specify purpose limitation on the level of specific analysis projects.

ICROS

The Internet Crime Reporting Online System (ICROS) will provide centralised coordination of reports of cybercrime from EU Member State authorities.

ICROS is a reliable and compliant platform available to relevant partners in order to share and exchange operational information on internet related crimes.

ICROS will provide support in terms of operational and strategic analysis and analytical results reflecting trends, patterns and emerging threats as input for the prioritization of the law enforcement response.

IFOREX

Internet & Forensic Expert Forum (IFOREX) is a secure environment for Cyber specialists, enabling them not only to share - within their respective communities - knowledge, best practices and non-personal data on Cybercrime but also to host technical data and training for law enforcement.

---

1 Convention on Cybercrime, CETS No.: 185, Council of Europe

ECTEG

The "European Cybercrime Training and Education Group" (ECTEG) was founded in 2007 and it is a law enforcement cybercrime investigation training and education group. ECTEG is an official ad hoc sub group within Europol and is managed by a Board of Law Enforcement officers and a group of special advisors comprising of Police officers, industry specialists and academic experts.

The group has developed, piloted, delivered and distributed 14 accredited cybercrime investigation training modules to police officers throughout the EU.

The membership of ECTEG is comprised of EU member state law enforcement agencies and Europol.

ECTEG has associate members such as; Non-EU Member State police forces, International Organisations and the Council of Europe.

EUCTF

The European Union Cybercrime Task Force (EUCTF) is formed by EU Heads of Cybercrime Units, the European Commission and Eurojust and it was established in 2010 in order to create a platform for managers in cybercrime investigations and prosecutions at Europol. The EUCTF will assist in the development and promotion of a harmonised EU approach for the fight against cybercrime, and to address problems caused by the use of cyber technology for committing crime.

The Computer Forensics Network (CFN)

Europol can provide distance and on-the-spot support to Member States' investigations by forensic analysis of, for example, computer systems and the use of specific laptops and tools to provide on-the-spot computer forensics support.

The CFN is a dedicated network of computers for the pre-processing and analysis of data obtained from digital sources in the framework of an AWF activity.

UFED

The Universal Forensic Extraction Device UFED is a standalone mobile forensic device for use out in the field or in the lab. It extracts data from 95% of all mobile devices, including Smartphone and PDA devices. Data extracted can then be brought back to the forensic lab for review and verification using the reporting/analysis tool.

MONITORING THE STATE AND CIVIL LIBERTIES IN EUROPE

BEN HAYES
Statewatch London, UK

How do we police the Internet?

I deliberately avoided using the word cybercrime in my title, precisely because I think that the focus on crime, and the focus on criminalisation, and the focus on prevention, security, sometimes blinds us to the fact that what we are really talking about is the way that we police the Internet.

It may be extremely complicated, but I think if we start thinking about as a sort of more holistic whole in terms of policing, we can start to see where some of the problems lie in terms of civil liberties, and particularly of democratic control; and I was very pleased to hear Mr. Buttarelli finish by raising the spectre of the role of private industry in all of this, and I'm going to try to add to those concerns with my presentation.

When I talk about policing the Internet, what do I mean? Broadly, as previous speakers suggested, the pillars of criminal law and procedure, and of course fundamental rights and civil liberties. I think it's also important to talk about the imposition of regulations on service providers and Internet intermediaries, because this poses a particular dilemma, I think, in terms of both policing and governance.

In terms of policing the Internet we're also talking about the regulation of technology itself, perhaps that causes us to think slightly differently about this issue. But the reason why I wanted to bring this back to the question of policing is that is with our democratic traditions of course we have an expectation on this state that all the policing work it does will be, as far as possible, open and transparent. Citizens need to know what the police are doing in their name, and it's only with sufficient openness and transparency that we can actually detect possible violations of fundamental rights, and I think that there's so much confusion and, I would say, secrecy and misunderstandings surrounding the way cybercrime legislation and policing techniques are developing that we have a real problem here.

Democratic and judicial control are also fundamentally important, but as previous speakers have suggested, the very global nature of the Internet and the jurisdictional problems are really making traditional forms of democratic and judicial control that much more difficult.

And, finally, accountability and redress. As I said before, without open-

ness and transparency we simply don't know what's going on and without meaningful forms of accountability we can't challenge perhaps where states overstep the mark. And of course without adequate redress mechanisms we can't challenge them at all.

What is cybercrime? I know I don't really need to tell any of you in this room, but one of the reasons why the term perhaps disturbs me a little bit is because it's so extremely broadly defined. Any crime that involves a computer and a network, essentially, and I know there are different definitions within different pieces of national and international legislation, but the sheer breadth of what we have come to recognise as cybercrime is perhaps confusing and also putting legislators in a difficult position.

And what you also see is that a lot of old crimes that really have just been re-hashed as cybercrimes, perhaps because they're perpetrated using new media, but of course we do also see new, specific forms of crime that we hadn't had to deal with in the past, that obviously do require new methods and models of policing. So, in terms of methods for policing the Internet, as previous speakers have mentioned, we're really talking about preventive measures, cyber security; how can we make our infrastructures and our networks as safe as possible?

And then we're talking about investigative measures; you know, in the event of actual crimes being committed, how do we ensure that the police have all the powers that they need to bring the perpetrators to justice?

The previous speaker mentioned data retention. It is simply a fact that without some form of data retention we're not going to be able to conduct these investigations. The worrying trend that we have is the way that the bar has been set so high in terms of data retention in European countries.

Blanket surveillance also appears to be a core model in terms of cybercrime policing because without the surveillance not just of Internet usage but of customers and of the use of certain websites and communication technologies, again we lack the powers to intervene as we need to.

The problem that we have –and I'll come on to this later- is that we seem to be harmonising surveillance and law enforcement powers at what we might call the highest common denominator, and then when it comes to thinking about fundamental rights, these are getting added on and due to the difficulties in getting agreement on these issues in international *fora*, we then see a lowest common denominator approach to fundamental rights.

I also want to talk about the new investigative agencies that are being set up to combat cybercrime. They're being set up all over the world with mandates that police agencies have never had before, yet the information about their methods, their activities, what they're doing on a day-to-day basis is really still shrouded in secrecy, and I don't think the public are yet aware, or I don't think

we've introduced, as yet, the proper forms of accountability that we need for these new cyber police bodies.

One of the most interesting thing, certainly from a criminological perspective about the cybercrime paradigm is that you're really talking about a public-private partnership in policing, and this changes the way we think about regulation and accountability.

This is not new, there is a huge privatisation going on across all coercive functions of our states, you know there's massive privatisation, the homeland security boom post 9/11 has seen private companies enter the sphere across the realm of policing, and as our former EU commissioner for Justice and Home Affairs said: "Security is no longer a monopoly of the public administrations but a common good for which responsibility and implementation should be shared by public and private bodies alike."

But there are differences in the way public bodies approach policing and the way private bodies approach policing, and we need to bear those in mind as we try to negotiate the contours of cyber-criminality.

This public-private partnership obviously also creates huge dilemmas for both states and corporations. As we all know, the Internet is largely - though not fully - managed by private companies, and dilemmas arise when states make demands on most companies on the grounds of national security or law enforcement, particularly because those demands impact directly on the fundamental rights and freedoms of individuals as well as on the technologies themselves. I think perhaps most important thing, and certainly for the ISPs and the Internet intermediaries is that they're getting demands from both democratic countries and from repressive ones. They're getting demands for legitimate purposes and demands for what are certainly, under international law, illegitimate purposes.

I was at a meeting last week at Google in the UK and there were all the major ISPs –Google, Facebook, Yahoo and so on- and really, I think is what you're going to start to see is those companies making demands on bodies like the European Union to help them deal with requests that they're getting from what they see as repressive regimes, because they're really trying to negotiate this sort of complex path.

I don't know if any of you saw recently that Google has taken a decision to publish the number of requests for surveillance or for information that it gets on a state-by-state basis, and the rationale behind this is that: "well, if we as Google can show that there are huge differences between the way different countries are approaching Internet surveillance, then perhaps we can work towards a more level playing field. If country A is making 100,000 demands and country B is making 200 demands, then the chances are that there is perhaps a problem in the way policing is done in country B as compared to country A."

I think that ISPs need to be given help in how to deal with all of this.

I also want to talk about accountability regulation and transparency. You know Iwork for an organisation like Statewatch; when I started there in 1995, police accountability was a huge issue and I'm happy to say that the British police are fairly accountable, they're fairly well regulated and they're a model, perhaps, for other jurisdictions in the world.

When you start talking about accountability, regulation and transparency in terms of corporations, a slightly different set of criteria emerges. Corporations aren't accountable to the public, or accountable to the law in quite the same way as police agencies have evolved to become. Private corporations are working for different aims in different situations.

GCHQ, the Government Communications Headquarters, is probably the biggest spying inception of communications, electronic eavesdropping centre in the world outside the United States. GCHQ is part of our security and intelligence services, but because it has a national security mandate it's exempt from data protection law, it's exempt from freedom of information law, and in terms of public accountability it's extremely difficult to work out what this organisation is up to on a day-to-day basis.

If we start thinking what these different sets of stakeholders -companies, governments, police agencies, citizens, civil society- actually want, and then look at really the direction of travel over the last few years, even the last decade, then some of the problems that we need to address will emerge. Obviously, private companies of course they want security for their customers, they want security of their business, infrastructure, they want to protect their market share, they want to protect the technologies that facilitate their business, they want to protect their content, they want to enforce their intellectual property rights… but of course the bottom line is that they want to continue to make money. They want to commercialise the Internet, they want to protect commerce. There are companies that act very responsibly and companies that I'll come on to later, that act extremely irresponsibly. But this commercial dynamic that underlies private sector involvement creates its own set of problems.

Corporations also want a level playing field. Google, Facebook, whatever, they're subject to broadly a framework for data protection, and a framework for data retention, but the actual mechanisms, the means of implementation have been left to the 27 member states and are for all intents and purposes subject to 27 different sets of regulations.

So, obviously their agenda is really "come on, let's just have single points of contact for things like blocking, single points of contact for things like lawful access requests." But when you start doing that kind of harmonisation, if indeed this is the road that the EU goes down, that the UN goes down, obviously we have this competing tension that I mentioned before in terms of "Do

we harmonise police powers at the right level? Do we harmonise fundamental rights at the right level?"

What do corporations want? The corporations also want to set the agenda increasingly, they want to set the political agenda to suit their own purposes and when I was invited to this conference, the first thing I did was look through the agenda to see which private companies would also be addressing you this weekend and this would be… I've probably been to 30 or 40 conferences like this. I can honestly say, would be the first conference I've been to without industry represented.

I was invited to speak at the Polish presidency's Data Protection Conference several months ago and on every single panel bar one was a private company. I asked the organisers "look, these kinds of events, they didn't use to be like this." And the organisers said to me "Look, as soon as a conference like this is publicised we get phonecalls, e-mails, every single day, you gotta have us on panel, you gotta have us on a panel."

I'm not saying, not even for a second, that those companies don't have a huge amount to bring to the table, but I think we also need to understand the dynamics driving their desire to shape the agenda. And I just pulled out a conference there, "Cyber defence and network security", the only cyber conference incorporating militaries, critical national infrastructures and big businesses at the highest decision-making level. I would say there is now a revolving door really between the security industry and the people tasked in countries with protecting law and order. And because of the commercial pressures under which some of these companies operate I would argue that this is capable of having a corrosive effect on a democratic decision making.

What do governments want?

Of course, they want to protect their citizens, they want to protect the infrastructure, they want to appear tough on crime, of course they do, they want to reassure the public, and they also want to address harmful content and illegal content.

And I think this is where two of the biggest dilemmas we've had around cybercrime have arisen over the past 5 years and more.

Oink file sharing music site was closed as a result of a criminal investigation into the identities and activities of the site's users. And I think we can expect to see these kinds of notices popping out more in the Internet in the coming years despite the very sound arguments about the rationale behind blocking, the effectiveness of blocking and so forth and I won't go into those now.

So, governments not only want to crack down on illegal content, they want to crack down on harmful content. And what I've done there [ ] is just search Facebook for an organisation called Muslims Against Crusades.

Any people from Britain in the audience? Maybe you know, there's a

group called Muslims Against Crusades, it's a group of about 5 to 10 people and whenever there's, like, the royal wedding or remembrance day parade they come along, they burn the flag, they have banners… whatever, they've just been prescribed by the UK under the Terrorist Act 2000.

The UK has now instructed Facebook to block the Muslims Against Crusades' webpage, so now when I search for Muslims Against Crusades I get to see all the people who were calling for the ban on this group but I don't actually get to see what the group was about. If you are curious about how this debate finished, you can see all these Facebook pages calling for the ban. Well, anyway, the irony is if you're in France or if you're in Italy or if you're in Germany you can see the Muslims Against Crusades webpage.

What else do governments want? Obviously they want greater powers over the Internet to deal with law and order situations, to deal with emergency situations and I'm sure that the riots in the summer in Britain this year made the news all over the world.

And one of the things to come out was: to what extent was the use of social media behind inspiration for the riots? So, as soon as the riots were over, there was David Cameron coming out and saying "Look, you know, we need to close down social networks in times of law and order crisis." And they talked about specifically closing down Twitter in that instance. A week later, China came out and applauded the UK on this tough stance against social networks, and a day later the UK government came out and said "Oh, we were just floating the idea, it was something we were never going to do anyway."

The irony in all of this debate is that the UK government actually does have the power to shut down websites, it has had that power since the Civil Contingencies Act 2003 was adopted. So, if in times of emergency, which is, as it happens, extremely broadly defined, the government has the power to take out a communication network, a transport network, whatever it may be.

What do law enforcement agencies, what do security agencies want? They want access to data, we've talked about that, but they also want broad powers and, dare I say, they also want minimal regulation. The amount of times that I've heard that data protection is a burden for law enforcement agencies.

Of course regulation of the public services creates a burden, but you know, if we're going to have respect for our fundamental rights then we need to make sure that we scotch these arguments about regulations being a burden.

What do citizens want?

I don't think you can say what citizens want. They just want a safe, secure Internet experience; and there's lots of different citizens out there who want to use the Internet for lots of different things. But I think pluralism, diversity, democratic values are the things that should be guiding us here.

Human rights: we've talked about the right to privacy, we've talked

about the right to data protection; it's also important to think about freedom of expression, the right to non discrimination, property rights, the protection of human dignity, the rights of the child, and perhaps for me what I think is the most important test, that any measure we adopt has to be necessary and proportionate in a democratic society; and I for one don't believe we've adequately struck that balance over the past ten years.

Then you have a sort of mass digital rights movement, with a different set of demands. They want the right to anonymity, they want the Net to stay neutral, they want to resist commercialisation, they believe in Internet freedom.

I'm not sure if the Internet can be free; I think people must be free, and content must be free and ideas must be free, but we also want good governance. I think that the idea that the Internet can and should remain free is a moot point; what is important here is the quality of the governance around it.

I think we're also in the midst of a bit of a moral panic about cybercrime, which kind of entwines with the sort of curious politics of fear, that doesn't always make for the best legislation. It doesn't always make for level headedness.

We're constantly being told that cyber attacks are rising by 100%, 600%, 1000%, this year there were X amounts of hundreds of thousands of cyber attacks. What do we mean by this? Is this just talking about some spam filter, just picking up some malicious e-mails? I think we really need to have some reliable, accurate, qualitative data about the real prevalence of cyber criminality.

Anonymous has really changed the rules of the game.

Chinese cyber attacks on the rise, left-wing extremist cyber attacks on the rise, attacks on critical infrastructures on the rise.

We need to have some real level-headedness about where the threats are and how best to approach them.

What about the cybercrime legislation that has been adopted over the past decade? Narrowly defined criminal defences are the sign of a flourishing democracy. But the tendency we've seen certainly within the European Union is that when we've chosen to harmonise criminal offences across Europe, we've tended to go for broader definitions just really to allow the differences that we have in the 27 legislative contexts. We have a provision in our Terrorist legislation that says you can be in prison for up to 7 years for possession of any article that could be used for terrorist purposes –undefined, any article.

We've just launched a new cybercrime strategy in this past week in Britain, and really what it does is confuses national security, ordinary crime and what we might consider as low-level crimes, and we get this kind of slippage. So we say "ok, we're going to spend £650m on cyber defence over four years. Fine, we're going to set up a cyber security hub, and this is going to be a specialist unit in our national crime agency." But then we listen to the Whitehall of-

ficials telling you what's going on, and it's "we will create a hub with GCHQ" that is the [intelligence] agency I mentioned, in the middle of it.

Creation of new cyber agencies: who are they? What are they doing? How are they regulated? Are they under adequate control? Are they publicly accountable? What about redress and defence rights?

All these things appearing all over the world. What are they doing? I look at their websites, I don't know, I can't understand it.

What do we see in the GCHQ? In the UK cybercrime strategy, we see GCHQ again to start working with British firms to offer expertise in cybercrime. Fine, it makes sense, of course, they're going to be the best people in the country at doing this stuff, but again we've got this kind of nagging doubt about whether an entirely unaccountable security agencies – this is an intelligence service - is the right body to be shaping a national policing strategy.

If you are charged with a cybercrime offence in Britain and you go to court, you will receive a dossier from the Forensic Telecommunication service, that will set out whatever is needed in terms of cyber for the trial, whether it's interception of communication, location, tracking, decoding, inspections etc.

The trouble is in Britain we've privatised the forensics science service, and our Forensic Telecommunication Service is a private company. Why does this matter? I'll come on to it. The cyber security market - here's a thing saying its worth $55 billion between 2010-2015, that's the US market, compound annual growth rate of 6.2%.

Who profits? Security defence and IT companies are all over this stuff. As one of our… director of one of Europe's arms companies said, in the wake of 9/11, "I see a shift in emphasis and an increase in imbalance in what is defence and homeland security. Security is a more politically acceptable way of describing what was traditionally defence."

I'm going to give you a quote by Naomi Klein now, because I think it really sums up, at least for me, my concerns about all this stuff.

"In just a few years, the homeland security industry, which barely existed before 9/11, has exploded to a size which is now significantly larger than either Hollywood or the music business. Yet what is most striking is how little the security boom is analysed and discussed as an economy, as an unprecedented convergence of unchecked police powers and unchecked capitalism, a merger of the shopping mall and the secret prison." And you can agree or disagree with this analysis, but I think Naomi Klein is right when she says this changes the values of a culture; it creates an incentive to spy, torture, generate false information, but it also creates a powerful impetus to perpetuate the sense of peril that created the industry in the first place, and this is my perhaps biggest bugbear with the security industry, it's that they are embroiled in the politics of fear to the extent that.

Yesterday, Privacy International launched Big Brother Incorporated, partly in response to the events of the so-called Arab spring, when it was clear that surveillance technology, public order technology, whatever, equipment made in Europe was being used by certain oppressive regimes to brutally repress people on the streets of North Africa and the Middle East.

There's going to be litigation very soon, litigation against European companies providing interception, location, tracking facilities etc to the repressive authorities. This is worse than a breach of privacy, this is complicity in international crime in my mind, and this is what this litigation is going to seek to expose, but the point in bringing this in, and this was exactly the point made by Mr. Buttarelli; these private companies developing the tools for cyber defence, surveillance of the Internet, or whatever, they're selling them on the open market, they're selling them to governments, but they're also selling them to private investigators and they're also selling them to extremely repressive regimes.

There's a huge lacuna in European law: you can't export any equipment that could be used for torture, under the EU's Torture Directive, you cannot export arms to countries that might use them for internal repression, but there was nothing at all under current law to stop you exporting social network analysis tools, data-mining systems, backdoor Trojans, whatever, to some of the most repressive regimes on the planet. So there's a huge problem there.

CYBERSELFDEFENSE AGAINST CYBERCRIME

MIGUEL ONTIVEROS ALONSO
Director of the National Institute for Criminal Science of Mexico, (OAS) Mexico

Before I begin speaking about the harmonisation process in Latin America, specifically in Mexico, I would like to mention something related to what Marco have said about the child exploitation; with this audio and voices it possible to hear about children being abused.

There is a great problem with child exploitation in Mexico. Mexico is the number one State, together with Spain, that produces child pornography in the world, to the point that UNICEF and the ILO have helped us making important reforms about this situation in Mexico.

This hypothesis of Marco about the victims, the children victims of exploitation, is already a punishable conduct in Mexico, but unfortunately this is just stated in our Federal Penal Code, –we have one Federal Penal Code, a Military Penal Code and 32 Penal Codes, one for each Mexican State-. The Federal Penal Code refers to this conduct as simulated exploitation, simulated pornography. Among the conducts that may include this hypothesis, is when there are videos where people who are not a child, dress like a child, or when someone uses images of non-real people –like Mickey Mouse or very well-known figures for children- having sex. These conducts are punished in Mexico, as simulated child pornography.

There are only two things that worry us in Mexico and in Latin America about the harmonisation process. First what we have done to harmonise our legislations, not only with regard to cybercrime, but with respect to all crimes in our countries; second, what we have not done and what we would like to do in the next years.

Clearly, this topic is very discussed in Latin America. In Mexico many congresses take place and many documents are produced on the subject. Incidentally, 3 years ago a major congress with the Max-Planck-Institute, with Professor Sieber, with Jan-Michel Simon, about the unification of the legislation in Latin America took place.

However, today there is no longer talk about unification, because it is perceived as both for Mexico and for the Latin American continent.

Today we talk about the harmonisation of our legislations, and we have made some progress about this theme and particularly about cybercrime.

I do agree, of course, with what has been said about the problem with cybercrimes; the fact that when we talk about cybercrime we are not just speaking about computers, but we are also speaking about protecting human rights, and specifically, child human rights. This is the reason why these topics are extremely important for us in Mexico. As mentioned above Mexico is together with Spain the world's number one producer of child pornography and victims of child.

We are conducting a dialogue with governors and legislators about this harmonisation process. We have already stressed the fact that by achieving the harmonisation of the legislations on cybercrime we are not only protecting the victims, but the economy as well.

Unfortunately, we do not have the support of our governors - we have 32 governors in Mexico -, because they feel they may lose power when they are not able to decide which conducts can be considered a crime, and which others cannot. They want to always decide in their small territories within Mexico and feel that they have the power and sovereignty over their states. In my opinion this is a mistake, a big mistake.

As already mentioned, this harmonisation process is a constant issue in the discussions in the academia, and in our justice congresses in Mexico. Through this process we have reformed many laws in Latin America, not only the criminal law or the penal codes, but also the civil, mercantile, administrative and the taxing law as well. They have a lot to do to protect the information, to protect the economy and to protect human rights of a country.

Indeed, we are making some progresses in these areas, but the progress in the criminal law area is going through a little bit slower.

There are some countries that have done these reforms, such as Bolivia, Cuba, Chile, Ecuador, Mexico, Peru, Paraguay and Uruguay. The Convention is our guideline; it contains the principles to reform our legislations, even if we have not signed it yet or we have not officially recognised it.

What have we done in Latin America to answer these questions? The most important point in this respect, even if we do not have this harmonised legislation in Latin America, we have harmonised our workshops and the way we teach, the way we prepare our lawyers, our prosecutors, our judges, our police officers; and the guidelines are the Federal Penal Code and the Convention. Therefore our operators in the justice system know what should be, even if they do not have it in their own law.

The countries I just named –I mean Chile, Cuba, Ecuador, Mexico, Peru, Paraguay and Uruguay-, have recognised the most important cybercrimes. Thus, there are some ways to go ahead and not to stop this harmonising process in Latin America.

Most Latin American countries have not officially recognised this Con-

vention, but they work in the universities, they work in the police institutes and they work in the prosecutors' institutes with this instrument as a model.

Main problems to harmonise the Latin American legislations against cybercrime

The most important problem we have suffered from in Mexico, is the lack of an institution that takes the leadership and works for a compromise in order to guide us through this process of harmonisation. Sometimes we copy what is done in Europe - yes, actually we copy it and we discuss it -, but there is no leadership. No institution has enough leadership and recognition to guide us through this harmonisation process.

Actually the harmonisation process, specifically regarding cybercrime, is not a real criminal policy in Latin America and particularly in Mexico.

There is no criminal policy in Mexico, we have enormous problems and the government has focussed its power on those problems. I am referring to the drug problems and the big power of cartels that live, work and commit crimes in Mexico.

So, we focus on organised crime but we forget that the organised crime works, as well, with cybercrime.

The reason why it is good news that UNICEF and the United Nations have worked greatly in Mexico, is because these organisations have done very good efforts to harmonise some legislations. In fact, the most harmonised legislation in Latin America is on the protection of child rights against trafficking in persons, against child pornography and against sexual tourism.

Another problem with the harmonisation of legislations in Latin America, is that some countries have not reformed their criminal or penal codes, but they have constructed laws for cybercrimes; this is a problem in Mexico, too. We have not reformed our penal code and we created new laws that are criminal laws, but they are not penal codes.

This is also the case of Chile and Venezuela, i.e. the countries that had preferred to make law against cybercrime. Other countries, such as Argentina, Ecuador, Mexico and Peru, have only incorporated the cybercrimes into their penal codes.

In fact, in Mexico there are 34 penal codes and there are about 50 laws, which contain all types of crimes. Therefore it is almost a impossible to find out how many crimes you do have in Mexico –we actually don't know it.

Another problem is that in Latin America there are two different legal systems: most of the continental countries, and a few more from the Caribbean region, have a system based on Roman and Germanic influence, while all the

Caribbean countries are based on common law. This is another major problem we face in trying to harmonise the cybercrime legislations in Latin America.

Yet another problem in America, is the lack of a general agreement about cybercrime, similar to what exists in the European Union. We have your model, and that is something very good for us.

Criminal law has a very special meaning related to the sovereignty and the independence of the country. Consequently, our country perceives itself as independent when it creates its own criminal law. This is a simulation?? I think, in each state, because the objective of criminal law is not the independence of a country, but the protection of the most important interests of the people. Sadly, this is not the criterion used by the governors in our countries, in Mexico and in Latin America.

We have about 34 penal codes in Mexico. I am not aware if there is another country with as many penal codes in the world. Out of these 34, only 7 – the federal code and another 6- have incorporated correctly cybercrimes in their text. The other ones are not really harmonised with the Convention that its at our disposal.

Proposals

We are willing to continue working to harmonise our legislations in Latin America and in Mexico, but at the same time, as we have seen in the last years, the unification is not possible; the harmonisation of our legislation is going to take time. We are working on developing another instrument that can help to protect the information, that can help to work together in Latin America and that does not need an instrument to go through the legislative process, which is very slow in our countries.

These instruments are protocols, forensics models, and legal frames. Legal frames or model frames that we can use to work, and we teach our prosecutors in our institutes, we teach our police officers, our cybernetic polices, that we do have in Mexico, with these instruments, and of course with our penal code.

Another thing we have already harmonised is the education model, or the formation model for the justice operators in our countries.

In Mexico we are talking about harmonising the legislation, but also we talk about harmonising the formation of the operators, the police officers and the prosecutors. What we are trying to do in Latin America is that all the prosecutors and police officers work with the same methods, even if they do not have the same laws or harmonised laws in Latin America or in Mexico. And we have done very important efforts and reached results working this way.

At the INACIPE, the national institute for criminal sciences in Mexico, we are developing studies about cybercrime. We have been working for 2 or 3 years on this topic with one or two researchers from our institute. Moreover we have these conventions and these agreements with other institutes in Latin America. We are trying to export these models of cooperation to Latin America even without the harmonisation of our legislations.

We are working at the same time harmonising and making these protocols to work together. We are very worried about what is happening in Latin America, in particular about organised crime, which is an unprecedented large scale problem, this violence and this way of making crimes. However, we know that the harmonisation of our legislations and the cybercrime will help us to fight against these cartels and all these criminal phenomena that are related to the web.

Printed by
DIGITAL TEAM – Fano (PU)
on behalf of
Fondazione Centro nazionale di prevenzione e difesa sociale/CNPDS - ISPAC
Piazza Castello, 3 – 20121 Milan, Italy
November 2012