Communications of the IIMA

Volume 5 | Issue 1 Article 7

2005

Cracking Down On Cybercrime Global Response: The Cybercrime Convention

Sylvia Mercado Kierkegaard

Cracking Down On Cybercrime Global Response: The Cybercrime Convention

Sylvia Mercado Kierkegaard
Sylviak_1952@hotmail.com

ABSTRACT

Computers and the Internet have brought innumerable benefits to society. They have revolutionized the way people work, play, and communicate. In spite of the benefits the Internet has introduced to the global community, it is also fraught with risks associated with undesirable elements keen to misuse its usage. Computers and the Internet present new ways to engage in old crimes, such as fraud and piracy. They also have made it possible for criminals to perpetrate new harmful acts, like data access and interference. However, national legislations and regional agreements are not sufficient to address the global nature of cybercrime. Therefore, in order to prosecute cybercrime as well as other types of crime, a common framework must be created that can punish these crimes irrespective of where they are committed. The International Cybercrime Convention has recently come into force focusing on an international solution to combat cybercrime. This paper analyses the implications of the new Cybercrime Convention on organisations and private individuals, and whether the requirements of the Convention balance the need for a criminal crackdown with the equally critical need to maintain basic freedoms.

Key words: *legal framework, privacy, surveillance, trust, business confidence, treaties, cybercrime.*

INTRODUCTION

Over the last decade, the use of computers and the Internet has grown rapidly. The Internet has revolutionized the way businesses approach and conduct work. For consumers, the idea of purchasing online is appealing for several reasons. A well designed and implemented e-commerce system can lower transaction costs, reduce inefficiencies, promote better information flow, and encourage better cooperation between buyers and sellers. In today's rapidly changing world of e-commerce, almost anything can be bought over the Internet and delivered right to one's front door. By transcending international boundaries, the Internet and the World Wide Web enable a company to market and deliver efficiently and cost-effectively by electronic means, products and services to customers located in target countries often thousands of miles away. With little more than a click of a mouse, businesses can communicate, engage in commerce, and expand their business opportunities. For consumers, shopping on the Internet provides more choices, better features at a more competitive price, quicker delivery, and greater information to make a more informed decision

Unfortunately, in addition to creating immense social and economic opportunities, the borderless and anonymous character of the Internet poses enormous challenges. Information Technology makes it an ideal forum to penetrate and facilitate criminal activities. Criminals exploit these same technologies to commit crimes and harm the safety, security, and privacy of IT users. In the hands of persons acting with bad faith, malice, or grave negligence, these technologies may become tools for activities that endanger or injure the life, property or dignity of individuals or damage the public interest. Indeed, as more people go online, more criminals are realizing that online crime can be lucrative, especially given the amount of valuable commercial and personal information now being stored electronically.

Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. International computer networks are the nerves of the economy, the public sector and society. The information infrastructure has become a critical part of the backbone of our economies. The security of these computer and communication systems and their protection against computer crime are therefore of essential importance. The spreading of computer technology into almost all areas of life as well as the interconnection of computers by international computer networks have made computer crime more diverse, more dangerous, and internationally present.

Companies and governments are realizing that it is no longer effective to use domestic solutions to address problems that encompass a multitude of constituencies across multiple geographies.

However, the borderless nature of the Internet poses a dilemma. Internet sites cannot function if they must conform to the varying legal requirements of every jurisdiction in the world. Standards of permissible advertisements, political speech, religious liberty and religious expression, and even permissible hate speech and discussion of drug use vary widely between nations and cultures. Complying with each of these standards would impose untenable compliance costs and burdens on portals and websites alike. The various national laws show remarkable differences, especially with respect to the criminal law provisions on hacking, trade secret protection and illegal content. Considerable differences also exist with respect to the coercive powers of investigative agencies (especially with respect to encrypted data and investigations in international networks), the range of jurisdiction in criminal matters, and with respect to the liability of intermediary service providers on the one hand and content providers on the other hand.

Computers and the Internet present new ways to engage in old crimes, such as fraud and piracy. They also have made it possible for criminals to perpetrate new harmful acts, like data access and interference.

For these reasons, countries around the world are taking measures to combat computer crime. However, national laws and regional agreements alone are not sufficient to address the global nature of cybercrime. Therefore, in order to prosecute cybercrime as well as other types of crime, a common international framework must be created that can punish these crimes irrespective of where they are committed. Without the proper legal and enforcement infrastructure, cybercrime will engulf the global business. The International Cybercrime Convention has recently been signed focusing on an international solution to combat cybercrime. This paper will attempt to provide an overview of the effects of cybercrime, to discuss the salient provisions of the International Cybercrime Convention and to determine its implications and repercussions for the industry and private citizens.

WHAT IS CYBERCRIME?

Various terms are used to define cybercrime. It can be broadly defined as a criminal offence that has been created or made possible by the advent of computer technology. Cybercrime can be divided into two categories: computer-related crimes and computer crimes. Computer-related crimes are traditional crimes where criminals are just using the computer to facilitate crime.

These crimes include: threats, child pornography, fraud, gambling, extortion, and theft of intellectual property, computer-generated counterfeit documents, threatening or annoying electronic mail, online gambling, hate speech, and stalking. Computer-related crimes already have equivalent criminal offence with corresponding criminal laws. Computer Crime is a new form of crimes which involves the use of a computer as the primary instrument to facilitate the crime and targets computer networks themselves. Included in this category are such crimes as hacking, releasing computer contaminant viruses, disrupting and denying computer services to an authorized user , shutting down computers by flooding them with unwanted information (so-called "denial of service" attacks), and taking, copying, altering, deleting, or destroying computer data, and software or programs. Computer crimes require a much higher degree of technical knowledge than computer-related crimes.

Cybercrime can also be divided into four categories: economic crimes (hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery, computer fraud and computer manipulations instead of deceiving a human); content-related offences (dissemination, especially via the Internet, of e.g. child pornography and racist statements); intellectual property offences (violation of copyright and related rights and cyber squatting); and privacy offences (illegal collection, storage, modification, disclosure.

While seemingly a straightforward task, defining cybercrime is not easy. The difficulty lies in properly defining what crimes should be considered as cybercrimes. There is no globally-accepted definition of cybercrime! Experts cannot agree on whether cybercrimes should only include computer crimes as criminal laws already exist that can be applied in the virtual world. In addition, countries may also not agree as to what is defined as cybercrime as conceptions of crime vary widely from culture to culture. For example, file sharing is not considered a "crime" in many under-developed countries, while in the United States (US), the Movie and Recording Industry is vigilant in prosecuting P2P file sharing of movies and songs. In a unanimous court judgement, the U.S. Supreme Court in *Metro-Goldwyn-Mayer Studios v. Grokster Ltd.* ruled that P2P firms can be sued if they encourage the use of their products to illegally swap copyrighted music and movies (Regan, 2005).

CYBERCRIME: IS IT REALLY SERIOUS?

According to the *Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime* (2004), economic crime, often in the form of cybercrime, accounts for 1.3 per cent of total crime, and 57 percent, or 6.8 billion Euros of financial damage.

Does Cybercrime Really Pose A Significant Threat To Society?

The *2004 9th Annual Computer Crime and Security Survey* by the Computer Security Institute (CSI) and the San Francisco FBI reports that cybercrime is real and continues at a steady pace, but financial losses from computer attacks are down (Gordon and Loeb, 2004). The *9th Annual* surveyed 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. The CSI/FBI survey clearly shows that cybercrime continues to be a significant threat to American organizations and respondents appear to be getting real results from their focus on information security. Their average dollar losses per year have dropped in each survey for four straight years. The message is that it makes sense for organizations to continue their adherence to sound practices, deployment of sophisticated technologies, and adequate staffing and training organizations that raise their level of security awareness have reason to hope for measurable returns on their investments. Highlights of the *2004 Computer Crime and Security Survey* include the following:

- Overall financial losses totalled from 494 survey respondents were $141,496,560. This is down significantly from 530 respondents reporting $201,797,340 last year.
- The most expensive computer crime was denial of service.
- Organizations are using metrics from economics to evaluate their security decisions. Fifty-five percent use Return on Investment (ROI), 28 percent use Internal Rate of Return (IRR), and 25 percent use Net Present Value (NPV).
- The vast majority of organizations in the survey do not outsource computer security activities. Among those organizations that do outsource some computer security activities, the percentage of security activities outsourced is quite low.
- Virus was the number one source of financial loss, followed by denial of service attacks.
- Fewer organizations are reporting computer intrusions to law enforcement.

In contrast, the *2004 E-Crime Survey* conducted among security and law enforcement executives by *CSO magazine* in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT Coordination Centre shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions. Respondents say that e-crime cost their organizations approximately $666 million in 2003 (CSO, 2004). Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization.

However, 30% of respondents report their organization experienced no e-crime or intrusions in the same period while a quarter (25%) experienced fewer than ten. The survey shows intrusions and attacks as very unevenly distributed: government offices, ICT firms, banks and other financial institutions are the most frequent targets, and 28.6% of e-crimes were apparently committed by "insiders. When asked what types of losses their organizations experienced last year, over half of respondents (56%) report operational losses, 25% state financial loss and 12% declare other types of losses. 32% of respondents do not track losses due to e-crime or intrusions. Of those who do track, half say they do not know the total amount of loss. Forty-one percent (41%) of respondents indicate they do not have a formal plan for reporting and responding to e-crimes, demonstrating room for improvement. Slightly more than half (51%) state they have a formal process in place to track e-crime attempts. Here is a summary of the specific types of crime reported: Virus or other malicious attacks,77.2 % ; Denial of service attack, 43.6% ; illegal generation of SPAM, 38.8% ; unauthorised access by an insider, 35.7% ; unauthorised access by an outsider, 27.2% ; fraud, 21.9% ; theft of intellectual property,20.5%; theft of proprietary info, 16.4% ; Employee identity theft: 12.0%; sabotage by an insider: 10.8% ; sabotage by an outsider, 10.8% ; Extortion by an outsider: 3.2% and ; other, 11.1%.

The rise of cybercrime has profound impact on firms and individuals. It may well inhibit any further growth of B2C propositions

TECHNOLOGY SOLUTIONS

As in the past years, technology is continually advancing and that the criminal element will adopt new technology as it comes along. With a growing number of personal data devices and other sophisticated technology, criminals are becoming more able to conceal their actions. Protecting the nation's critical digital infrastructure requires a comprehensive view of security that combines physical, digital and procedural components. These components are necessary and unique to each individual environment and must not impact normal daily activities, while providing the level of cyber security necessary to guard against the many known and unknown threats in cyberspace. Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. Cybercrime can affect service providers, banks, individuals and law enforcement authorities. A compromise on one network can allow an intruder either direct access to a partner's private data or indirect access by allowing a back door into the partner's network. Further threats to cyber security include (1) misconfiguration of computer systems; (2) poor user and administrator education; (3) poor software design; (4) network and system design issues; (5) substandard operational procedures; (6) use of insecure protocols; (7) weak passwords; (8) and finally, lack of awareness and indifference.

A large number of companies still do not have in place an information security policy. Awareness is fundamental as without it, market forces will not drive improvement. If the client is not demanding security with the supplied service, then IT suppliers will not be encouraged to supply it. By putting in place a security policy, businesses promote best practice in relation to the use of their systems and access to their information. Security breaches are often caused by poorly implemented internal processes, and a lack of staff awareness or lax control. Businesses need to implement their own cybercrime crackdown and install up-to-date bug patches. Tools are available to prevent unwelcome intrusion, secure e-commerce infrastructure and protect communications between businesses and third parties. The most common technologies employed are: firewalls, physical security systems, encryption of critical data in transit and storage, manual patch management and filtering and virus scanning.

However, technological tools are not enough to combat transborder cybercrime problems. For example, the computer virus dubbed the *"Love Bug"* had forced email servers to shut down in Europe and spread wildly in the US. The virus caused US$7 billion damage. Reonel Ramones authored the Love Bug virus, but was not prosecuted for computer hacking because the Philippines did not have a law that dealt with computer crime at that time. The Philippines subsequently brought into force a new law covering electronic commerce and computer hacking, but it could not be applied retrospectively to the *Love Bug* case. The case illustrates the need to update current legislations and to address cybercrime at an international level through a harmonized legal framework, such as a Convention or Treaty. As any action taken over the Internet is global, it also requires a global response.

CYBERCRIME CONVENTION

The Council of Europe (COE) is a body created in 1949 and dedicated to "agreements and common action in economic, social, cultural, scientific, legal and administrative matters and in the maintenance and further realization of human rights and fundamental freedoms." In 1997, the Council created a working group on cybercrime to draft a convention on computer crime. The draft was prepared by an ad-hoc group of experts of a "limited number of countries". The U.S. Department of Justice was instrumental in the development of the final accord. It is widely believed that the US wrote this and pushed it through the Council, both to get access to foreign communications and especially to impress on Congress that *Carnivore* in the US should be seen as business as usual, and something demanded by its allies (Froomkin, 2004). It took four years and 27 drafts before the final version was submitted to the European Committee on Crime Problems in June of 2001. A major issue has been that the Convention has been drafted behind closed doors. Whilst law enforcement bodies have actively participated in the drafting process, there has been no direct input from civil liberties bodies, representatives of industry or citizens' interests, despite the significant operational and financial impact it would have on industry and other private organizations and its implications for privacy and human rights.

In November of 2001 the Council of Europe's Cybercrime Convention was signed by 30 countries. Its signatories are not limited to Europe but also include Japan, Canada, South Africa and the United States. For the Convention to have the force of law it must also be ratified, i.e. given effect to in the laws of a participating country, by five of those states, three of which must be members of the Council of Europe. Following its ratification by Lithuania as the 5th country in March of 2004, the Convention on Cybercrime entered into force for Albania, Bulgaria, Croatia, Cyprus, Romania, Slovenia, Estonia, Hungary, Lithuania and Macedonia, but will not come into force in the other signatory states until it has been ratified by their respective national parliaments in accordance with Article 24 of the Vienna Convention.

The U.S. has already signed the treaty, but it has not yet been ratified by the Senate although President Bush has written a letter urging the treaty's passage which he said is "the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering "(Poulsen, 2004).

In addition, the Council of Europe ratified several measures designed to prevent racism and xenophobia on the Internet in 2002, which have been integrated into an additional protocol as part of the Convention on Cybercrime although this had to be separated from the main text to avoid alienating the US, where it would likely be deemed inconsistent with the country's Constitutional right of free speech. It demands that member states criminalize the dissemination of racist material using IT systems, as well threats or insults with a racist or xenophobic motivation, the denial, gross minimization, and the approval or justification of genocide or crimes against humanity. A nation ratifying the Convention on Cybercrime is not obliged to adhere to the protocol.

The Convention is divided into 4 chapters: Chapter I defines relevant of terms; Chapter II, the measures to be taken at the national level; Chapter III, international cooperation and; Chapter IV, the final provisions. The Convention requires Parties to criminalize, if they have not already done so, certain conduct that is committed through, against, or related to computer systems and establish the procedural tools necessary to investigate such crimes under their own national laws. Chapter II contains the measures to be taken at the national level and is divided into substantive criminal law and procedural law. The criminal activities are set out in the five titles of Chapter II.

- Illegal access to the whole or any part of the computer system without right
- Illegal interception *without right*, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data
- Data interference when committed *intentionally*, such as the damaging, deletion, deterioration, alteration or suppression of computer data without right
- System Interference when committed *intentionally*, such as the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

- - Misuse of Devices to commit any of these offences when committed *intentionally* and *without right* such as the production, sale, procurement and possession for use, import and distribution and making available the device or computer password, access code, or similar data for the purpose of committing the offences
- Computer-related forgery and fraud
- Child pornography.
- Infringement of copyrights and related rights
- Attempt on aiding and abetting
- Provisions on Corporate Liability to ensure that a legal person can be held liable for a criminal offence by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: a power of representation of the legal person; an authority to take decisions on behalf of the legal person; and an authority to exercise control within the legal person. The legal person can be held liable where the lack of supervision or control by a natural person has made possible the commission of a criminal offence for the benefit of that legal person by a natural person acting under its authority.
- All of the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. The determination of *mens rea* (guilty mind) is left to the member parties to interpret individually.

The Convention also covers a series of procedural powers such as searches of and interception of material on computer networks. More controversially, the Convention includes "powers to preserve data, to search and seize, to collect traffic data and to intercept communications. Article 15 of the Convention establishes minimum safeguards on the establishments, implementation and application of the powers and procedures provided for in the Convention which should be subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. However, the Convention only refers to parties who are parties to the previously-signed treaties; non-parties to these treaties are not bound by this requirement." This is particularly important because a number of C.O.E. states do not yet conform

to the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols or the International Covenant on Civil and Political Rights. This is of particular concern since many of the Articles in the document expand law enforcement power but do not explicitly place limitations on those expansions, relying on national laws or practices or outside agreements such as the European Convention on Human Rights to set the framework. Many of the countries that are likely to sign this treaty, such as China and Singapore, are not a party to these agreements and have a history of hostility to human rights interests" (Bannisar, 2000)

Nations would have to cooperate with other nations in sharing electronic evidence across borders. This cooperation requirement would apply to all crimes not even defined by the Convention (Art.14). Moreover, law enforcement authorities in countries that ratify the Convention undertake to provide online wiretap assistance (for both content and traffic data) to their treaty partners in the form of a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (Crawford,2004).

IMPLICATIONS

Under the corporate liability provision (Art.12), corporations may face criminal liability if through a lack of supervision permit the undertaking of criminal activity for the corporation's benefit. The strict liability clause imposes untenable obligations on corporations to monitor employee Internet usage under threat of liability. This would make companies pay closer attention to their employee's computer habits and lead to employee surveillance in the workplace. It could also result in imprisonment in foreign jails for representatives of companies for activities of their employees.

Copyright infringement (Art.10) will be considered a criminal offence despite the fact that it is treated a civil offence and that there are already international treaties such as the World Intellectual Property Organization, which address this issue. Thus, on-line conduct is not treated in a manner consistent with the way offline conduct is treated.

The Convention will create a global cyberpolice which will have a huge extension of powers in cross-border sphere to investigate hacking, net espionage, pornography etc. However, the power has gone beyond its remit and will empower investigators to eavesdrop on network communications, to store intercepted data and confiscate the computers of suspected users. The key aspect of the Convention is that it imposes a duty on signatories to do Carnivore-like snooping on domestic internet users at the request of a foreign government so long as the snooping method is consistent with domestic law. Carnivore is a controversial program developed by the U.S. Federal Bureau of Investigation (FBI) to give the agency access to the online/e-mail activities of suspected criminals. For many, it is eerily reminiscent of George Orwell's book "1984." Carnivore is capable of collecting more information than law enforcement is legally authorized to acquire. While the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors and is subject to intentional abuse as well. The unauthorized over-collection of private communications, whether accidental or intentional, raises fundamental issues under both federal wiretap law and the Fourth Amendment of the United States (Sobel, 2000).

The Convention would impose the heaviest burden on Internet Service Providers (ISP) as the data retention requirements would put economic and technical burdens on them. ISPs in signatory countries would be required to respond to and comply with legal process from other signatory countries with respect to the cybercrime provisions, regardless of the laws of the country in which they reside. Many companies fear they will be swamped with subpoenas for computer data as investigators in other countries take advantage of the breadth of the accord (Rosen, 2002). Processing these requests costs money and strains network systems. Nevertheless, the ISPs would have to foot the bill, which will be passed to the consumers. The Convention will apply to any business or individual who cable together two computers. Governments often have collected and analyzed threat information in the process of providing for their national security. Both types of information, vulnerabilities and threats, can be of great value to businesses, but the industry should not be burdened with excessive regulation and costs that are disproportionate to the benefits which may be achieved.

If an individual is suspected of involvement in cybercrime, surveillance and data gathering can be mounted. This constitutes the deprivation of citizen's rights without recourse to judicial process. A member country can impose legal penalties on a citizen of another country for online activity that is perfectly legal in the citizen's country. Supra-national investigation allows abuses of legal processes by facilitating the storing of information in jurisdictions, such as Romania, where protection of individual right is weakest. The same powers given for example to France will be handed over to such countries whose histories do not necessarily reflect strong checks on police

power. Article 24 of the Convention makes it possible to extradite and prosecute foreign nationals for computer-related crimes. This will allow a French to be extradited to Macedonia under Macedonian law.

Mutual Assistance agreements is not required to be subject to the conditions of dual criminality, but it would be permitted irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws and if the other party insists. (Art.25 (5)) There is no distinction between minor and major offence.

There is also an evident lack of commitment to data protection principles (Akdeniz, 2003). The Convention does not mention data protection or make reference to existing data protection treaties, such as the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Data (CETS No.108), which came into force in 1985. Data transfer to third country which does not have an adequate level of protection will also infringe Art.25 of the European Union's EC Directive 95/46 on data protection.

It is still too early to determine the effect of the Cybercrime Convention as it has only recently come to force for most of the 10 signatory countries and has not been transposed into their national law. But in a nutshell, the Cybercrime Convention will have major implications for various actors. It will strangle the Internet with a suffocating blanket of overlapping jurisdictional claims and strengthen the right of the authorities to intercept Internet communication. This causes concern that law enforcement agencies will abuse their power to wire tap Internet traffic without restraint. [1] The COE will not stop serious cybercriminals from continuing to operate in cyberspace unless there is a coordinated policy initiative at national, supranational or international level: they will simply find safe havens. The significance of the will only materialize when (or perhaps if) the major world powers ratify the Treaty.

CONCLUSION

Cybercrime continues at a steady pace. Organizations and individuals need to be able to operate in a commercial and legal framework where criminal activity is minimized. In order to combat the malaise, the International Cybercrime Convention was signed by 30 States. However, the Convention raises a host of legal issues, the more egregious of which is its lack of data protection and human rights safeguards. Concerns about privacy dominate. Collection of personal information and the monitoring of information systems use will surely increase, and the general exchange of sensitive information between countries, some having data protection standards far below others, evokes concern. The potential opportunities to exploit data are growing exponentially because technological developments are lowering the cost of data collection and surveillance, while increasing the quality and quantity of the data.

International Cooperation is the treaty's most contentious aspect. The problem with the Convention lies not with what it criminalizes, but with the procedural powers for police to search and seize computer data, to investigate cybercrimes outside their state, and to receive mutual assistance in cross-border investigations without increasing protection for personal privacy. For example, it will allow countries to exchange information without considering data protection. The Convention reflects a one-sided concern with the interest of the criminal investigation service and favours the interest of law enforcement agencies over individuals. Right to search and seizure, interception and retention and storage of data must be proportionate and subject to jurisdiction equivalent to that employed in the offline world. When law enforcement officers need information that is not publicly available, they should be required to obtain a warrant from a court prior to requesting data from an Internet Service provider. The warrant should be specific and should be valid for a limited period of time.

Citizens and businesses should be able to rely on the safe working of the infrastructure. This means protecting it against criminal attack or e-crime. This is not achieved by diverting attention to issues, such as child pornography or drug running, which deserve separate, urgent consideration and treatment. Cybercrime should place its emphasis on crimes against the information infrastructure itself, rather than on traditional crimes. Action should focus on ensuring safe operation of the infrastructure: protecting it against criminal attacks such as hacking, viruses, denial of service etc.

Trust and confidence are key factors for the successful growth of electronic business. Business confidence will be undermined if disproportionate interception and data retention are imposed. Firms are wary of the provision on corporate liability as the strict liability clause imposes untenable obligations on corporations to monitor employee Internet usage.

The requirements of the Convention fail to balance the need for a criminal crackdown with the equally critical need to maintain basic freedoms and respect to individual rights and its economic impact. Combating cybercrime should not lead to the crime of violating the fundamental rights of privacy and data protection of cyber users.

REFERENCES

Akdeniz, Y. (2003). An Advocacy Handbook for the Non Governmental Organizations. Cyber-Rights and Cyber-Liberties

Bannisar, D. (2000). A Draft Commentary on the Council of Europe Cybercrime Convention. Retrieved 1 July,2005, from, ttp://www.privacyinternational.org/issues/cybercrime/coe/

Convention on Cybercrime is available at: http://conventions.coe.int/Treaty/en/

Crawford, S. (2004, December 19). Cybercrime Convention. Retrieved 1 July, 2005, from, http://scrawford.blogware.com/blog/_archives/2004/12/19/209645.html

Froomkin, M. (2004, March 19). Cybercrime Treaty Goes Live. Retrieved 1 July 2005 from, http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html

Germany to Ratify Cybercrime Pact. (2004).German American Journal: SSL. Retrieved 16 March 2005, from http://www.recht.us/amlaw/2004/09/21#z0921cooperation.

Loeb, M. & Gordon, L. (2004) CSI Computer Crime and Security Survey: The 2004 Annual Computer Crime and Security Survey. Computer Crime Research Centre. PRnewswire. Retrieved 1 July, 2005, from,crime-research.org/news/11.06.2004/423

Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime. Council of Europe Octopus Program. Retrieved 1 July, 2005, from, http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/

Poulsen, Kevin. (2004, April 24).US Defends Cybercrime Treaty. Security Focus. The Register. Retrieved 1 July, 2005, from, http://www.theregister.co.uk/2004/04/24/us_defends_cybercrime_treaty/

Regan, K. (2005,June 27). Supreme Court Ruling Deals Blows to P2P Firms. Ecommerce Times. Retrieved 1 July, 2005, from, http://www.ecommercetimes.com/story/44188.html

Rosen, M. (2002). The EU-US Convention on Cybercrime. UCLA Journal of Law and Technology. Notes 19. Retrieved 1 July, 2005, from, http://www.lawtechjournal.com/notes/2002/19_020819_rosen.php

Sobel, D. (2000, December 1).Independent Review of the Carnivore Technical System. EPIC. Retrieved 1 July 2005, from, http://www.epic.org/privacy/carnivore/review_comments.html

2004 E-Crime Survey. (2004). Carnegie Mellon Software Engineering Institute. Retrieved 8 March, 2005 from www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf

[1] A recent well known case illustrates the true danger of Internet surveillance for human rights: on October 7th 2004 the servers of the Independent Media Community -known as Indymedia- were seized by the FBI. While the reasons for this act remain still unveiled, Rackspace, the UK-based Indymedia host server, claims that it acted "in compliance with a court order pursuant to a Mutual Legal Assistance Treaty (MLAT)". This episode clearly shows how international legislation can easily be used to undermine freedom of expression. http://www.choike.org/nuevo_eng/informes/2450.html)