Cyber-policing: the role of the police in fighting cybercrime

Tatiana Tropina
Germany

(2009 Conference in Bad Hoevedorp)

Introduction

The recent growth of ICT ([1]) has brought all the opportunities provided by its global character and easy usage of new technologies for the development and facilitation of business processes or communications in the legal sector and within wider society. At the same time, it has also provided new possibilities for criminals who can exploit the same advantages offered by these technologies. The growing number of internet users offers society the perspective to speed up communications in everyday life and for commercial purposes, to lower the transactions and the costs of doing business, to increase the availability of information for educational purposes and to facilitate the development of such services as e-government. However, with the creation of new opportunities for economic and social development, the distribution of new technologies changes the criminal landscape and generates challenges for government and society with regard to the use of these instruments for criminal purposes. Cyberspace constantly remains the greatest source of different illegal activities that include not only new types of crime, such as hacking or malicious codes and programmes, such as 'spam', but also the migration of traditional crime, such as child pornography, fraud and copyright infringements to the ICT networks.

The fight against cybercrime requires the adoption of effective substantive criminal legislation and procedural instruments that allow for the investigation and prosecution of the misuse of the ICTs for committing crime. In addition, the international dimension of internet-related crime and the cross-border nature of ICT networks also evoke the need for harmonisation of legislative approaches and coordinated actions in preventing and investigating cybercrime on different levels: national, regional and international (Gercke, 2006, 2009). Furthermore, since the networks are mainly privately owned, the comprehensive strategy of addressing cybercrime also includes the development of the tools for effective cooperation with industry, the private sector, encouraging the application of co-regulation and self-regulation tools. Every actor in this multi-stakeholder environment of fighting and preventing crime in cyberspace faces a number of challengers, that could be either general problems emerging due to the global nature of internet or unique issues related to the changing nature of duties, responsibilities and functions of the stakeholders which used to operate in the real world and are now in charge of addressing crime in cyberspace. The police as a body responsible for maintaining public order and detecting, monitoring and preventing crime is one of the actors on this scene that faces great number of challenges (Wall, 2007) related to the migration of old crime to the ICT environment and the emergence of the new forms of criminal activity (Quille, 2009; Kozlovski, 2005; Wall, 2007).

This chapter provides an analysis of the problems that police organisations are currently facing as a result of new threats emerging with the spread of communication technologies; and investigates the opportunities for

([1]) Information and Communication Technologies.

addressing the problem of policing cyberspace. The first section examines the role of the police in fighting cybercrime and the problems of addressing the new threats in this area, while the second part focuses on the opportunities for developing new tools to meet the challenges, capacity building and possibilities for cooperation. Finally, conclusions are drawn to highlight the need for reviewing the concept of police activity in the real world to address the challenges emerging in cyberspace, as well as the necessity for capacity building and cooperation in a multi-stakeholder environment.

The role of the police in fighting cybercrime: problems and challenges

The existing approaches to fighting crime in the real world often do not work in cyberspace or cannot be applicable to the misuse of ICT for criminal purposes. The development of a comprehensive approach addressing different aspects of cybercrime goes along with the unique challenges that are new for legislators as well as for investigatory bodies, and must be taken into consideration when developing strategies to fight crime in virtual world:

- Number of users. The spread of internet use in people's everyday lives and as a way for doing business is the driver for dramatic growth in the number of users in recent years. In 2005 the number of first-time internet users in developing countries exceeded the number in industrialised states. (Development Gateway's Special Report, Information Society — Next Steps?, 2005) The increasing number of users connected to the global communications network represent a challenge for policing cyberspace because, firstly, one of the main weak points which presents an opportunity to criminals is the lack of the understanding of individual security online along with the application of social engineering techniques (Rash et al., 2009); and, secondly, while identity theft, spam and phishing activities can be performed automatically (Berg, 2007; Ealy, 2003) without investing much money or effort, it is very hard to automate the process of investigation (Gercke, 2009, p. 65).
- The availability of tools and information. The internet was designed as a network with open access to information, and nowadays criminals can easily find either information or tools to commit crimes online (Gercke, 2009, p. 65). The availability of software and devices that allow hacking password protection, automating attacks, the possibility of using search engines and robots for illegal purposes (Long, Skoudis and van Eijkelenborg, 2005; Dornfest, Bausch and Calishain, 2006) and instructions on how commit crime offline facilitate the development of crime both in the real world and in cyberspace.
- Difficulties in tracing offenders. The different possibilities for hiding identity in the global ICT networks, and the various tools and ways for anonymous access, surfing and communications make it really difficult for law-enforcement agencies to trace offenders (Lovet, 2009). The opportunities for using proxy servers, anonymisers, unprotected public wireless networks (or breaching the passwords of wireless networks) and the use of anonymous communication services (Gercke, 2009, p. 75) are widely exploited by cybercriminals. When criminal activity involves different states, it is very hard to investigate such offences involving both an international aspect and hidden identity.
- Missing mechanisms of control (Gercke, 2009, p. 75). The internet was not designed to be governed vertically. The horizontal structure and decentralised architecture of the network impede control over activity on the internet and hamper the investigation of crimes committed in cyberspace. The co-regulatory and self-regulatory approaches of the private sector and cooperation with owners and operators of the infrastructure as well as with internet service and host providers are necessary when addressing the problem of ICT misuse (Sieber, 2010; Sieber 2000, pp. 319-399).
- The absence of borders in cyberspace and the international component of cybercrime. Criminal law and criminal investigations are considered a question of national sovereignty, while the protocols applied for internet data transfers are based on the most optimal routing meaning that data transfer processes go through more than one country (Sofaer & Goodman, 2001, p. 7). Moreover, since cyberspace has no borders, criminals and victims can be located in different countries or even different continents, which requires the cooperation of all countries involved in an international investigation (Putnam & Elliott, 2001, p. 35 et seq.; Sofaer & Goodman, 2001, p. 1 et seq.). However, the permission of the local government when exercising investigations on other states' territories is required under the principle of national sovereignty [2] (Roth, 2005). While it takes time to meet formal requirements for cooperation, the investigation could be often hindered (Gercke, 2006, p. 142; Sofaer & Goodmann, 2001, 16), evidence and traces are usually very vulnerable and can disappear

[2] National sovereignty is a critical principle of international law.

a very short time after a crime is committed. The states, which have no frameworks for cooperation on cybercrime issues, can become safe havens for offenders that want to hamper the process of investigation. Furthermore, the internet still makes it possible to be physically present in one state while committing a crime in another state; offenders can also exploit gaps in substantive criminal law, by operating from countries that have no effective cybercrime legislation.

The role that the police are supposed to play in fighting cybercrime, is challenged by all these issues. Not only investigation of crimes in cyberspace is complicated, but also policing of cyberspace in general tends to be impeded. It is very hard for police units to start investigations because of the low visibility of such crimes and the lack of reporting (Lovet, 2009, p. 69) that could happen due to different reasons: from the unwillingness of commercial entities, especially financial companies to report to the police on account of reputational questions and negative publicity to the lack of knowledge that such a crime could be reported or lack of trust in the police (CSI and FBI, 2004, 19; Wall, 2007, 193). Because of the low reporting rate, lack of resources and under-reporting law-enforcement agencies have no possibility to investigate and prosecute more than a 'tiny fraction' (Vogel, 2007) of what is happening in cyberspace. Moreover, it is very hard for police units to justify the impact on public interest of initiating an investigation, especially in the case of a low impact, single crime with the one victim (Wall, 2007, p. 191). Since use of internet and ICT technologies provides offenders with the opportunity to create aggregated revenue with low impact on one victim (e.g. stealing 1 euro millions of times rather than millions of euros only once), one of the most important challenges for the police is the justification of a public order breach and the initiation of investigatory procedures.

Furthermore, the next biggest challenge is the principle *Nullum Crimen, Nulla Poena Sine Lege* (Hall, 1937, p. 165) that plays a critical role in policing transnational and borderless cyberspace. Differences in criminalisation of various offences, cultural dissimilarities in consideration of the seriousness of the crime, the great disparity in what should be considered illegal, especially with regard to some sensitive areas like religious offences harden the process of cross-border investigations, sometimes even making it impossible. The issues of jurisdiction and dual criminality are usually considered a problem for legislators as well as the challenges of harmonisation of cybercrime legislation, however, police units are among those which are most affected by these challenges (Wall, 2007, p. 191).

In addition, finding the right balance between investigatory power and human rights, applications of safeguards and maintaining the open nature of the internet remain very serious problems of internet policing. On the one hand, the missing mechanisms of control, the initial design of the internet and the architecture of the network require the development of tools for policing cyberspace, mechanisms for monitoring ICT networks, prevention and detection of illegal activity in the internet. On the other hand, the initial idea of the internet as a room for open discussions, exchanging and sharing opinions and views, as well as the free flow of information should not be abandoned; thus, the challenge is also to maintain the openness of the network and its further developments that can benefit the legal sector.

Taking into account the demand for new skills to investigate crimes in cyberspace, the necessity to review policing concepts, such as the justification of a breach of public order, the applicability of techniques in policing the real world to the maintenance of order in virtual space, implementation of these instruments in a practical environment remains the highest priority. For instance, according to the Interpol National Central Bureau's (NCB) poll data issued in April 2009, 83 % of national bureaus had dedicated cybercrime units but lack capacity for high-profile incidents (Interpol, 2009, p. 11). Furthermore, the poll shows that 79 % of NCBs have no accreditation standards for advanced skills, 52 % have no national reporting system, only 40 % use Interpol tools such as I-24/7 and 32 % are still outsourcing capability for forensic activities (Interpol, 2009, p. 11). These figures clearly show that even the availability of international tools for cooperation being the prerequisite for addressing the problem of cybercrime, the required next important step is the development of effective mechanisms of utilisation of these tools and preparedness for participation in global mechanisms of cooperation on the national level.

Policing cyberspace: future agenda for addressing the problem

The unique challenges from cybercrime for policing cyberspace require reviewing traditional approaches to the concept of policing, application of new tools, both legislative and technical, for investigation, development of the skills of working with electronic evidence, ability to cooperate with industry players. One of the critical issues is also the capacity building, because the possession of the new technologies for investigation and detection of crime does not mean the ability to utilise them.

The global context of cybercrime calls for international cooperation and provides the opportunity for a stronger role of international and regional police organisations, such as Interpol and Europol, firstly, in facilitating trans-border cooperation between police units in different countries in policing cyberspace. This area of activity focuses on maintaining the mechanisms allowing effective operational cooperation, that is now conducted in the form of contact points (I-24/7 Network (Interpol, 2008a); ICAID (Interpol, 2008b)) and created the channels for information exchange and sharing (regional working parties, training). International and regional police organisations can assist countries in investigating individual cases ([3]) where higher-level help is needed due to the transnational character of the crimes or because of the lack of capacity in a particular country, or because of the necessity for independent expertise. Apart from helping police units in investigations, capacity building and information sharing, the focus should be also be directed towards the development of strategic partnerships with the private sector and ICT industry.

The existing initiatives of Europol and Interpol highlight the importance of fighting cybercrime by policing cyberspace, developing the ability to conduct investigations of online crimes and, which is even more important, by participating in different projects with the private sector to address current threats propelled by cybercrime. For instance, Europol introduced the agenda for fighting cybercrime that includes the establishment of hi-tech crime centres, the creation of the European Cybercrime Platform (Europol, 2008, 14) consisting of analytical work file on cybercrime (Cyborg), a common online reporting system at European level (I-CROS) and a knowledge management platform (exchange of best practices) (Quille, 2009). As part of the agenda, Europol in cooperation with the private sector, conducts a number of training programmes such as Falcone, AGIS and ISEC programmes that are aimed at building capacity among police units; and operates a working group on the harmonisation and coordination of cyber crime training (OSCE, 2008).

On the global level police initiatives are represented by the activity of Interpol (Gonzales, 2006) which regards the fight against cybercrime as a part of a global security initiative (Interpol, 2009), which includes computer forensic, online investigation, training, public-private partnership, review and evaluation of technology and law enforcement. As part of the agenda for the creation of effective mechanisms for policing cyberspace, Interpol intends to operate both on the level of regional working parties (Africa, the Americas, Asia and the South Pacific, Europe, and the Middle East and North Africa) and on the global level, facilitating sharing information within participants. The mandate of Interpol includes the functioning of global 24/7 network which represents an early-warning system between IT crime investigation units in different countries and aims to facilitate operational contacts between Interpol National Central Reference Points (NCRP) for computer-related crime (Interpol, 2008a).

Furthermore, Interpol runs and maintains the Child Abuse Image Database (ICAID (Interpol, 2008b)) that facilitates the sharing of images and information to help law-enforcement agencies identify victims and offenders ([4]). The database contains hundreds of thousands of images. Moreover, the system uses image-recognition software to compare details of where the abuse took place to connect images from the same series of abuse or images taken in the same location with different victims (Interpol, 2008b). One of the

([3]) E.g. in 2008, Interpol was asked by Colombia to carry out an independent forensic analysis of computers and hardware seized during an anti-narcotics and anti-terrorist operation on a Fuerzas Armadas Revolucionarias de Colombia (FARC) camp, in order to establish whether the equipment had been tampered with following its seizure. Interpol's team of forensic experts conducted an independent technical study and issued a report, which concluded that there was 'no evidence of modification, alteration, addition or deletion' in the user files. See: Interpol, Cybercrime, Factsheet, COM/FS/2008-07/FHT-02.

([4]) http://www.interpol.int/Public/ICPO/InterpolAtWork/iaw2008.pdf.

successful examples in which Interpol has exercised its mandate in child protection is the so-called Vico Case that represents an instance of effective international cooperation in solving problems related both to the technical side of ICT and the transnational character of the issue. The work of German police computer experts allowed successful production of clear images of the face of a paedophile, which had been digitally manipulated to mask his image in more than 200 images of child sex abuse posted to the internet. The global appeal launched by Interpol after unscrambling the suspect's face identified him after 11 days as Christopher Nail and facilitated his arrest in Thailand. The identification of the suspect and his arrest required coordinated activities between Interpol and police in several countries (Interpol media release, 2008).

As well as the unique Vico case that combined both legal and technical challenges, there are some long-term projects for police cooperation established to fight child abuse online. For example, the Virtual Global Taskforce (VGT) project was created with the aim of cooperation between Interpol and law-enforcement agencies (police organisations in Australia, UK, Italy, Canada and United States) to address the problem of child pornography and other forms of abuse of minors in cyberspace ([5]). At the European level, cooperation between Interpol, Europol and national police authorities in 14 countries across the EU is facilitated by CIRCAMP, a European Commission-funded network of law-enforcement agencies across Europe, including Europol and Interpol, operating with the aim of fighting child abuse in cyberspace ([6]).

In addition to the projects intended to increase the online safety of minors and investigate cases of crimes committed against children, a number of public-private partnerships have been created on various (national, regional, international) levels with the participation of police organisations to tackle different aspects of cybercrime, cybersecurity and policing cyberspace. Among them are forensic software development projects (e.g. Microsoft's COFEE software designed to help police in conducting investigations of cybercrimes ([7])), the IMPACT project ([8]), cooperation with social networks such as Facebook, different educational programmes, e.g. cooperation with IT-industry players, such as eBay ([9]) and academia, various universities conducting training courses and building capacity among police units.

Public-private partnerships nowadays can be considered one of the most promising ways of future policing cyberspace. Since private actors have played a dominant role in driving ICT sector development and innovation, and, as owners of infrastructure or possessors of direct access to it, industry plays a key role in fighting cybercrime. While governments have the power to establish legal order and to enforce it through police and law-enforcement agencies, the private sector has an in-depth understanding of various aspects of infrastructure and communications networks ([10]), expertise in the changing and converged ICT environment and greater adaptability to the new technologies and their utilisation. The competences and resources of both parties mutually complement each other, creating the ground for voluntary cooperation.

Cooperation between public and private sectors on investigating crimes in ICT networks creates a platform for better understanding of the issue of addressing and preventing cybercrime because neither police nor industry can effectively fight cybercrime alone (*Legal manual for combating cybercrime,* 2003). Law-enforcement agencies need the industry's expertise in complex ICT issues because police and prosecutors often suffer a lack of knowledge in this area, especially in comparison with ICT sector experts. Furthermore, police units often have no capability

([5]) http://www.virtualglobaltaskforce.com/.

([6]) http://circamp.eu/.

([7]) Microsoft COFEE http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

([8]) The International Multilateral Partnership against Cyber Threats (IMPACT) represents initiatives of training and skills development, security assurance, research and international cooperation programmes. It has the support of key intergovernmental organisations such as the ITU, UN and Interpol. See: IMPACT, ITU calls for borderless cybersecurity http://www.networkworld.com/news/2009/072009-impact-itu-calls-for-borderless.html; IMPACT and ITU's cybersecurity agenda www.itu.int/cybersecurity/gca/impact.

([9]) See e.g. *Freedom, security and justice: what will be the future?* — Public Consultation, response from eBay/PayPal, December, 2008

([10]) ITU Cybersecurity Gateway.

and resources to monitor all volume of suspicious internet communications 24/7 or to collect and store all ICT data. Criminal justice and successful crime investigations therefore depend to great extent on the ICT industry and internet service providers (Vogel, 2007) In turn, the private sector needs government expertise and enforcement power because no matter how big and powerful a corporation is within the ICT market, and its level of expertise and familiarity with the internet, it cannot investigate cybercrimes, network attacks and prosecute offenders because that requires the power of the state. Public-private partnerships can be conducted either as operational cooperation in specific cases or long-term campaigns (for example, cooperation on training courses, or monitoring and blocking illegal content in the internet, or setting up networks of contact points in both the private and the public sector (Vogel, 2007)).

The shared responsibility and cooperation between police and the private sector promises to be an effective way of enhancing the effectiveness of addressing cyber-related threats and also in the fight against cybercrime (Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, 2007). As has been pointed out in a number of studies and publications, such cooperation along with developing co- and self-regulation could deliver even better results than criminal law enforcement (Sieber, 2000, 319-399; Sieber, 2010).

Conclusions

The fight against cybercrime needs a comprehensive approach including the development, application and revision of technical and legal measures, along with the building of organisational structures to address the problem. Furthermore, addressing cybercrime requires effective international coordination on cyber-related issues that must be built on policy coordination at the national level. (WGIG Report, 2005) The multi-stakeholder approach implemented on the national level has to be coherent with the international harmonisation of tools for addressing cybercrime in order to be efficient. Efforts of national governments in establishing policies and legal measures need to be supported (WSIS Declaration of Principles, 2003) ([11]) by the technical and economical expertise of the private sector, the readiness of civil society, and facilitated by the activity of intergovernmental and international organisations developing common standards and harmonising approaches. Despite the number of challenges that need to be addressed, police units and organisations, as one of the main stakeholders on the scene of fighting cybercrime, can act as a central spin-off for building links between different stakeholders, establishing cooperation with the private sector and developing the national and international approaches to tackling the problem of ICT misuse.

([11]) The importance of roles of all stakeholders is especially highlighted in the WSIS Declaration of Principles, 2003, available at: http://www.itu.int/wsis/docs/geneva/official/dop.html

References

- Berg, T. (2007), The Changing Face of Cybercrime — New Internet Threats Create Challenges to Law Enforcement, Michigan Bar Journal 2007, pp. 18-22
- Brenner, S.W. and Clarke, L.L. (2005) Distributed Security: a New Model of Law enforcement, John Marshall Journal of Computer & Information Law, Forthcoming. Available at SSRN: http://ssrn.com/abstract=845085
- CSI and FBI (2004) Computer Crime and Security Survey, San Francisco
- Communication from the Commission to the European Parliament the Council and the Committee of the Regions (2007) Towards a general policy on the fight against cyber crime, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF
- Development Gateway's Special Report, Information Society — Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.
- Dornfest, R., Bausch, P. and Calishain, T. (2006) Google Hacks: Tips & Tools for Finding and Using the World's Information. O'Reilly Media, Sebastopol, CA.
- Ealy, K (2003) A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://netsec.persiangig.com/Training/E-Book/General %20Hacking %20Methods.pdf.
- Europol (2008) Annual Report 2008.
- FBI (2004) Computer Crime and Security Survey, San Francisco.
- Freedom, Security and Justice: What will be the future? — Public Consultation. Response From E-Bay / Paypal. December, 2008.
- Gercke, M. (2006) The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International. available at: http://www.unafei.or.jp/english/pdf/RS_No79/No79_05VE_Gerke.pdf
- Gercke, M. (2009) Understanding Cybercrime: A Guide for Developing Countries, ITU, Geneva. available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- Gonzales, S. T (2006) Interpol's Role in Fighting Cybercrime. available at: http://www.nyu.edu/intercep/lapietra/Interpol_Cyber.pdf
- Hall, J. (1937), Nulla Poena sine Lege, *Yale L. J.*, *47*, pp. 165-93.
- Interpol (2008a) Cybercrime. Factsheet, COM/FS/2008-07/FHT-02.
- Interpol (2008b) Crimes against children. Factsheet, COM/FS/2008-07/THB-03.
- Interpol (2009 Interpol's Global Security Initiative for the 21st Century. Microsoft Public Safety Symposium. 14-16 April 2009. Redmond, WA, USA.
- Interpol media release (2008) Thai Court jails paedophile arrested after Interpol's global appeal, available at: http://www.interpol.int/Public/ICPO/PressReleases/PR2008/PR200840.asp
- Kozlovski, N. (2005) A Paradigm Shift in Online Policing — Designing Accountable Policing, Yale Law School Dissertation, June 2005 available at: http://crypto.stanford.edu/portia/papers/Kozlovski.pdf
- Legal Manual for Combating Cybercrime (2003) I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 137–141 available at: http://iospress.metapress.com/content/ldpya76u2r9lgqpb/
- Long, J., Skoudis, E. and van Eijkelenborg, A. (2005) Google Hacking for Penetration Testers, Syngress.
- Lovet, G. (2009) Fighting Cybercrime: Technical, Juridical and ethical Challenges, Virus Bulletin Conference, September 2009. available at: http://www.fortiguard.com/papers/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf
- Microsoft COFEE // http://www.microsoft.com/industry/government/solutions/cofee/default.aspx
- OSCE (2008) Report Annual Police Experts Meeting 'Fighting the Threat of Cyber Crime' Vienna, 30 and 31 October, 2008.
- Putnam, T.L. and Elliott, D.D. (2001) International Responses to Cyber Crime, in: Sofaer, A.D. and Goodman S.E. (ed.) Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press, pp. 31-67; available at: http://media.hoover.org/sites/default/files/documents/0817999825_35.pdf
- Quille, M. (2009) Keynote Address. Current Threats and Future Challengesposed by cybercrime. Octopus Conference, CoE.
- Rash, H. et al. (2009) Crime Online. Cybercrime and Illegal Innovation. NESTA. Research Report. July, 2009. available at: http://eprints.brighton.ac.uk/5800/1/Crime_Online.pdf
- Roth, B. (2005) State Sovereignty, International Legality, and Moral Disagreement, available at: http://www.ihrr.net/ss08-global-justice-theory/view-category/Page-2?mosmsg=You+are+trying+to+access+from+a+non-authorized+domain.+ %28www.google.at %29

- Sieber, U. (2000) Legal Regulation, Law Enforcement and Self-regulation, in: Watermann, J. and Machill, M. (eds.) Protecting Our Children on the Internet, Gütersloh, Bertelsmann Foundation Publishers.
- Sieber, U. (2010) Internet Crimes — Annex 1 to the Questionnaire for the 18th International Congress of the IACL.
- Sofaer, A.D. and Goodman, S.E. (2001) Cyber Crime and Security — The Transnational Dimension in: Sofaer, A.D. and Goodman S.E. (ed.) Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press.
- VGTF http://www.virtualglobaltaskforce.com/
- Vogel, J. (2007) Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico.
- Wall, D.S. (2007) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, Police Practice and Research, 8:2, 1, 2007.
- WGIG Report (2005) available at: http://www.wgig.org/docs/WGIGREPORT.pdf
- WSIS Declaration of Principles (2003) available at: http://www.itu.int/wsis/docs/geneva/official/dop.html