**LEGAL**
An interview with Peter Sommer, a pioneer expert witness in cybercrime and complex digital evidence cases.

**DATA PROTECTION**
Giuseppe Corasaniti, Magistrate specialized in computer crimes talks about the implementation of the 2001 convention on cybercrime in Italy.

**TECHNICAL**
How do different governments control our access to web contents? A study of government filtering of online content by Joan Tous, a forensic analyst at Cybex.

**LAW ENFORCEMENT**
Syrus Abubakar explains the services that IMPACT offers law enforcement bodies on the fight against cybercrime.

**INSTITUTIONAL**
The Council of Europe details its actions for fighting against Cybercrime through an article by Cristina Schulman

**JURISPRUDENCE**
The cases noted in this issue all relate to the various issues arising from digital evidence. Understanding the nature of digital evidence can be complex, and it is essential to ensure digital evidence specialists understand what they are doing when investigating a case, and for the layers to be sufficiently knowledgeable to ask the specialist witnesses the correct questions.

**EVENTS**
Selection of conferences for the months of August and September 2009 that might benefit to lawyers, prosecutors, technitians, judges, computer forensic specialists, law enforcement bodies or any person that deals with cybercrime and electronic evidence.
INTRODUCTION
The "Electronic Newsletter on the Fight Against Cybercrime" (ENAC), a Cybex initiative cofunded by Cybex and the European Commission’s Directorate General Freedom, Security and Justice within the framework of the Criminal Justice 2008 JPEN Programme, remarks its international status reaching the five continents.

LEGAL
“Cybercrime happens in an instant!”
Interview with Peter Sommer • Visiting Professor at the London School of Economics

DATA PROTECTION
“Implementation of the 2001 convention on cybercrime by Italy with transposition into law no. 48 of 18 March 2008”
Giuseppe Corasaniti • Magistrate - Public Prosecutor’s Office of Rome, District Group for computer crimes

TECHNICAL
“Government filtering of online content”
Joan Tous • Forensic analyst at Cybex

LAW ENFORCEMENT
“IMPACT - Introducing the world’s first public-private partnership against cyber-threats”
Syarisa Abubakar • Director of Policy at IMPACT

INSTITUTIONAL
“Council of Europe measures for fighting against cybercrime”
Cristina Schulman • Programme Manager for Cybercrime at the Council of Europe

JURISPRUDENCE
Netherlands - Voorzieningenrechter In Kort Geding (Services Court Judge Amsterdam) Norway - Borgarting Appelate Court
Singapore - Public Prosecutor V Neo Khoon Sing [2008] SGDC 225
Poland - Sad Najwyzszy Rzeczypospolitej Polskiej (Polish Supreme Court)
United States of America - United States Court of Appeals, Ninth Circuit
Russian Federation - Arbitrazh Court of Moscow

EVENTS
Conferences, events, trainings and seminars related to cybercrime, electronic evidence and computer forensics.

EDITORS
Introduction of the team of seven editors that has been engaged to create the Electronic Newsletter on the Fight Against Cybercrime, each one being an expert on the ENAC Section of which they are in charge

DISTRIBUTOR PARTNERS
To ensure the widest possible distribution of the Electronic Newsletter on the Fight Against Cybercrime, the ENAC relies on the collaboration of Institutions and Organizations who will distribute the e-Newsletter monthly to their contacts database.
The newsletter against cybercrime (ENAC) displays its international status reaching five continents.

The successful launch of the first issue of the ENAC increases the number of collaborators around the world.

On July 1st, the ENAC team launched the first issue of the Electronic Newsletter on the Fight Against Cybercrime, a Cybex initiative cofounded by Cybex and the European Commission’s Directorate General Freedom, Security and Justice within the framework of the Criminal Justice 2008 JPen Programme. This monthly and free electronic publication is addressed to judges, technicians, lawyers, specialists in forensic analysis of digital devices, human resources directors, law enforcement bodies and anyone handling electronic evidence and seeking the prevention of cybercrime.

At present, the ENAC published in Spanish, English and Russian, has been downloaded in Asia, Africa, Oceania, America and Europe, highlighting its international nature and the interest awoken in this subject around the world.

Owing to the successful first issue, several institutions and companies, both Spanish and foreign, have requested to become partners of the project, offering even greater dissemination for this second issue.

In this second issue, the ENAC team wants to give special recognition to the project partner thanks to whom the Russian version of the ENAC is possible; the International Training and Methodology Centre for Financial Monitoring (ITMCFM).

Mr. Alexndr Batalov, General Director of the ITMCFM stated the following:

"The ITMCFM is happy to contribute to the ENAC. In the modern era of rapidly developing information technologies, countering cybercrime gains high relevance and importance. New tools should be introduced to fight various forms of electronic crime and the ENAC provides a truly comprehensive and effective platform for worldwide cooperation of experts in this field*.

We truly appreciate your support!
Enjoy the read,

Mrs. FREDÉSVINDA INSA
Project Director
finsa@cybex.es

Mrs. MIREIA CASANOVAS
Project Coordinator and Chief Editor
mcasanovas@cybex.es

Cybex
Plaza Cataluña 20, 9ª floor · 08002 · Barcelona · España
tel. +34 93 272 20 41 · fax. +34 93 215 50 72

Go to Russian version of the ENAC
Go to Spanish version of the ENAC
Peter Sommer is a Visiting Professor in the Information Systems Integrity Group in the Department of Management at the London School of Economics and also a Visiting Senior Research Fellow, Faculty of Mathematics, Computing and Technology, Open University. He is one of the world’s pioneers of digital evidence / computer forensics and has acted as an expert in many important criminal and civil court proceedings.

His first degree was in law and in the course of a long professional career has carried out many post-incident investigations, acted as risk analyst for leading insurers and loss adjusters and acted as an expert witness in many leading criminal and civil trials involving complex digital evidence. Case-work has included charges of high-value fraud, industrial espionage, defamation, theft of intellectual property, software counterfeiting and piracy, global computer misuse, large-scale distribution of paedophile material, multiple murder, narcotics trafficking and terrorism. He is a former Parliamentary Specialist Advisor and sits on a number of UK Government Advisory Panels. www.pmsommer.com; www.pmsommer.net

ENAC: You started working on cybercrime, providing computer-related expert witness and digital forensic services in 1985, what is the most important evolution you have noticed in the international scene?

Peter Sommer (PS): The most important change is the arrival of an international treaty, the Cybercrime Convention promoted by the Council of Europe. Its importance lies in the fact that its signatories include countries that are not European, like USA, Japan, Canada and South Africa.

This treaty takes some of the major categories of cybercrime and defines them. Individual countries undertake to see that they have their own local versions. Harmonised definitions of crime are a pre-requisite of mutual legal assistance and extradition, because the courts in the country receiving requests will only do so if there is a very similar law in their own jurisdiction. The same applies to rules for collecting and sharing evidence; another pre-requisite in cybercrime which very often moves seamlessly across national borders.

ENAC: Do you consider the Cybercrime Convention is enough as legal tool or do you think legislators should go further?

PS: The most important step is to get many more countries to sign after it.

But the law and any of these international conventions merely provide the framework for something to happen; you still need the active willingness to co-operate.

ENAC: Cyber investigation requires great international cooperation, what is your perception on current rules for international cooperation among enforcement and judicial authorities?

PS: Despite the fact that my first degree is in Law, or perhaps because of that, I am sceptical about the fact that simple passing of laws is all that you need to do. You have to look at the way of how individual law enforcement officers work together and the quality of their training.
It does not matter what the law says...

The formal procedures of Mutual Legal Assistance Treaties (MLATs) can be quite cumbersome; typically a front-line investigator has to go up his line of command; some at the top involves lawyers, who draw up papers, which then get transmitted via quasi-diplomatic channels to a high official in the jurisdiction from where assistance is being sought. That high official then needs to relay the needs down to the front-line law enforcement people in his country. By that time much of the potential evidence will have disappeared, because cybercrime happens in an instant!

In practice, if the respective law enforcement officers know each other, perhaps from conferences or training schemes, what happens is that officers will collect and freeze evidence for their overseas colleagues on a contingency basis, and then release it once the formal paperwork has been sorted out. They may even assist their superiors so that mistakes in the formal procedures are spotted early. Everything depends on countries wishing to cooperate with each other. My observation is that the main category in which is very easy to get cooperation is related to child sexual abuse, trafficking, and indecent images of children, because this enjoys pretty near universal revulsion.

If you start looking thinks like fraud, when you try to pursue cyber fraud taking in one country, attacking people in another country, you find that the level of cooperation drops dramatically because in effect, people do not see the need to pursue a criminal who did not cause any harm to people in their country.

They will say that they do not have got enough resources to handle local crime, let alone worry about foreign victims. That pattern tends to be repeated once you get outside of a scope of a European mutual support scheme, for example if somebody in my country approaches the Russian or the Bulgarian authorities, then on the whole, they do not got very much support because these two countries have huge law enforcement issues anyway.

ENAC: Which is your perception on the current role of European structures and policies on cybercrime?

PS: Although I am not anti-European, in relation to cybercrime I am very sceptical about the value of tackling things at a purely European level, because cybercrime tend to be International, so I am not personally convinced that organisations at European level as the European Network & Information Security Agency - ENISA¹ can add some extra value, except perhaps for training.

There are also limits to the extent to which we can have a worthwhile pan-European approach to law. We have a number of separate traditions in relation to how the law works and also in terms of criminal justice procedure.

For example, in most European countries the law is based on a Code; in England we have what is called the "common law" approach where significant parts of the law emerge through judicial precedent. In relation to procedures: in many mainland European countries the investigation and charging is in the hands of an examining magistrate.

¹ http://www.enisa.europa.eu/
In England investigations are handled by the police and charges are determined by a separate prosecuting authority - the Crown Prosecution Service. And our court procedures are different too, we have an adversarial as opposed to inquisitorial process.

On the other hand all European countries can share certain sorts of general principles and requirements. A good example of that are the various Data Protection Directives and the Directive on privacy and electronic communications\(^2\). You can also have pieces of legislation that works like the Data Retention Directive\(^3\), when all European countries agree that they would retain communication data for a given period - not without some controversial aspects, like how the right period is and the circumstances to retain and when they should be released- but to do something on the grounds of legal systems is running to difficulty.

ENAC: Law enforcement officers are often the first people in contact with cybercrime scenes. How should they understand e-evidence to deal with these scenarios?

PS: One of the discussions is going on here in Britain at the moment is how far you should be recognising a separate category of e-crime or cybercrime police, as digital evidence can be significant in a very wide range of so-called ordinary crime.

In United Kingdom, over 70 per cent of homes have personal computers; 90 per cent of British homes have access to Internet; It is not unusual to find 2 to 3 computers in a very ordinary home plus some older computer lying around because they are obsolete. They all contain digital evidence! And can be involved in cybercrime or in ordinary cases.

I have been involved as expert in very high profile cases which do not appear at first sight to have much to do with cybercrime. For instance, in one case - people trafficking- 58 Chinese illegal immigrants were found dead in the back of a truck. The case was not a cybercrime case, but there was digital evidence. I did another case, when a whole family was murdered by a career criminal. It was not central but there was also an amount of digital evidence found on a computer allegedly used by the ring-leader. Most of us know of the use of botnets in which many innocent computers are taken over by criminals and then made to mount co-ordinated “distributed denial of service” attacks on victims who are then made the subject of extortion demands - “Pay us a consultancy fee and you will get your website back”. In the UK although we could prosecute this as a cybercrime, in practice it will get treated as “blackmail” or “extortion”.

We have had specialist “high tech” crime police since 1984. We now have about 300 across England and Wales in formal high tech crime units. Overall, we probably have 500-600 police officers and police employees who can do high grade computer forensics and investigations - and these are augmented in the private sector.

\(^2\) [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0058:EN:NOT]
\(^3\) [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML]
My experience is that the high-profile cases are investigated and prosecuted to a very standard. However in the more routine cases the quality of work drops dramatically. We recognise that we need many more investigators who understand the basics and can handle the simpler cases. One of their skills, of course would be the knowledge of when to seek the assistance of a specialist.

UK Police are also looking at various triage techniques so that important evidence is identified but they don’t need to examine large numbers of "irrelevant" computers.

A related aim is to ensure that all investigators understand the fundamentals of digital evidence - and also that they receive frequent refresher courses, because the digital world is constantly changing.

The problem is matching the skill resources to the problems.

ENAC: What is your opinion on the need of a Certification/education of experts who give evidence in court? Do you consider that some kind of regulation in this field is possible or desirable in Europe?

PS: The rules for experts giving opinion in court will vary on different countries. One of the worries is that it is all too easy for individuals who know very little to be accepted by the courts as experts able to offer opinions which then influence the outcome of a trial.

In English Law, we use the word ‘experts’ in two ways.

One is for people carrying out a technical inquiry or process: for example making a forensic copy of a disk and then searching it for specific files. These people are essentially skilled technicians and they report to the court about what they did and what they found. The second class of ‘expert’ may be the same but is someone allowed by the court to express an opinion on things that the court would not normally know by themselves.

The danger is really in this second kind of experts. What should be their qualifications? Are the opinions actually right? Is there any range at the Court to check if what I did is right?

The problem is whether we can have a reliable scheme to which potential experts can apply before they are allowed to give opinion-type evidence; or whether their expertise should be tested before the trial starts by the judge.

ENAC: One of the major issues with electronic evidence is its easy manipulability, that is a very recurrent argument in court. However, nobody doubts about the reliability of DNA analysis tools. Based in your experience, what is the ‘remedy’ to deal with this issue?

PS: In English, we have the term 'Continuity of evidence'; in North America they call it 'Chain of custody'. The idea is the same. Everything done within the computer, from the moment it is seize is very carefully documented.

---

Police officers pay attention to the location and decide; they make detailed notes on everything they do, they take pictures, they take videos, they put computers in a bag, the bag is sealed, it goes to a secure location, what we call ‘secure custody’. When it is opened, a forensic image is made... The biggest weapon against an accusation of tampering is to have a reliable and detailed knowledge of the chain of custody.

For this purpose, the ACPO Guide for Computer Based Electronic Evidence[^1] was developed in England over 10 years ago. It has undergone to a few changes and is followed by many other countries. It is a very useful piece of Best Practice when dealing with electronic evidence cases.

ENAC: Finally, what are the challenges you see in the near future in these matters?

PS: For digital evidence, there are 4 main technical challenges. Challenge number one is quantity, The cost of hard disk storage is dropping dramatically. At the moment you can buy an external hard disk with 1 Terabyte (1000 GB) capacity at 100€. This means that law enforcement and experts have to review a lot of data every time one of these devices are involved in a cyber case. Most people have a great deal of data on their computers and it often provides "digital footprints" going back many years. The good news is that there is much potential evidence which may assist any enquiry. The bad news is the time and effort required to examine everything.

The second challenge is the rate of change; In most areas of forensic science the thing you are examining remains static. The human body does not change so much, so DNA is the unique mark. But in this field, we have new hardware and software every 4/5 years. Microsoft will shortly release the latest operating system, ‘Windows 7’. Every time there is new operating system there are new artifacts, new things to think about.

The same is true for new versions of software, new types of software and new things people use computers for, such as social networking, e-commerce, and online gaming Computer forensics engineers have to understand how each of these new things work and also where they might locate configuration and other files which are forensically useful in reconstructing events.

The next element is fragmentation; Years ago, when you had a suspect to investigate, you went to that person’s internet service provider, and they were able to give you (provided you had the necessary warrant) access to the e-mail and so to other records.

Today, you can see ordinary people use one service provider for connection to home for internet, they may be using a web-based email service with a company in another country; they maybe having Website hosting in yet another country, they may belong to several social networks and to a number of Peer to peer (p2p) file sharing sites, all with different companies in different countries.
But, in order to be able to build up a picture of what they are doing, the law enforcement officers have to be able to identify all these people and get to the right authorities to get the records they may be holding.

There is not a great deal that can be done other than to increase police powers to look at the entire data stream of a suspect; so-called Deep Packet Inspection. There are significant legal problems, like privacy, and how it interacts with data protection legislation. But there are also many technical problems as well, for instance, how do you actually carry it out. And the costs will be considerable as well; Taxpayers in every country will have to decide how much they are willing to pay and how much of their privacy they are willing to cede to law enforcement.

The last emerging problem is called ‘fast flux’. We have already spoken of the ways in which sophisticated cybercriminals can easily operate across national boundaries and can hijack innocently-owned computers to mount attacks which disguise the identity of the controlling criminal. But they can now also change rapidly and from moment to moment the apparent places from which attacks are mounted. It makes tracing very difficult.

And all these lead me to conclude that while cyberlaws and cyber police are essential, a large number of cyber crimes will never be "solved" - and there must also be renewed emphasis on assisting potential victims to protect themselves and their computers.
GIUSEPPE CORASANITI
Magistrate - Public Prosecutor’s Office of Rome, District Group for computer crimes

IMPLEMENTATION OF THE 2001 CONVENTION ON CYBERCRIME BY ITALY WITH TRANPOSITION INTO LAW NO. 48 OF 18 MARCH 2008*

A prominent expert on legal issues regarding communications, computer networks and Computer Law. He is the author of numerous papers on freedom and fundamental rights and interactive communication.

He recently played an important role in the debate on the European Directive 1pred2 in respect of criminal measures for protecting intellectual property rights, where he endorsed very critical positions regarding privacy and data protection of European citizens in opposition to extremist stances.

He is a part-time lecturer in computer law at the The Università degli Studi di Roma “La Sapienza” university, Department of Computer Science, Faculty of mathematical, physical and natural sciences; in the past he has also been a senior lecturer for the degree course on mass media law at the Faculty of Law at the Libera Università Internazionale degli Studi Sociali (LUISS-Guido Carli) in Rome.

Convention on cybercrime adopted in 2001 was not a starting point but, rather, represented the point of arrival for a complex legislative course that originated in Europe and, likewise, was defined in Europe, and to which the United States acceded (together with Japan). Obviously, the first testing bench for the Convention is represented by the number (and the calibre) of those ratifying it and it is appropriately this very factor that could be essential for its full implementation.

Besides being an abstract legal tool, the more the Convention represents a set of harmonised rules valid cross-border and the greater the number of States that affiliate themselves with its general principles, then crime will be less likely to flourish by exploiting conditions of invisibility and substantial immunity which, to date, have been maintained due to international sensitivity on the issue.

* Original article language: Italian. The original article may be found at the following link
The course for integrating and adapting the Convention to domestic legislation is complex and, at times, problematic (and Italy is certainly no exception to this rule, although it had the advantage of having introduced a number of criminal offences with Law no. 547 in advance in 1993 and, namely, the crimes of illegal access, electronic fraud, data interference and illegal interception, by adapting the general provisions of the Italian penal code and code of penal procedure) and international co-operation requires effective working methods and well-organised institutional figures and entities appointed to apply them and, primarily, awareness of the various implications offered by advances in technologies and by the issues posed in unremittingly respecting fundamental rights (of potential criminals as well as potential victims of crime) with sensitivity and care.

Implementation of the Convention in Italy was achieved with enactment of Law no. 48 of 18 March 2008 that primarily envisaged the adaptation of provisions of the Italian code of penal procedure, and with enactment of Law 231/2001 regulating the liability of entities and legal persons.

Specifically

- Articles 1 and 2 of the Law provide for “full and complete” implementation of the Convention and, consequently, we can hold that, outside of amendments expressly introduced, the legislator has fully adopted all terminology and the statements of principle contained in the European Convention, also in respect of parts not cited and, all the more so, where no significant formal statements are forthcoming on the subject of transposition.

- Article 3 of Law 48 introduces a unified definition of the electronic document, amending article 491-bis of the Italian penal code and acknowledging complete parity of digital and paper documents with regard to the crime of forgery, combining this guarantee for any digital document also to public and private computer documents “having evidentiary validity”; in addition, with the new provisions, a specific crime was introduced (article 495-bis) false statements or certification rendered to the electronic signature certifier on the identity or on a person’s own personal characteristics or those of others. On the same subject of digital signature, Law 48 introduced a new crime under article 5 and provided for in article 640-quarter of the Italian penal code, i.e. a particular kind of computer fraud committed by a person who provides electronic certifying services. If such a person, for the purpose of procuring for himself or others, wrongful benefit or causing damage to others, breaches the obligations provided by law for the issuing of a valid certificate, such person shall be punished with a prison sentence of up to three years and a fine ranging from 51 to 1,032 Euros.

- Article 4 amends article 625-quinquies of the Italian penal code punishing the conduct of any person who illegally damages a computer or computer network system, the information, data or programs contained therein or pertaining to it or abets the total or partial interruption or alteration of its working and who procures, produces, reproduces, imports, distributes, communicates or, in any case, makes equipment, devices or computer programs available to others with a prison sentence of up to two years and a fine of up to 10,329 Euros.
Article 5 of the law reforms the offence of “computer damage” already provided for in law 547/1993 and, specifically, under the new wording of article 635-bis of the Italian penal code, the aggravating circumstance for the offences contemplated in § 2 of article 635-bis numbers 2, 3, 4, 5 and 5-bis disappears, and only number 1 remains regarding damage to a computer system or data with duress or intimidation. The “new” computer damage now covers several references to criminal offences, each associated with an event, specific subject matter and various forms of conduct.

Under article 635-bis of the Italian penal code, the wording specifically refers to damage to information, data and computer programs. Save in cases where acts constitute a more serious crime, whoever destroys, corrupts, cancels, modifies or suppresses information, data or computer programs belonging to others, on action filed by the injured party, is punished with a prison sentence of six months to three years. The circumstance set forth under number 1) of § 2 of article 635 (i.e. duress or intimidation) or, whenever the act is committed with abuse of a system operator’s position, the punishment is a prison sentence of one to four years, with the public prosecution automatically filing the case the case.

The new article 635-quater, likewise, provides for an independent offence of damage in relation to computer or telecommunications and information systems. Save in cases where acts constitute a more serious crime, whoever, by way of their conduct as set forth in article 635-bis, or by introducing or by transmitting data, information or programs, destroys, damages or renders, in whole or in part, computer or telecommunications and information systems belonging to others unusable or seriously obstructs their working is punished with a prison sentence from one to five years.

The circumstance set forth under number 1) of § 2 of article 635 or, whenever the act is committed with abuse of a system operator’s position, the sentence is more severe. § 2 and § 3 of article 420 of the Italian penal code have been abrogated (that provided for the crime of “computer attack” in 1993) while, for combating crimes that damage the State, public agencies or services that in any case are of public utility, article 635-ter has been introduced to the Italian penal code that provides for damage of information, data and programs used by the State or by another public agency or in any case of public utility.

Save in cases where the acts constitute a more serious crime, whoever commits an act directed at destroying, corrupting, cancelling, altering or suppressing information, data or programs used by the State or another public agency or pertaining to them or in any case of public utility, is punished with a prison sentence of one to four years. Whenever the act causes the destruction, corruption, cancellation, alteration or suppression of information, data or computer programs, punishment is a prison sentence from three to eight years.
The circumstance set forth under number 1 of § 2 of article 635 is referred to or, whenever the act is committed with abuse of a system operator’s position, the sentence is more severe. For damage to a computer system or a telecommunications or information network reference is made, instead, to article 635-quinquies that provides that, whenever an act is directed at destroying, damaging, rendering, in whole or in part, computer or telecommunications and information systems of public utility unusable, or seriously hinders their working, punishment is a prison sentence from one to four years. Whenever the act causes the destruction or damage to the computer or telecommunications and information system of public utility or, whenever these may be rendered, in whole or in part, unusable, punishment is a prison sentence of one to eight years. The circumstance set forth under number 1) of § 2 of article 635 is referenced or, whenever the act is committed with abuse of a system operator’s position the sentence is more severe.

Criminal liability of legal persons has been amended under article 7 in respect of computer crimes committed in their interest or for their benefit by introducing a provision (Article 24-bis) to Legislative Decree no. 231 of 8 June 2001 referring to computer crimes and illegal data processing. In relation to committing the crimes provided for under articles 615-ter and 617-quater, 617-quinquies, 635-bis, 635-quater and 635-quinquies of the Italian penal code, a pecuniary sanction is applicable to the entity ranging from a hundred to five hundred so-called quotas. In relation to crimes committed, provided for under articles 615-quater and 615-quinquies of the Italian penal code, a pecuniary sanction is applicable to the entity of up to three hundred quotas. In relation to crimes committed, provided for under articles 491-bis and 640-quinquies of the Italian penal code, except where provided for in article 24 of the Decree, for cases of computer fraud perpetrated against the State or another public agency, a pecuniary sanction is applicable to the entity of up to four hundred quotas.

Very important changes have been introduced by article 8 of the Italian code of penal procedure. Specifically, investigative tools for gathering evidence. For the first time the Italian legislator appears to have given dignity to the normal techniques of computer forensics for investigating and collecting digital evidence. Whenever inspections concern digital evidence, the judicial authorities may order, pursuant to article 244 of the Italian code of penal procedure, all technical operations “also in relation to computer or telecommunications and information systems, by adopting technical measures directed towards ensuring the conservation of original data and preventing that said data may be altered”.

During the course of searches, pursuant to amended article 247 of the Italian code of penal procedure, whenever there is reason “based on grounds to believe that data, information, computer programs or evidence in any case pertaining to the crime may be found in a computer or telecommunications and information system, even when said systems are protected by security measures, a search may be ordered, by adopting technical measures directed towards ensuring the conservation of original data and preventing that said data may be altered”.

The ENAC project is funded by the European Commission’s Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008.
On the basis of the "new" § 2 of article 248 of the Italian code of penal procedure, «papers, documents and correspondence and, likewise, data, information and computer programs at banks» may be examined. In the case of being caught in the act of committing a crime or, whenever the circumstances and conditions exist, article 352 of the Italian code of penal procedure, as amended by Law no. 48, authorises the officers of the Criminal Investigation Department, by adopting suitable technical measures for the conservation and prevention of any alteration, may search computer or telecommunications and information systems, even when these are protected, whenever there is reason to believe that these systems conceal data, information, computer programs or evidence in any case pertaining to the crime and that may be cancelled or lost.

Article 353 of the code of penal procedure has been amended under § 2 with the addition of the wording: «and the ascertaining the content», while under § 3 after the wording «the other objects of correspondence», «also whenever in electronic form or forwarded using electronic mailing systems» has been added, and after the words: «postal service» the following wording has been introduced: «telegraph, computer and information or telecommunications».

Under § 2 of article 354 of the code of penal procedure, after the first paragraph, the following wording has been added «In relation to data, information and computer programs or information and telecommunications systems, officers of the Criminal Investigation Department shall, likewise, adopt technical measures or shall give any instructions necessary for ensuring the conservation and prevention of data alteration and access and shall provide, whenever possible, for their immediate duplication using suitable supports, via adopting a procedure that ensures conformity of the copy with the original and that said copy cannot be altered in any way.». Also seizure of correspondence has undergone substantial amendment: § 1 of article 254 has been replaced with the wording: «At the facilities of those who provide postal, telegraphic, computer and information networking or telecommunications, seizure of letters, parcels, packages, valuables. telegrams and other correspondence, even if forwarded using computer and telecommunications systems, which the judicial authorities may have grounds to believe as having been sent by the accused or which have been addressed to him, also under another name or via another person or, that, in any case, may be connected to the crime»; likewise, under § 2, where it is provided that Criminal Investigating Officers are prohibited from having knowledge of the content, there is the further addition after the words «without opening them» of the offence of alteration.

Furthermore, a new and essential investigative instrument has been inserted and, namely, the seizure of computer data at providers of computer, information and telecommunications services (article 254 of the Italian code of penal procedure). The judicial authorities, on ordering seizure at providers of computer, information networks and telecommunications services of data held by these, including traffic or data located there, may establish, for requirements linked to the normal provision of said services that data be acquired by copying on a suitable support, using a procedure that ensures conformity of the acquired data with original data and that data cannot be altered in any way. In this case, however, the service provider is ordered to «conserve and suitably protect the original data». 
Those persons who are bound by professional privilege (the clergy, lawyers, the police, technical consultants, notary publics, health professionals and operators, etc.) or by virtue of their office (public officials, state employees and providers of public services), as a result of amendment to § 1 of article 256, may be ordered to hand over documents and, likewise, data, information and computer programs, also “as copies of the same provided on a suitable support”.

In addition, new provisions concern computerised custody of seized or acquired data. «Whenever custody concerns data, information or computer programs, the person in charge of custody is, likewise, duty bound to prevent alteration or access by third parties, unless, in the latter case, otherwise ordered by the judicial authority. Article 260 of the code of penal procedure concerns putting seized items under seal and has undergone the following amendments: Under «with other means», the wording «also of an electronic or computer-based nature» has been added and under «Whenever data, information or computer programs are involved, a copy shall be made using suitable supports, adopting a procedure that ensures conformity with the original and ensuring copies may not be altered in any way; in such cases, custody of originals may be ordered in places other than clerk’s office or secretariat».

• Law 48/2008 also amended – under article 11 - the code concerning personal data protection (Legislative Decree 196/2003), by introducing a new paragraph under article 132. Specifically, it concerns «The Minister of the Interior or, on his authority, the persons in charge of central specialist departments for computer or telecommunications crime in service with the State Police, the Carabinieri and the Finance Police, as well as other subjects indicated under § 1 of article 226 of the enabling instruments, co-ordination and transitory procedures of the code of penal procedure contained in Legislative Decree no. 271 of 28 July 1989 may order, also in relation to requests made by foreign investigative authorities, providers and computer and telecommunications service operators to conserve and protect, according to indicated methods, data regarding network traffic and, however, excluding the content of communications, for the purpose of preliminary investigations provided for under the above cited article 226 of the legislative provisions of Legislative Decree no. 271/1989 or for the purpose of ascertaining or repressing specific crimes, for a period that shall not exceed ninety days.

This order, which may be extended, for justified reasons, for a total period not exceeding six months, may provide for special data custody procedures and the possible unavailability of the data in question at providers and computer or telecommunications operators or third parties. 4-quarter. The provider or computer or telecommunications operator receiving the order provided under § 4-ter must comply with the order forthwith, providing the authority making the request with assurance that the order will be obeyed.

The provider or computer or telecommunications service operator is under a duty to keep the order received secret and confidential and, likewise, the resulting activities expedited for the period indicated by the authorities. In the event of breach of this duty, except where acts may constitute a more serious crime, provisions of article 326 of the penal code are applicable. 4-quinquies.
Orders adopted pursuant § 4-ter are notified in writing without delay and, in any case, no later than forty-eight hours from notice being served on the recipient to the public prosecutor at the place where the order is to be executed, who, where the circumstances shall not be enforceable. “In caso di mancata convalida, i provvedimenti assunti perdono efficacia”.

- Under article 11 jurisdictional competence for computer crimes has also been redefined by introducing a substantial amendment to article 51 of the code of penal procedure, as occurred for terrorism, with the addition of «Whenever proceedings for crimes, whether actually committed or attempted are involved, as set forth in articles 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter and 640-quinquies of the penal code, the functions indicated under § 1(a) of this article are assigned to the public prosecutor’s office at the court of the provincial seat of the district where the competent judge is in residence». In practice, district sections are set up for this purpose for computer crimes for the public prosecutor’s office.

- Under article 12 the National Centre for preventing child pornography on the Internet is financed and provided for under article 14-bis of Law no. 269 of 3 August 1998, while the security structure and the normal provision of telecommunication services for requirements in relation to computer protection of computerised critical infrastructures of national interest was introduced by article 7-bis of Law-Decree no. 144 of 27 July 2005, converted into law, with amendments, as Law no. 155 of 31 July 2005.

- Article 13 of the law identifies in the person of the Minister of Justice, the central authority as defined pursuant to article 24, § 7, and article 27, § 2, of the Convention also designates the Minister of Justice. Article 27 provides that each Party designates a central authority in charge of forwarding and replying to requests for mutual assistance, for executing these requests or forwarding them to the competent authorities to be executed. The central authorities must communicate directly with each other.

These functions appear to come under the competence of the Directorate of criminal justice within the department for legal affairs pursuant to article 4 of Presidential Decree no. 55(2) (b) and, specifically, within the scope of international co-operation activities – whether prosecution or defence - with regard to criminal law, in the correlated processing of cases concerning orders regarding criminal matters for which the Minister has competence; in international relations regarding criminal matters and, specifically, in the preparatory study and elaboration of international conventions, as within relations with the European Union and with the United Nations Organisation, as well as the other international institutions for the prevention and control of crime.
The assignment of tasks to the Minister of Justice appears also to set the course for steps for specific arrangements in the future that are destined to establish efficient and permanent co-operation with the Ministry of the Interior, with the intersecting role played by both the judiciary and the investigative police departments involved, with the aim of promoting their actions and rendering co-operation and information exchange more effective. The Minister of the Interior, together with the Minister of Justice, has to identify the 24/24 point of contact as provided under article 35 of the Convention.

The tools made available today could reveal themselves as being totally insufficient, given application that is either too strict or that sides excessively with the advocate and defender of civil liberties.

It is nonetheless true that also with regard to this aspect, the methodology for comparison and exchange is similar to the one that the Convention advocates as the basis for the co-operation that has just been set up and which could reserve positive and significant new developments not only from the standpoint of exchange of cases between the various institutional figures involved, but also and, more importantly, for adapting the requirements of the various criminal legal systems, and all its provisions, in a harmonised framework of substantial guarantees; as we have seen, this issue will, the first instant, progressively be defined in Europe institutional seats.

Looked at from another angle, it is just such tools as stability and on-going international co-operations and, as a result, the definition of harmonised procedures and figures qualified to talk to each other institutionally, exchanging not only data but operational recommendations and tangible investigative experiences that paves the way for spontaneous regulation of cyberspace, exactly as was seen for acts of aircraft hijacking or for international terrorism. An initial criticism of Italian implementation of the Convention can be summed up in failure to have introduced specific implementation of the legislative provisions as expressly defined by the Convention (and, it should be added, even further expanded and underscored in the framework decision that obliged States to adjust and conform no later than 16 March 2007).

The chosen line, that maintaining the legal system within the well trodden path of the Italian penal code and code of penal procedure and, above all, to maintain the system in some way as being capable of being traced back to the 1993 legislation, a line of action expressly acknowledged when the legislation underwent parliamentary review, may appear somehow easier, but which, at the same time unhatches very sensitive issues in relation to the adequacy of existing sanctioning and process machinery in relation to the complexity of inspections as in the case of the need to expedite the same in a much shorter time frame and with suitable guarantees.
It is possible, nonetheless, to hold that just such an acknowledgement for implementation that the ratifying law introduces, works somehow not only from a formal standpoint as a limited tool for introducing into our legal system, with well identified provisions but as a general acknowledgement of the fundamental principles that the Convention advocates, and, thus implicitly transposing into our legal system, also substantially, those guidelines, in establishing significant legal assets as in identifying application of its provisions, aware of the existing implications of the need for the rapid ascertainment of crimes and protection of interest which may often be constitutional of all subjects involved, needs that only a suitable technical verification can render compatible, first by identifying the technologies used and identifiable techniques and, then, moving on to the communications network used and methods for accessing the system or for data extraction actually found.

In substance, the main problematic issue has not so much to do with the abstract assumptions of the criminal action that can be brought via the non uniform acquisition of evidence of computer crimes for which proceeding have been initiated, but rather for the need to harmonise significant conduct that is under investigation in an objective framework that can be identified in a territorial context that is incredibly vast and diversified.

So, then, a very important window is opened for international co-operation and, European co-operation in particular, that can play an extraordinary role through meetings and exchange between operators, exchange with companies involved (in the first instance telecommunications industry operators and providers of interactive on-line services) and a harmonised approach to legitimate requests via targeted and not mass use of investigative tools.

Section Editor: Mrs. Elena Domínguez Peco

This section will expose the different realities regarding the data protection policies in different countries. You are welcome to collaborate in the development of the section or give us your opinion by contacting the Editor.
GOVERNMENT FILTERING OF ONLINE CONTENT

1. Introduction

Online content filtering can be exercised by any of the entities within a final user and the web server hosting the content. Companies routinely restrict access to certain web contents in order to improve productivity and to protect themselves from lawsuits or complaints due to the possible improper use from part of their employees. Also, public institutions usually limit the contents accessible to the general public when they provide open connections and educational institutions are even required by law to ensure that minors are protected from harmful web contents on their premises.

All those situations have something in common: the user is free to use a personal network connection in order to access the Internet without being subject to those restrictions. However, in some countries access to certain web contents is restricted for a number of reasons. The present article seeks to explain how this control is exercised, mentioning the techniques used, the types of filtered contents and also some of the consequences of those filtering mechanisms, including available evasive techniques. Some examples involving specific countries are mentioned, with no pretension of exhaustivity, to show representative cases and to illustrate the current status of this matter around the world, although the Chinese example will be predominantly used, as it is the most paradigmatic and combines all the filtering techniques that are described in this article.

Online content filtering or censorship is not conceptually different from other types of censorship, but presents some technical difficulties derived from the decentralized nature of the Internet: this network was specifically designed so that the information between two nodes could follow multiple paths, which makes the setup of a central filtering infrastructure quite difficult. On the other hand, even when authorities can legally impede the hosting of specific web contents in their respective countries, those contents can be migrated to a server physically located in another country in a matter of minutes; and if contents are considered legal on that country, or it is difficult for any reason to contact its authorities and request their removal, the only resort left for a government that wants to prevent access to them by their citizens is to implement some kind of filtering system. It is therefore important to distinguish the legal prosecution of illicit web contents (with the intent to permanently remove them and possibly to prosecute their authors or distributors), from the simple filtering of contents, which only has the effect to prevent or make it difficult for users to access them. The present article covers the second approach.
2. Types of filtered contents

The motivation for censoring online contents range from the efforts to protect the victims of a crime from the harm that the continued availability of contents pose to them (as in the case of victims of child sexual exploitation, or the victims of any other type of abuse) to the wish of limiting the freedom of expression and impede access to political contents. Also, the protection of economic interests, mainly related with multimedia content distributed without the authorisation of the rightholders but also with applications like VOIP that pose a threat to local telecommunication monopolies, and are consequently blocked in countries like UAE (United Arab Emirates)\(^1\), is often a matter of concern.

Governments that impose a strict control over contents on traditional media are also the most restrictive when it comes to deciding which web contents are forbidden by law, blocking access to them and controlling who tries to access them. Those countries are predominantly concentrated in three world regions: East Asia, the Middle East and North Africa, and Central Asia\(^2\). But even though those are the most active countries when it comes to limiting the access to online information, lots of countries try to block access to sensitive contents, like child pornography or pages hosting malicious software - or at least are considering it - using the very same techniques that other countries use to place limits on the exercise of the freedom of expression via web. Those techniques are described below.

3. Filtering techniques

Internet is open by nature and it facilitates the dissemination and permanence of contents, which makes the placement of limits on the information that users can access a quite complex task.

Two different approaches provide the means to filter the web contents that are made available to final users: ISPs providing Internet access to those users can be requested or required by law to implement the necessary filtering mechanisms, or alternatively a filtering infrastructure can be deployed on strategic points that connect national networks with the international backbone, which constitutes a kind of virtual border. The latter option has been chosen by countries where the deployment of telecommunication networks has been carried out, or strictly supervised and controlled by the State, and foreseeing from the beginning the need to impose a certain degree of web content filtering. Among those countries, the most shining example is the famous Chinese “Great Firewall”: In that country, all the network infrastructure providing international connectivity is owned by Government-owned or controlled organizations, like the Ministry of Information Industry (MII), China Telecom (the public telecommunications company) and ChinaNET (the backbone operator), which provides an absolute control over communications with external networks, and having ISPs operate solely as licensees of that infrastructure\(^3\). The existence of a central filtering infrastructure results in homogeneous criteria all over the country, in contrast with what usually happens when filtering responsibilities are delegated to ISPs, which may technically implement in different ways a common set of filtering criteria.

---

1. Web: http://opennet.net/studies/uae
2. An excellent compared study of the situation in different countries is “Access Denied: The Practice and Policy of Global Internet Filtering” (2008, MIT Press), by Ronald Deibert, John C. Palfrey, Rafal Rohozinski. Moreover, Journalists Without Borders (http://www.rsf.org) has an updated list of countries considered “Internet Enemies” (currently twelve) that describes the filtering and censorship practices of each one of them.
The recent decision of the Chinese government to force every computer manufacturer to preinstall a program called "Green Dam/Youth Escort" whose function was to filter online content raised many concerns over those manufacturers, and that decision was finally and indefinitely postponed. That program was developed by two Chinese companies called Jinhui Technology and Dazheng Language Technology and contained essentially the same filtering functionality that commercially available products had been offering for years, but obviously adapted to the configuration parameters set by the Chinese government. Even though that was a unique initiative, not currently being used in any other country, it could become the start of a new trend on the control of web contents. Other recent examples of the forced installation of software in user devices, not specifically related to web filtering but interesting nevertheless, are the recent push of a Blackberry firmware upgrade by the local telecommunications operator in the UAE" or a request by some German authorities of legal authority to install trojans to intercept communications in the computers used by suspects.

But content filtering usually occurs at a network level, before contents arrive to the computer of a final user, and are based in some kind of black list of forbidden resources, which may be IP addresses, domain names or keywords, as we will explain in detail.

3.1 IP address-based blocking

This blocking method consists on denying access to a list of IP addresses that have been marked as forbidden. It is the most primitive and simple to implement, since it does not require a significant economical investment in specialized equipment (due to the fact that only TCP/IP headers must be examined) and it has virtually no impact on network performance, which makes it a good "emergency" measure for situations where an ISP or authorities wish to immediately block access to a specific resource. For this reason, blocking the IP address or addresses where some contents can be found is often the first method to be adopted, before evolving to more sophisticated and expensive solutions.

The main drawback of this approach is its low degree of granularity, since it does not allow to selectively filter only some parts of a website. For example, in the case of search engines and huge repositories of information like online encyclopedias, it is not possible to hide or block only specific results and entries: a decision has to be made between allowing unlimited access to the whole site or fully blocking it. Besides, in the case of different websites sharing a single IP address (mainly small sites using shared hosting services), if a block is set on one of them it will also apply to the rest. One example of the impact of this approach is that an offending blog hosted on Blogger could result in the blocking of all blogs using that publishing service. Another disadvantage of this technique is its low effectivity against sites that use a pool of IP addresses to distribute the load between different servers, or sites that deliberately change their IP address often with the purpose to evade IP blocking in a transparent way for the final user. But even being this simple and rudimentary, this technique is widely used by ISPs, organizations and countries all over the world, specially to block known sources of malicious software and spam.

---

4 Source: http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc
5 Source: http://news.bbc.co.uk/1/hi/technology/813576.stm
One way to evade this kind of restrictions is to use a web proxy, asking a server from a foreign country to act retrieve the desired content and forward it to the final user. These servers are used by ISPs and corporations to speed up the delivery of static contents to multiple clients, and also to filter which contents can be delivered (more about that later), but the use of a proxy whose IP address is not blacklisted also constitutes a very easy way to evade IP blocking. A simple Google Search using the terms “free open proxy” will find many servers that can be used for this purpose, some of them being made available for free in the name of the freedom of expression, others providing free tools but trying to sell access to more advanced functionality and also many others acting as a proxy as a result of a misconfiguration or with the intent to intercept valuable information, like user credentials and credit card numbers.

3.2 Domain-based blocking

An evolution of the described blocking method is to use the domain name as the filtering criteria instead of using the IP address, which makes the filtering more precise and does not affect legitimate domains sharing a hosting provider and an IP address with blacklisted ones. However, this method still forces to choose between entirely blocking or allowing access to each domain name.

The most common way of implementing this type of restriction is to alter the way DNS servers work, making them return incorrect results that point to an error page - or simply no results - for forbidden resources.

One country opting exclusively for this type of control is Germany, where a recent law forces ISPs to block DNS queries for a list of domain names that the authorities will keep updated, in an effort to quickly impede access to child pornography contents as soon as they are identified. Other countries like Australia, United Kingdom and Norway also use DNS blocking. In most cases, when a user asks for the IP address of a balcklisted domain name, the DNS server will return the address of a static web page warning them of the nature of the requested content, and technically there’s also the possibility that DNS servers keep track of the IP addresses of all the users that have requested that content.

The easiest way to evade this kind of blocking is to configure the computer to use a DNS server located in another country and not subject to restrictions, like OpenDNS.

3.3 URL-based blocking

A more advanced blocking method is to examine the complete URL that has been requested and decide if access is allowed or forbidden based on more complex rules, which makes it possible to deny access to certain parts of a website only. Technically, this filtering method is usually implemented by setting up a web proxy, transparent or not, of compulsory use, and blocking all attempts to retrieve web contents that do not go through that proxy. Since this proxy becomes the only source of web contents for all users, it is easy to create rules that control its behaviour depending on the requested domain, page or even parameters.

---

7 Legal text: http://dip21.bundestag.de/dip21/btd/16/128/1612830.pdf (in German)
8 Example: http://kid.telenor.net/ (Noruega)
9 Web: http://www.opendns.com
For example, it becomes quite easy to block online searches using Google or any other search engine when they contain blacklisted keywords, since search terms appear as GET parameters in the URL that gives access to the results.

Several commercial solutions implement this technique, mainly designed for corporate environments but also used by some governments for the massive filtering of web contents, some of them being McAfee SmartFilter o Fortinet Fortiguard. An important drawback is the significant amount of information that has to be processed and served, which makes it important to set up an adequately dimensioned infrastructure to prevent it from becoming a “bottleneck” slowing the navigation experience of all users.

This restriction can usually be evaded using open proxy servers, as it has already been described, or using any other server capable of retrieving web content and serving it back, like the Google cache or translating services like Google Translate.

3.4 Keyword-based blocking

The previously described methods are based on extensive lists of specific forbidden resources, which must be manually maintained and will obviously never include all existing contents of a specific category, given how fast and easily new contents are made available on the Internet. To overcome this, some products examine the full content of web resources before they arrive to the final user, and intercept them if they contain any blacklisted keyword. This technique requires what is known as “Packet filtering” or “Deep Packet Inspection”, because all transmitted data packets must be examined.

This approach will tend to block more contents than intended, for example preventing access to educational contents on reproductive biology because they contain terms usually associated with pornography, so it is usually used in combination with “white lists” of trusted domains, and where keyword-based restricciones do not apply. The main disadvantage though, is that it requires a great amount of processing power, making it technically and economically unfeasible to analyze all traffic (besides, it is highly redundant in the case of static contents that can be retrieved thousands of times each day) so countries like China use this approach in combination with the other techniques, using it as a source of information to generate automatic rules setting blocks on IP addresses or URLs, so that aside from impeding a specific communication, static rules for blocking the offending contents are created on-the-fly and applied to all traffic. Another way of reducing the impact of this thorough exam is to make it in a parallel infrastructure, allowing normal arrival of contents to the end user instead of holding them until they have been examined. Only if their examination reveals the presence of forbidden terms, and provided the necessary infrastructure is in place, TCP/IP packets can be injected to abort the connection and prevent the content from reaching the final user.10

The most effective method to evade this, and any other kind of control, is to use a VPN connection that creates an encrypted secure channel between the final user and a remote server, that will in turn retrieve the requested content and seive it back. That way, none of the intermediate nodes can see the actual content of communications. The only way to ensure that this is not a feasible way to evade the filtering is to examine all internet traffic and discard everything that can not be processed by the filtering equipment, including encrypted data. However, since many companies rely heavily on this technology for their operations, the great economic impact that such a measure would have is taken into account, and encrypted communications are not filtered, thinking that the majority of the population does not have the necessary knowledge or resources to use this evasive method. To this effect, many commercial services offering encryption solutions specifically designed to evade government filtering are available.

Other similar technologies used to evade all the described filtering mechanisms are Tor\textsuperscript{11} and FreeNet\textsuperscript{12}, which hide the specific activities of a user in such a way that the only available information is that a user is communicating with a node belonging to these networks, being impossible to determine the specific contents that are being transmitted.

3.5 Alteration of search results

Instead of -or besides- implementing mechanisms that block access to contents, another possibility is to ask search engines to remove illegal or undesired content from their search results. Usually, those contents are also filtered using some of the described techniques and this elimination seeks to hide the very existence of censorship activity. This elimination of results, carried out by all major search engine in countries like China, has generated ample criticism on part of civil right organisations.

4. Transparency and information to the end user

Aside from the used technique, a distinction can be made between countries that opt for transparency in their filtering and control, informing the user that a requested resource is forbidden and in some cases offering a way to suggest the revision of filtering criteria, and those who redirect or filter without any explanation.

In the case of China, no explanation is given when a content is blocked, and users simply receive a technical error like “The connection can not be made” or “Timeout exceeded”\textsuperscript{14} in an effort to hide the filtering and to prevent the users from looking for ways to evade them. The opposite approach can be found in countries like Saudi Arabia, which in spite of being among those that filter a wider range of contents, does so with a message telling the user the motives for the block and even providing a mechanism to ask the authorities to reconsider the ban\textsuperscript{15}.

\textsuperscript{11} Web: http://www.torproject.org/
\textsuperscript{12} Web: http://freenetproject.org/
\textsuperscript{13} Source: http://www.chnw.org/reports/2006/china806/index.htm
\textsuperscript{14} Source: http://chinayuwen.com/2009/01/22/1354
\textsuperscript{15} Fuente: http://opennet.net/studies/saudi
In any case, the full content of black lists with the resources that will be filtered is not generally available to the public or any regulatory body, which sometimes results in the abuse of a system exclusively conceived with a specific purpose, like the filtering of sexual images of minors, for other purposes.16

5. Concluding Remarks
Government initiatives to filter web contents have increased in the last years and will probably continue to do so, even though users with a minimum of knowledge can elude them quite easily. Content filtering is currently the subject of an intense debate among those who advocate a stricter regulation of the Internet and civil rights organisations, which have found in new social agents like the Swedish Pirate Party an ally in their fight to keep an Internet true to their anarchic origins.

---


Section Editor: Matias Bevilacqua

This section will focus on the technical side of cybercrime and electronic evidence. The reader is highly encouraged to contribute to this section. Given the technical complexity rating system used, we are open to divulgative introduction articles on technology, state-of-the-art white papers and everything in between. Please contact the Editor if you’d like to contribute to this section.
SYARISA ABUBAKAR
Director of Policy at IMPACT

IMPACT - INTRODUCING THE WORLD’S FIRST PUBLIC-PRIVATE PARTNERSHIP AGAINST CYBER-THREATS

We live in a world that has become used to spectacular and daring acts of conventional terrorism. But, as with the world around us, terrorism, and the threat it poses, is constantly evolving. We understand the power of the bullet and the bomb but now we also face exposure to a new, complex and potentially devastating form of terror-cyber-terrorism. IMPACT is a newly formed international organisation established to respond to these threats and can offer law enforcement a wide variety of services likely to be of assistance when conducting global cyber investigations.

As readers of this article are well aware, many ICT systems-in both the public and private sector- face daily threats from hackers and their bot net armies, some millions of computers strong, bombarding scanning and probing websites and other communication channels. For the most part, the probes come from criminal gangs’ intent of stealing identities, credit details, passwords and other information they can turn to financial gain. As well as groups of so-called black hats trying to break-in simply for the thrill and kudos for breaching multi-million dollar security networks.

But as the coordinated attack on Estonia’s cyber-infrastructure in March 2007 showed, these same skills can be used for political purposes, to create a breakdown in a country’s social and economic fabric. That attack proved very publicly that cyber terrorism is not a game, not a hoax, and that these nightmare scenarios are a very real threat.

This is why it is essential for governments worldwide to do more than ensure their citizen’s physical security. There is an absolute need to come together and share the information and resources that will also guarantee their cyber security.

With dozens of international bodies and organizations jostling for position and power in the cyber security sector, the problems of legal jurisdiction and national interest are equally boundless. Yet, as systems and software become ever more complex and connected, allowing hackers to breach so-called ‘soft targets’ and find a back door into more crucial and secure systems, the race to find a coordinating body becomes ever more desperate, and the need to cooperate across borders and jurisdictions increases.
Joining forces

Clearly, governments cannot contain the threat of cyber-attackers by domestic measures alone. Without expert collaboration and knowledge sharing, individual countries lessen their ability to respond to cyber attacks, as well as exposing other countries to even greater risks as cyber attackers learn to exploit nations’ ICT weaknesses one-by-one.

No single government possesses all the expertise to counter cyber terrorism. The talent pool of experts needed to meet disparate threats is dispersed across the globe, and in most instances, it is to be found in the private sector and academia rather than government hands.

The ability to quickly contain and learn from cyber attacks is critical if damage is to be limited and the threat to other nations reduced. However, governments generally hesitate to collaborate with other governments on security related matters, thus increasing risks to all.

A Global Coalition-The Founding of IMPACT

IMPACT, the International Multilateral Partnership Against Cyber Threats is the first global public-private initiative allowing countries of the world to interact among themselves together with the global private sector and academia. Its International Advisory Board reflects this aim and comprises some of the most renowned experts from industry and academia.

Members of IMPACT’s advisory board include Eugene Kaspersky, founder and CEO of Kaspersky Lab; Mikko Hypponen, Chief Research Officer of F-Secure; Howard Schmidt, former White House Cyber Security Advisor; Dr. Vincent Cerf, Google’s Chief Internet Evangelist and H.E. Dr. Hamadoun Toure, Secretary-General of the International Telecommunication Union (ITU). The board advises IMPACT on key issues, allowing the day to day running of the organization to be conducted by its Management Board along with its International Secretariat which includes highly placed and qualified cyber security personnel from around the world.

As a not-for-profit international organization, IMPACT is strategically positioned as a politically neutral platform to foster collaborative partnerships between nations and the commercial and government sectors. IMPACT acts as a forum that enables all member countries to collectively take a global leadership role in the interest of their national cyber-security.
Inspired by the Centre of Disease Control and Prevention (CDC), IMPACT seeks to offer the global community the best brains and the best facilities to complement the nations of the world to counter cyber threats. IMPACT is inclusive in its outlook and actively pursues joint efforts with other public, private and academic organizations that share similar core objectives of protecting and defending against the common threats of cyber attacks. These types of collaborations can take the form of:

- Jointly organized activities
- Information sharing
- Training
- Utilisation of common facilities
- Sharing of resources

**Partnering with the ITU**

In September 2008, IMPACT signed a Memorandum of Understanding (MoU) with the International Telecommunications Union under the terms of which IMPACT’s new state-of-the-art Global Headquarters in Cyberjaya, Malaysia will be used to operationalise the ITU’s Global Cybersecurity Agenda (GCA). The GCA is a “framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society”.

The Agreement will see ITU and IMPACT collaborating closely to increase security and confidence in the use of ICTs globally. Leveraging on the facilities and best practices of both organizations, the GCA will provide:

- Real-time analysis, aggregation and dissemination of global cyber-threat information
- An early warning system and emergency response to global cyber threats
- Training and skills development on the technical, legal and policy aspects of cyber security
- Advisory services to national governments on the technical, legal and policy aspects of cyber security

**IMPACT’s Services and Tools for Law Enforcement**

IMPACT is built on four key dynamic pillars. Each focuses on specific functions designed to increase the world’s capacity to quickly identify, monitor, respond to and secure against the spectre of cyber terrorism and are organized into specific functional centres.
Global Response Centre

The Global Response Centre (GRC) is IMPACT’s first line of defense against cyber threats and is designed to be the foremost cyber threat resource centre for the global community, providing early warning networks as well as coordinating worldwide resources and personnel and channeling them towards areas of incident.

Indeed, information is the key to detecting and monitoring cyber-threats around the world. One of the major issues confronting the cyber security community is not that there is too little information in the cyber security arena, but too much. Addressing cyber terrorism for example is about having access to the right information at the right time. Currently, the information is duplicated across numerous information channels. With some information in government hands and some in private hands, the filed lacks the kind of effective collaboration channels that can bring governments together to pool their expertise and share their resources. IMPACT’s GRC is the first dedicated body to address those international strategic and structural weaknesses.

Specifically, it is mandated to:

- Build expertise and become the leading cyber threat resource for global cyber community
- Establish and maintain a comprehensive database of international experts who can be called into service at short notice
- Facilitate and coordinate a swift response to threats and the sharing of available resources to assist its members during emergencies
- Serve as a central, trusted partner in security incident reporting and analysis.

While its primary role is threat analysis, the GRC is not simply for emergencies. It provides members with an ongoing value package that includes:

- 365/24/7 NEWS early warning and threat detection system
- Sample submission and analysis
- Daily security briefs, updates and announcements
- Documents library
- Forum for discussion
- Best practice guidelines for adoption and analysis

The GRC is the centrepiece of IMPACT’s imposing seven-acre Global HQ in Malaysia. Inside the GRC is a crisis room, state-of-the art IT and communications equipment, a Security Operation Centre that will be operating 24 hours a day, 365 days of the year plus facilities for its shift workers, an onsite broadcasting centre, viewing gallery and a fully-redundant secure data centre. Whether as a means of case generation, investigative support or cyber incident monitoring, law enforcement officials can benefit from access to the GRC which will provide a variety of useful tools (including malware analysis) to help security officials respond to various cyber threats.
Centre for Policy & International Cooperation

One of the trends in cyber threats undertaken by cyber criminals has been to set up base in countries the necessary legislative or regulatory framework to bring them to justice. Therefore, an international consensus is required to close down loopholes, strengthen law and infrastructure and direct resources to where they are most needed to prevent cyber attacks from gaining a foothold in any country.

Many countries have already done a good job in ratifying their template of laws. IMPACT, while respecting the need for different cyber security definitions and frameworks among its members, believes that such measures are essential to prevent the creation of safe havens for cyber criminals.

As a neutral entity, IMPACT recognizes that there are already organizations that are better placed to deliver sanctions and other actions towards countries or organizations and so maintains an inclusionary policy of dialogue between all its members. Issues of national security and intelligence sharing are often raised, but IMPACT firmly believes that the sharing of cyber security information can only lead to a safer and more harmonious environment that is better able to respond to isolated or concerted acts of cyber attacks.

Currently, the Centre for Policy & International Cooperation is working with numerous partners at national and international levels, such as Interpol, the EU, the COE and the ITU to formulate new policies and harmonize national laws to tackle a variety of issues relating to cyber threats.

In the very near future, the centre will also provide advisory services to member governments on policy and regulatory matters, and share its wealth of data and experience in the cyber security arena to ensure that they are able to implement functionally effective anti-cyber threat laws and frameworks.

With the use of extensive facilities at its Cyberjaya HQ and resources like the GRC, the centre will be able to foster international cooperation through meetings, and plenaries that make use of IMPACT’s far-reaching infrastructure.

Centre for Training & Skills Development

The Centre for Training & Skills Development is where IMPACT’s unique mixture of national governments, global enterprises and world leading academia comes to the fore. It will conduct highly specialized training, host seminars and other activities for the benefit of member states. Relevant commercial and academic enterprises currently spend billions of dollars each year on research & development (R&D). This gives them a unique understanding of technology trends and valuable insight when it comes to anticipating and predicting the future cyber threat landscape: information that is invaluable when shared amongst IMPACT members, the governments of the world.
Many of IMPACT’s key partners, among them Symantec Corporation and Kaspersky Lab, have taken an unprecedented step and pledged to make their CTOs, CROs and other in-house experts available to a one-of-a-kind IMPACT high-level program that will address present and future cyber threats at ministerial level and beyond. These closed-door, cross-industry briefings will give IMPACT members invaluable exposure and privileged insight from the private sector in terms of the latest trends, potential threats and emerging technologies. These sessions will develop into an important forum where leading private sector companies can share constructive ideas and best practices with IMPACT member governments.

In addition to these high-level sessions IMPACT will conduct world-class cyber security training in the form of specialized seminars and workshops throughout the year. To ensure that the highest levels of training and information are delivered, IMPACT is collaborating with a series of globally renowned partners, among them the SANS Institute, EC Council, the Honeynet Project and more with a view to supporting the IMPACT objective of capacity building. One such project with SANS Institute is aimed at assisting the nations of the developing world to secure and upgrade their cyber infrastructure and to introduce them to some of IMPACT’s global best practices. This is aimed at shutting the door on the creation of so-called safe havens for cyber criminals in countries that lack the necessary infrastructure or legal framework to bring them to task.

All of these activities benefit from the comprehensive training facilities housed in the IMPACT Global HQ in Cyberjaya. These include specialized training rooms, auditoria, the GRC’s Security Operations Centre, labs, on-site accommodation facilities, IMPACT’s fully-equipped data centre and the other modern amenities needed to support high-tech specialized training programs. IMPACT welcomes proposals from law enforcement entities around the world to take advantage of these facilities and jointly offer training of use to the law enforcement community.

Centre For Security Assurance & Research

In partnership with leading ICT experts, IMPACT’s Security Assurance Division is formulating a checklist of relevant global best practices with a view to establishing an international benchmark of specific relevance to governments. On request, IMPACT’s Security Assurance Division will conduct independent ICT security audits on government agencies and critical infrastructure companies such as national utilities and telecommunications companies with a view to ensuring that these organizations subscribe to the highest security standards.

Meanwhile, IMPACT’s Research Division’s primary function is to stimulate debate and research around areas of concern within the ambit of cyber security that are not being adequately addressed in the public or private sphere, but are no less critical to ensure the security of cyberspace. As well as instigating research into new areas of development such as IPv6 (Internet Protocol version 6) and other subsequent generations of the Internet, a major focus of the division will be in directing resources towards niche areas of research that will improve the security of its members.
Law enforcement officials particularly challenged on one of their cases and requiring university level technical expertise can avail themselves of the latest research available in the fields of cybercrime, security and forensics. IMPACT will assist them in finding suitable research partners -making its facilities available and providing a suitable environment to encourage participating research partners to embark on joint research projects with governments in these areas of concern.

The promise of a safer, more secure cyberspace

As the only multi-stakeholder cyber-security organisation in the world - IMPACT is undertaking a role which has never quite been done before. However, the strong support it is receiving from governments and the cyber security community at large bears testament to the critical need for such an organization and the value that it brings in helping to foster a safer, more secure cyber-space for all. IMPACT looks forward to partnering with and supporting law enforcement organisations around the world. Further information on IMPACT may be found at www.impact-alliance.org.
COUNCIL OF EUROPE MEASURES FOR FIGHTING AGAINST CYBERCRIME1

Cristina Schulman holds a law degree from the University of Lasi in Romania and a post graduate diploma in international law from the University of Bucharest. She is currently the Programme Manager for Cybercrime, Economic Crime Division, Directorate General of Human Rights and Legal Affairs at the Council of Europe, having the main duty to provide expert assistance to the Economic Crime Division in the implementation of the Projects on Cybercrime, which support States in implementing the Convention on Cybercrime.

1. The threat of cybercrime

Societies all over the world rely on information and communication technologies (ICT). The number of Internet users worldwide increased by four times from 300 million in 1999 to almost 1.2 billion in 2007. Threats include virus, worms, spyware, bots and other malware compromising the confidentiality, integrity and availability of public and private computer systems. This may include attacks against the critical infrastructure of a country. Malware is used for identity theft in order to commit credit card, e-commerce and other types of fraud, and ICT are used for a wide range of other serious offences such as money laundering, trafficking in human beings, child pornography, extortion or other forms of organized crime. Cybercrime is very much transnational crime requiring extensive international cooperation.

2. The legislative response

In order to meet this challenge, countries need to equip themselves with a comprehensive legal framework:

2.1. They should criminalise certain conduct in their substantive criminal law. As a minimum this should include:

- Illegal access to a computer system ("hacking", circumventing password protection, exploiting software loopholes etc)
- Illegal interception (violating privacy of data communication)
- Data interference (malicious codes, viruses, trojan horses etc)
- System interference (hindering the lawful use of computer systems)
- Misuse of devices (tools to commit cyber-offences)
- Computer-related forgery
- Computer-related fraud
- Child pornography
- Hate speech, xenophobia and racism
- Infringement of copyright and related rights

1 For more information about Council of Europe activities in fighting cybercrime see: www.coe.int/cybercrime
2.2. They should give law enforcement and other criminal justice authorities the means to investigate, prosecute and adjudicate cybercrimes in their criminal procedure law. Among other things this should allow for the possibility to take immediate action to preserve electronic evidence. As a minimum this should include specific provisions for:

- The expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

2.3. They should allow for efficient international cooperation, which means to harmonise their legislation with the international standards on the matter and provide for mutual legal assistance and police cooperation and join international treaties such as the Budapest Convention on Cybercrime of the Council of Europe.

3. The Council of Europe Convention on cybercrime (Budapest Convention)

3.1. The need for criminalizing cybercrime at global level

Cybercrime may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects.

Among the general trends:

- The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised;
- Clear indications point to a growing involvement of organised crime groups in cyber crime.

In the light of this changing environment, there is an urgent need to take action - at the national as well as the global level - against all forms of cyber crime, which are increasingly significant threats to critical infrastructures, society, business and citizens.

Cybercrime is very much transnational crime and it cannot be fought successfully without cooperation at the global level. In order to do so, countries must develop comprehensive criminal legislation, which - to the extent possible - is harmonised or compatible with that of other countries.
More specifically, countries need to criminalise certain conduct (substantive criminal law), provide law enforcement and criminal justice with the means to efficiently investigate, prosecute, and adjudicate cybercrimes (procedural law), including the need to take rapid action to preserve volatile evidence, and include provisions for efficient international cooperation.

3.2. Why Council of Europe Convention on cybercrime?

The Convention on Cybercrime provides a guideline for the development of legislation. This treaty has been developed by the Council of Europe (currently 47 member States) in cooperation with Canada, Japan, South Africa and the United States of America and was opened for signature in 2001. It entered into force in 2004. This Convention is open to any country from around the world that may seek accession.

Costa Rica, Mexico, the Philippines, Dominican Republic and very soon Chile are invited to become a party, and a number of other countries from different regions of the world are about to seek accession. Being the only multilateral global treaty dealing with these matters has been ratified and implemented in many countries while others are taking into consideration to become party or are currently preparing new cybercrime legislation using the Convention as a model (e.g. Argentina, Brazil, Colombia, Philippines, Indonesia, India, and others). Although many countries are not yet Party to the Convention, the treaty has a great influence on the legislative developments all over the world.

As a result of the harmonisation of the legislations around the world and by implementing the provisions of Chapter 3, the Convention on Cybercrime ensures a framework for international cooperation.

The treaty provides for adequate protection of human rights and liberties. Article 15 ensures that powers and procedures required by the Convention are subject to conditions and safeguards provided under domestic law and the relevant international instruments that provide for the adequate protection of human rights and liberties.

It also contains numerous mechanisms to avoid conflicts between different legislations. Some provisions are included for the situations where countries may have divergent treatment of the procedural or substantive legal provisions allowing attaching additional requirements (e.g. the mere unauthorized intrusion (illegal access) should in principle be illegal in itself but parties have the option to attach some requirements in order to criminalize this conduct; countries can also submit declarations or reservations with respect to obligations under Convention).

2 For more information including on cybercrime legislations see: http://www.coe.int/legalcooperation/economiccrime/cybercrime
3.3. Structure of the Convention:

- Chapter I: Definitions of a computer system, computer data, service provider, traffic data.

- Chapter II: Measures to be taken at the national level
  
  - Section 1 - Substantive criminal law - conduct to be made a criminal offence. This includes:
    - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
    - Computer-related offences (computer-related forgery, computer-related fraud)
    - Content-related offences (Child pornography, and in a separate Protocol also xenophobia and racism)
    - Infringement of copyright and related rights
  
  - Section 2 - Procedural law - measures for more effective investigations of cybercrimes. These include:
    - Procedural safeguards
    - Expedited preservation of stored computer data
    - Expedited preservation and partial disclosure of traffic data
    - Production order
    - Search and seizure of stored computer data
    - Real-time collection of traffic data
    - Interception of content data
  
- Section 3 - Jurisdiction

- Chapter III: International cooperation

  - Section 1 - General principles of cooperation - general principles on international cooperation, principles related to extradition, principles related to mutual legal assistance, spontaneous information, mutual legal assistance in the absence of applicable international instruments, and confidentiality and limitation on use.

  - Section 2 - Specific provisions for more effective cooperation. These require parties to be able to apply procedural tools also internationally. Provisions include the expedited preservation of stored computer data, the expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data, trans-border access to stored computer data, mutual assistance in the real-time collection of traffic data, and mutual assistance regarding interception of content data. This Section also provides for the creation of a network of contact points which are available on a 24/7 basis to facilitate rapid cooperation.
-Chapter IV: Final provisions. This chapter is of particular interest to non-European countries as it provides for the accession on non-member States to the Convention.

The Convention on Cybercrime thus provides a framework for international cooperation:
- It serves as a guideline for the development of national cybercrime legislation and helps ensure harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries.
- It provides tools for the gathering of electronic evidence and tools for the investigation of cyberlaundering, cyberterrorism and other serious crime. Using the Convention these tools can also be applied in international cooperation.
- Chapter 3 of the Convention provides the legal basis for international law enforcement and judicial cooperation with other parties to the Convention.
- It requires Parties to establish 24/7 points of contact based on the experience of the G8 network.

3.4 Advantages for countries becoming a party to the Convention

The Convention is open for accession to any country. It serves as a guideline or "model law" for the development of national legislation even if a country does not actually become a party to this treaty. However, accession to the Convention on Cybercrime implies additional benefits:

1. It serves as a legal basis for international cooperation in cybercrime cases. Parties to the Convention can make full use of the provisions of chapter III on international cooperation, ranging from police to judicial cooperation. This is essential in cybercrime matters.

2. Parties to the Convention participate in the Cybercrime Convention Committee (T-CY). This Committee follows the implementation of the Convention and also initiates future work related to the Convention, such as the preparation of additional protocols etc. This means that countries that may not have been involved in the drafting of the original treaty would still be involved in the elaboration of future international cybercrime standards.

5. Council of Europe Projects on cybercrime

The Council of Europe helps countries to ratify, accede and implement Convention on Cybercrime and its Protocol on Xenophobia and Racism through technical cooperation projects.
5.1. Project on cybercrime Phase 1 (September 2006 - February 2009)

The aim of the project was to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189), and to deliver specific results in terms of legislation, criminal justice capacities and international cooperation. The project was possible due to voluntary contributions from Microsoft and Estonia, which complemented Council of Europe funding.

Within the Project more than 110 activities were carried out during this period ranging from legislative reviews, training workshops and global conferences to contributions to events organised by others. The project relied on cooperation with a multitude of other stakeholders, national authorities, international organisations as well as the private sector and non-governmental initiatives. It helped to create and sustain a global momentum toward stronger legislation. As a result, more than 100 countries around the world either have cybercrime laws in place or are in the process of preparing legislation using the Convention on Cybercrime as a guideline or "model law" and thus establishing the Convention as the primary standard of reference globally.

In terms of actual ratifications/accessions to the Convention, the progress made has been less satisfying although legislative work is underway in many countries.

By February 2009 almost half of the European Union member States (13 out of 27) had not yet ratified this Convention. The call for ratification of the EU Justice and Home Affairs Council of November 2007 and again in November 2008 may help accelerate this process. Six member States of the Council of Europe (Andorra, Monaco, Russia, San Marino and Turkey) had not yet signed the Convention⁴.

Among the reasons for this rather slow process of the ratification/accession are the complex legislative reforms of criminal law necessary in order to comply with the Convention requirements and to ensure the protection of fundamental human rights. Furthermore, cybercrime is not always a priority of governments/parliaments and the seriousness of this threat is often ignored. For some countries cybercrime policy has became a priority only after they experienced serious problems in the area (e.g. Romania, Philippines, Indonesia, Estonia, Georgia etc).

The project contributed to a number of training events specifically aimed at forensic investigators and others at prosecutors. Furthermore, it contributed to efforts for the harmonisation of law enforcement training (working group led by Europol) and the creation of centres of excellence for training in cybercrime investigations and forensics (2Centre initiative supported by the public and private sector).

⁴ In the meantime Germany, Republic of Serbia and Moldova ratified the Convention on cybercrime.
While law enforcement officers of many countries have made much progress in developing their subject-matter skills and while this is also partly true for prosecutors, the judiciary is clearly lacking behind. Steps have therefore been taken by the project to promote the training of judges. The ground has thus been prepared to move towards institutionalising cybercrime training for judges in the future.

A particular problem identified in different countries is related to the need for law enforcement to cooperate with service providers in the investigation of cybercrime. The guidelines developed under the Project on Cybercrime and adopted in April 2008 can be considered a major achievement in this respect. These guidelines served as a basis for the draft agreement between the French service provider association and the Ministry of Interior, the Government of Romania recommended their use by different public and private institutions in Romania, and they served as a basis for the EU Justice and Home Affairs Council of November 2008. They were circulated in a large range of other countries.

The capacity of countries to cooperate internationally will be largely enhanced once they become parties to the Convention. By February 2009, fifty countries had either signed/ratified this treaty or been invited to accede. Once they are all full parties, the value of the Convention as a framework for international cooperation will be greatly enhanced.

The Project promoted the creation of 24/7 points of contact in a number of countries and contributed to the strengthening of the 24/7 points of contact in line with Article 35 of the Convention and the experience of the G8 High-tech crime Subgroup.

In October 2007, a study was launched to document good practices in the implementation of the international cooperation provisions of the Convention. A follow up report on the effectiveness of the network of 24/7 contact points was prepared between September 2008 and February 2009. The report documented lessons learnt and brought a number of issues to the forefront that need to be addressed to make these contact points and international cooperation in general more efficient.

In addition to the Cybercrime Convention Committee (T-CY), the Project against Cybercrime was the most important resource that the Council of Europe had at its disposal to support the implementation of the Convention and its Protocol between September 2006 and February 2009.

The main result of the project is that over a period of 30 months it has been possible to create and sustain a global momentum towards:

- the strengthening of cybercrime legislation in a harmonised manner, including measurable results in terms of laws adopted;
- improving public-private (in particular law enforcement - ISP) cooperation in the investigation of cybercrime;
- closer cooperation among a multitude of stakeholders.
5.2. The Global Project on Cybercrime Phase 2 (1 March 2009 - 30 June 2011)

Built on the achievements of the Project on cybercrime (Phase 1), the Global Project on Cybercrime (Phase 2) was launched in March 2009. The Government of Romania, Microsoft and McAfee have agreed to provide initial funding. It is hoped that other donors will follow their example and join this undertaking.

The project is to last from 1 March 2009 to 30 June 2011 with a budget of Euro 1.4 million. Its objective is to promote broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and related international standards. In addition to what has been covered during the first phase it will put a stronger focus on the implementation of the LEA - ISP guidelines, on promoting financial investigations, on the training of judges, on data protection and privacy and the protection of children.

5.3. Project on cybercrime in Georgia (1 June 2009 - 31 May 2010)

The Council of Europe with the authorities of Georgia and the European Commission have agreed to implement the joint Project on cybercrime in Georgia from 1 June 2009 to 31 May 2010. The objective is to help Georgia develop a consistent policy on cybercrime in view of implementing the Convention on Cybercrime (ETS 185).

6. Conclusions

Considering the international dimension of cybercrime it can be concluded that there is not possible to succeed in this fight by a country alone but only cooperating internationally.

Cooperation depends on countries legal systems and harmonization between the different national legislations. Therefore, in order to combat cybercrime it is essential for all countries to create an adequate legal framework, both nationally and internationally, capable of providing the legislative and investigative tools for fighting cybercrime.

Using the Council of Europe Convention on cybercrime in the process of drafting national legislations it can be achieved international standards in the area and an efficient framework for fighting cybercrime. Ratifying the Convention by more and more countries all over the world will increase its value as a framework for international cooperation.

Section Editor: Ličana Selinsek

The reader is invited to contact the Editor to present his or her institution’s activities in reference to the fight against cybercrime, or any other contribution regarding this topic.
Country: Russian Federation  
Case citation: No. 240-19735/08-10-141  
Name and level of Court: Arbitrazh Court of Moscow  
Date of decision: 25 June 2008  

Keywords: Digital evidence · status of scanned copies as written evidence · contractual agreement for e-mail correspondence

• SUMMARY

The Arbitrazh Court of Moscow accepted print-outs of e-mail correspondence as written evidence. In accordance with the provisions of article 161 of the Russian Civil Code, all contracts between the legal entities must be in writing. Article 452 further stipulates that all amendments to the contract shall be in the same form as the contract, unless otherwise provided by the law, contract or usage of trade. The general consequence for non-compliance with this requirement of form is that the contract cannot be enforced on the basis of oral evidence. However, under the provisions of article 162 of the Russian Civil Code, the parties may produce ‘written and other evidence’ to prove the existence and terms of a contract.

In July 2008 Media Planning Group (MPG) filed a claim with the Arbitrazh Court of Moscow against Meridian Plus (Meridian+) for agency fee and expenses to place advertisements on television. The parties entered into an agency agreement in 2007 whereby MPG undertook to place advertisements for and on behalf of Meridian+ in the mass media (television, newspapers, internet). The contract provided that the principal will separately confirm to the agent its consent to specific terms of advertising by commitment letters sent by e-mail. Meridian+ issued two such letters, confirming its consent to place advertisements on certain television channels and guaranteeing payments according to the relevant schedules.

During the hearing, MPG produced print-outs of the scanned commitment letters it received by e-mail. The letters were accompanied by affidavits sworn by MPG employees, who certified the receipt of the e-mails. MPG further stated it could produce the original commitment letters as Microsoft Outlook files identifying the sender, addressee and time of receipt.

The court resolved that since the contract specifically provided for the commitment letters to be sent by e-mail, their form was in accordance with the agreement of the parties.

Source: Case note by Alex Dolzhich. The complete case note will be published in the Digital Evidence and Electronic Signature Law Review, 6 (2009).
Country: Singapore
Case citation: Public Prosecutor v Neo Khoon Sing [2008] SGDC 225
Name and level of Court: District Court

Keywords: Digital evidence - the standard of proof for circumstantial evidence -
it should lead one to ‘the irresistible inference and conclusion’ that the offence
was committed by the accused

SUMMARY

The accused worked at an independent office at the National Environment Agency North East Regional Office.

On 18 October 2005 two false terrorist attack warning messages were sent through the web sites of the Ministry of Home Affairs, the first of which read ‘Rumours of possible suicide bomb in Bedok area in 2 to 3 weeks time’ and the second of which read ‘a possible bomb attack in Singapore in an event with water activities involving head of state, ministers etc. Within a month’. A third message was sent through the web site of the Prime Minister’s Office (PMO) on 19 October 2005.

The alarming messages were communicated to the respective recipients via the feedback function in web sites, not e-mail. Police investigations revealed that the alarming messages had emanated from NEA’s computer network. In particular, they had been sent from the desktop computer located in the office in which the accused worked, and which had been allocated for use by the accused.

The timings of the sending of the e-mails and logging into the accused’s account contradicted the accused’s claim that he was not in his office at the time the alarming messages were sent. The prosecution relied on circumstantial evidence and the evidence in the statements of the accused to establish its case.

The court concluded that the accused deliberately sent three alarming messages, peppered with alarming details of terror attack against the Prime Minister and other leaders at a public event. The accused was sentenced to 30 month’s imprisonment.

**Country:** Poland  
**Case citation:** I KZP 39/08  
**Name and level of Court:** Sad Najwyższy Rzeczypospolitej Polskiej (Polish Supreme Court)  
**Date of decision:** 26 March 2009

**Keywords:** Electronic document - secure electronic signature (digital signature) - criminal procedure - Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Law of 2001.09.18 on electronic signature) - legal effect

***SUMMARY***

A criminal appeal sent to a court in the form of an electronic document signed with a secure electronic signature as required by the Law of 2001.09.18 on electronic signature is without legal effect, because this method of signature in criminal procedure and in the procedure for contraventions (minor infractions which are treated prosecuted and tried differently from substantial crimes) is not regulated.

The Supreme Court expressed an opinion that despite the wording of article 5 section 2 of the 2001 Act, which equates a secure electronic signature with handwritten signature, the appeal was not acceptable. The use of an electronic signature in criminal procedure is not possible because there are no relevant regulations in place. This was treated by the members of the Supreme Court as a legal gap, which indicated the intent of the legislator not to permit the use of electronic signatures in criminal proceedings. Where an appeal is sent electronically as it was in this case, it is without any legal effect and no further steps are to be taken.

**Source:** Case note by Dr Arkadiusz Lach. The complete case note will be published in the Digital Evidence and Electronic Signature Law Review, 6 (2009).
When repairing the defendant’s computer, a computer technician discovered what she believed to be child pornography. The police were contacted by telephone, and the detective who received the telephone call obtained a search warrant from a judge of the Long Beach Superior Court. When the detective arrived at the store to execute the warrant, the defendant had already collected his computer. The detective then submitted an affidavit, and a sworn statement from the computer technician, describing the images. On the basis of this affidavit, the officer obtained a second warrant, this one directed at the defendant’s home, authorizing the seizure of the same items. The search warrant was executed, but the computer was not in the defendant’s apartment. However, the following computer storage media was found and seized: 22 5.25-inch floppy disks, two CD-ROMs, 124 3.5-inch floppy disks and six zip disks. Two of the zip disks were found to contain images of child pornography. The defendant was subsequently charged with one count of possession of child pornography.

In the district court, the defendant moved to suppress the evidence recovered from the two zip disks on the grounds that, (1) contrary to the magistrate’s finding, the warrant affidavit did not establish probable cause to believe the defendant was guilty of criminal activity; and (2) the warrant was over-broad in allowing seizure of all discovered computer storage media with no regard to whether such media contained child pornography, and in placing no limitation on the police officers’ search of the seized disks. The district court denied the motion to suppress and the defendant entered a conditional plea of guilty to the charge, reserving the right to appeal the district court’s evidentiary ruling. The defendant appealed.

The court of appeal determined that the search was supported by probable cause and, notwithstanding the shortcomings of the search warrant affidavit, the manner of its execution does require the suppression of the evidence found during the course of the search. The district court’s denial of the defendant’s motion to suppress was affirmed.

Editor’s Note: Circuit Judge Fisher illustrated the range of technical problems faced by the police in such a case, thus making a search on site, together with a selective removal of relevant evidence, virtually impracticable.

Country: The Netherlands
Case citation: LJN; AY6903, Services Court Judge Amsterdam, 345291 / KG 06-1112 AB
Name and level of Court: Voorzieningenrechter In Kort Geding (Services Court Judge Amsterdam)

Keywords: Protection of intellectual property rights · internet · illegal downloads · privacy of customer personal data · right of interested parties to require ISP to provide personal data

SUMMARY

BREIN (the Dutch anti-piracy foundation for the entertainment industry) served a subpoena on UPC, an Internet Service Provider (ISP). BREIN wanted to take action against customers of UPC for large scale copyright infringement. BREIN requested UPC to provide the personal data (name and address) of those alleged to have infringed copyright, to enable BREIN to initiate legal action against them. The ISP wanted a declaration that it was not acting unlawfully by failing to provide personal data of customers to BREIN, and that they were not obliged to do so because of the provisions of the Dutch Data Protection Act.

To undertake action, BREIN required the personal data of those infringing the intellectual property rights of others. It was argued that privacy interests should not prevail above the interests of BREIN to prevent people from infringing the intellectual property rights of others.

The court determined that UPC was required to provide the personal data to BREIN.

Source: Case note by Arnold Roosendaal. The case note in full, together with a translation of the case into English will be published in the Digital Evidence and Electronic Signature Law Review, 6 (2009).

Note from the Editor:

Due to an inadvertent error, the text on page 32 of the July issue did not correctly reflect the position regarding judgments that are not reported in the UK. Judgments that are not reported in the UK can be referred to by judges and lawyers, and the text should have read:

In the UK (comprising the three jurisdictions of England & Wales, Northern Ireland and Scotland) the trial of a case is rarely reported. Also, appeals might also not be reported. This does not prevent judgments and trials that are not reported to be referred to in the judgment of judges and in academic articles and legal text books.

Section Editor: Mr. Stephen Mason

The reader is invited to send details of cases (both civil and criminal, reported and not reported) that have relevance to digital evidence direct to the Editor. Please provide the correct citation as it would be in your own country, together with a full copy of the judgment. Translations into English will be appreciated if it is possible. Also, if there are any significant items of legislation that are of interest, please inform the Editor of any such changes. It is important to understand that because digital evidence moves over physical borders with ease, the changes to national legislation dealing with digital evidence and cyber crimes affects all other nation states.
• CONFERENCES

17-19 August 2009
DFRWS (Digital Forensic Research Workshop) 2009 Annual Conference
Montreal, Canada
Purpose: DFRWS brings together leading researchers, developers, practitioners, and educators interested in advancing the state of the art in digital forensics from around the world. As the most established venue in the field, DFRWS is the preferred place to present both cutting-edge research and perspectives on best practices for all aspects of digital forensics. As an independent organization, we promote open community discussions and disseminate the results of our work to the widest audience.

1-2 September 2009
CFET 2009 3rd International Conference on Cybercrime Forensics Education & Training
Canterbury Christ Church University, Canterbury, UK
Purpose: A broad inclusive approach taken with respect to anything to do with the development of cybercrime forensics as a new discipline.
Web site: http://www.canterbury.ac.uk/social-applied-sciences/computing/conferences/CFET2009/BCSCybercrimeForensicsSG.aspx

15-17 September 2009
IMF 2009 5th International Conference on IT Security Incident Management & IT Forensics
Stuttgart, Germany
Purpose: IMF’s intent is to gather experts from throughout the world in order to present and discuss recent technical and methodical advances in the fields of IT security incident response and management and IT forensics. The conference provides a platform for collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

17-18 September 2009
Internet Security Operations and Intelligence 7 (ISOI7)
San Diego, California, United States of America
Purpose: The main topics of interest are Internet infrastructure defense, cyber crime, online fraud, phishing, DDoS and botnets. ISOI is a closed conference for members of the different Internet security operations communities, bringing different groups together.
Web site: http://isotf.org/isoi7.html
• LEGAL TRAINING

14-17 September 2009
European Certificate on the fight against Cybercrime and Electronic Evidence (ECCE)
Cyprus

• TRAINING OF LAW ENFORCEMENT OFFICERS

30 August - 5 September 2009
ISEC cybercrime training programme - Malware Analysis and Investigations Course
Microsoft, Copenhagen
Purpose: This training course is part of the EC funded ISEC cybercrime training project. All travel, accommodation and subsistence costs are paid for by the project. Places are still available to law enforcement staff from the following countries: Bulgaria, Czech Republic, Estonia, Finland, Greece, Luxembourg, Poland, Slovakia, Slovenia, Sweden, Turkey and the Former Yugoslav Republic of Macedonia.
Anyone interested in these courses is asked to contact the Project Training Manager, Nigel Jones at nigel.jones@ucd.ie or Tel: +44 7786 317995 for further information on how to apply for a place on the course.

7-11 September 2009
ISEC cybercrime training programme - Forensic Scripting using BASH Course
Centro de Convenciones Mapfre, Avda. General Perón, 40 - 28020 Madrid, Spain
Purpose: This training course is part of the EC funded ISEC cybercrime training project. All travel, accommodation and subsistence costs are paid for by the project. Places are still available to law enforcement staff from the following countries: Bulgaria, Czech Republic, Estonia, Finland, Greece, Luxembourg, Poland, Slovakia, Slovenia, Sweden, Turkey and the Former Yugoslav Republic of Macedonia.
Anyone interested in these courses is asked to contact the Project Training Manager, Nigel Jones at nigel.jones@ucd.ie or Tel: +44 7786 317995 for further information on how to apply for a place on the course.
• DEGREE COURSES

Commences on 1 September 2009 and is a two year part time taught programme
ISEC cybercrime training programme - Master of Science degree in Forensic Computing and Cybercrime Investigation
University College, Dublin, Ireland and various locations for the taught modules
Purpose: This training course is part of the EC funded ISEC cybercrime training project. All travel, accommodation and subsistence costs are paid for by the project. Places are still available to law enforcement staff from all EU Member States and candidate countries.
Anyone interested in this programme is asked to contact the Project Training Manager, Nigel Jones at nigel.jones@ucd.ie or Tel: +44 7786 317995 for further information on how to apply for a place on the programme.
Web site: http://www.csi.ucd.ie/content/forensic-computing-and-cyber-crime-investigation

• VENDOR TRAINING

7-10 September 2009
EnCase® v6 Computer Forensics I
Centro de Convenciones Mapfre, Avda. General Perón, 40 - 28020 Madrid, Spain
CPE credits: 32
Level: Introductory
Prerequisites: Basic computer skills. Advance preparation for this course is not required.
Purpose: This hands-on course involves practical exercises and real-life simulations. The class provides participants with an understanding of the proper handling of digital evidence from the initial seizure of the computer/media to acquisition, and then progresses to the analysis of the data. It concludes with archiving and validating the data.
Delivery method: Group-Live. NASBA defined level: basic.
Web site: http://www.cybex.es

Section Editor: Mr. Stephen Mason

The reader is invited to send details of conferences, university degree courses, legal training seminars and vendor seminars direct to the editor for inclusion in future issues of the eNewsletter. By submitting your event or course, you accept that it will not necessarily be included in a future issue of the eNewsletter. The inclusion of events and courses is at the sole discretion of the Editor. The criteria for inclusion of events and courses focuses on what, if any, relevance it will have for judges, lawyers and digital evidence specialists within the legal framework.
Editors

A team of seven Editors has been engaged to create the European Electronic Newsletter on the Fight Against Cybercrime, each one being an Expert on the ENAC Section of which they are responsible.

The Editors are in charge of recruiting writers and articles and reviewing and selecting the most appropriate to be included in the ENAC.

According to the order of appearance of their Sections in the ENAC, the Editors are the following:

Mrs. CARMEN LÁZARO
Responsible of the Litigation Support Department
Cybex
cizaro@cybex.es

Mr. PEDRO VERDELHO
Public Prosecutor and trainer
Editors Board Member
Section in ENAC: Legal
pedro.verdelho@gmail.com

Mrs. ELENA DOMÍNGUEZ PECO
Public Prosecutor and Collaborator for the Spanish Data Protection Agency
elena.dominguez@comjib.org

Mr. MATIAS BEVILACQUA
Computer Forensic Expert
IT Manager
Cybex
mbevilacqua@cybex.es

Mr. NIGEL JONES
Director
Technology Risk Limited
nigel.jones@technologyrisklimited.co.uk

Mrs. LILJANA SELINSEK
Assistant Professor at the Law Faculty of University of Maribor
liljana.selinsek@uni-mb.si

STEPHEN MASON
Barrister
Chambers of Stephen Mason
stephenmason@stephenmason.eu

Mrs. MIREIA CASANOVAS
ENAC Chief Editor
Cybex
micasanoas@cybex.es
To ensure the widest possible diffusion of the Electronic Newsletter on the Fight Against Cybercrime, the ENAC counts with the collaboration of Distributor Institutions and Organizations, who will distribute the ENAC monthly to their contacts database.

If you are interested in being a Distributor partner please contact the Project Coordinator Mrs. Mireia Casanovas at mcasanovas@cybex.es.

The Distributors of the ENAC Project are the following:

- **Actuar Asociación Civil**
- **Agencia Española de Protección de Datos**
- **Alba Advisors LTD**
- **Altmark and Brenna**
- **Ambassade du Costa Rica**
- **Asia Pacific Cyberlaw, Cybercrime and Internet Security Institute (Waseda)**
- **Justicia y Opinión**
- **Association of Prosecutors of Republic of Serbia**
- **Attorney-General’s Department Sri Lanka**
- **Centro de Estudios Judiciarios**
- **CERT-LEXSI**
- **Ciberdelincuencia.org**
- **Comisión Interinstitucional Sobre Terrorismo CISTE**
- **Consejo General de la Abogacía Española**
- **Conselho Distrital de Lisboa da Ordem dos Advogados**

---

*The ENAC project is funded by Cybex and the European Commission's Directorate-General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008.*
<table>
<thead>
<tr>
<th>Organization</th>
<th>Country/Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ledjit Consulting</td>
<td>Lithuania</td>
</tr>
<tr>
<td>Lithuanian Bar Association</td>
<td>Lithuania</td>
</tr>
<tr>
<td>Malta Police Force</td>
<td>Malta</td>
</tr>
<tr>
<td>Microsoft Europe, Middle East and Africa</td>
<td>Europe</td>
</tr>
<tr>
<td>Ministerio della Giustica Diario per gli Affari di Giustizia</td>
<td>Italy</td>
</tr>
<tr>
<td>Ministry of Justice and Citizens Liberties Romania</td>
<td>Romania</td>
</tr>
<tr>
<td>Ministry of Justice of the Slovak Republic</td>
<td>Slovakia</td>
</tr>
<tr>
<td>National Institute of Criminology Budapest</td>
<td>Hungary</td>
</tr>
<tr>
<td>National Prosecuting Authority of South Africa</td>
<td>South Africa</td>
</tr>
<tr>
<td>National Public Prosecutor’s Office of the Republic of Poland</td>
<td>Poland</td>
</tr>
<tr>
<td>NACPEC.org</td>
<td>United States</td>
</tr>
<tr>
<td>North American Consumer Project on Electronic Commerce</td>
<td>United States</td>
</tr>
<tr>
<td>OSCE</td>
<td>Europe</td>
</tr>
<tr>
<td>Organization for Security and Cooperation in Europe</td>
<td>Europe</td>
</tr>
<tr>
<td>Policia Federal Preventive Delegacion Coyoacan</td>
<td>Mexico</td>
</tr>
<tr>
<td>Ministerio Publico Procuraduría General de la República Dominicana</td>
<td>Dominican Republic</td>
</tr>
<tr>
<td>Seriously Organized Crime Agency (SOCA)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Risk Analysis Consultants RAC</td>
<td>United States</td>
</tr>
<tr>
<td>Sindicatos dos Magistrados do Ministerio Publico Portugal</td>
<td>Portugal</td>
</tr>
<tr>
<td>Serious Organized Crime Agency (SOCA)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>State Prosecutor Department of Justice Philippines</td>
<td>Philippines</td>
</tr>
<tr>
<td>Technology Risk Limited</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Disclaimer:

ENAC e-newsletter provides news and opinion articles as a service to the readers. Statements and opinions expressed in these articles are solely those of the author or authors and may not be shared by the ENAC Board of Editors, Cybex management or the European Commission.

The translations included in the ENAC newsletter were prepared with the utmost care. However, ENAC Board of Editors, Cybex management or the European Commission do not accept any liability for the accuracy and completeness of the compilation and content of these translations, or the direct or indirect consequences of acting or failing to act based on these translations.

Design: © Cybex 2009. All rights reserved
Articles: © 2009. Protected by Law