

CYBER CRIMES AND E_GOVERNMENT APPLICATIONS: SOME EMPIRICAL EVIDENCES.

Massimo, Pollifroni, Department of Business Administration, Faculty of Economy,
University of Turin, ITALY
pollifroni@econ.unito.it

Abstract

Computer technology presents many new challenges to social policy regarding issues such as privacy, as it relates to data mining and criminal investigations. Cyber crime consists of specific crimes dealing with computers and networks (such as hacking) and the facilitation of traditional crime through the use of computers (hate crimes, telemarketing /Internet fraud, etc.).

The paper wants to discuss the most important connections between cyber crimes and eGovernment applications. To counteract cyber crimes the costs of eGovernment initiatives are almost always underestimated because of two reasons: under-appreciate their complexity and lack good models or guides for identifying all cost factors. New technologies offer the possibility for governments to become far more responsible to the will of the people, to work and make the democracy work better than ever before. They offer governments the opportunity to achieve a quantum leap towards tomorrow's democracy. This is one of those exciting moments in the history when leaders and authorities are challenged to act. New challenges ask for new co-ordinated responses. Networks are not stopped by national borders, so governments should co-operate in order to take advantage of the new opportunities and to limit the risks they make arise.

Keywords: Cyber crimes, eGovernment, Government Policy.

JEL Code: L98, M1, M21.

1 CIBER CRIMES: DEFINITIONS AND CLASSIFICATIONS

Cyber crime (or Cybercrime) consists of specific crimes dealing with computers and networks (such as hacking) and the facilitation of traditional crime through the use of computers (hate crimes, telemarketing /Internet fraud, etc.) (cyber crime is also names as e-crime: a general label for offences committed using an electronic data storage or communications device.).

The Oxford Reference Online defines cyber crime as “*crime committed over the Internet*”. *The Encyclopedia Britannica* defines cyber crime as “*any crime that is committed by means of special knowledge or expert use of computer technology*”¹. Cyber crime could reasonably include a wide variety of criminal offences and activities. The scope of this definition becomes wider with a frequent companion or substitute term “*computer-related crime.*” Examples activities that are considered cyber crime can be found in the *United Nations Manual on the Prevention and Control of Computer-Related Crime*. The manual includes fraud, forgery, computer sabotage, unauthorised access and copying of computer programs as examples of cyber crime² (NISER³, 2004).

In addition to cyber crime, there is also “*computer-supported crime*” which covers the use of computers by criminals for communication and document or data storage (Iqbal, 2004.). While these activities might not be illegal in and of themselves, they are often invaluable in the investigation of actual crimes. Computer technology presents many new challenges to social policy regarding issues such as privacy, as it relates to data mining and criminal investigations⁴.

There has been a discernible shift in the threat landscape. Attackers are moving away from large, multipurpose attacks on network perimeters and concentrating instead on more focused attacks on client-side targets. This new threat landscape will likely be dominated by emerging threats such as, e.g.: customizable modular malicious code, Bot networks and targeted attacks on Web applications and Web browsers. Moreover, where traditional attack activity was motivated by curiosity and a desire to show off technical virtuosity, the new threats are motivated by profit.

Pavan Duggal (Duggal, 2002), who is the President of cyberlaws.net and consultant⁵, in a report has clearly defined the various categories and types of cyber crimes (Gulapa, 2006). Cyber crimes can be basically divided into three major categories:

- *Cyber crimes against persons;*
- *Cyber crimes against property;*
- *Cyber crimes against government.*

Cyber crimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cyber crimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one cyber crime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled. The second category of cyber crimes is that of *Cyber crimes against all forms of property*. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.. The third category of cyber crimes relate to *Cyber crimes against Government*. Cyberterrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual “*cracks*” into a government or military maintained website (Duggal, 2002).

The emerging new targets that will become prominent over the current year include the following risks⁶: Modular malicious code, Bot networks, Phishing targets, Adware/spyware, Wireless security, VoIP threats, Shift to non-PCs and IM (Instant Messaging). These risks are explained in the following points.

- *Modular malicious code.* This is malicious code-such as worms, viruses, and Trojans-that initially possesses limited functionality; however, once installed on a target computer, it downloads other pieces (or modules) of malicious code with different functionalities and further compromises the infected computer.
- *Bot networks.* Bots (short for “robots”) are programs that are covertly installed on a user’s computer in order to allow an unauthorized user to control the computer remotely. Symantec has determined that there is strong correlation between the number of Bot computers and the number of denial-of- service attacks. Over the next year it is expected that there will be a more coordinated community of Bot network computers carrying out more sophisticated, targeted attacks.
- *Phishing targets.* Phishing⁷ has evolved from simple attempts to obtain small items of information like gaming passwords to all-out identity theft. Because there are far more small targets (such as regional banks) than large ones (like credit card companies) and because smaller targets generally present fewer challenges for attackers, the number of phishing targets will most likely continue to grow.
- *Adware/spyware.* As cellular telephones, PDA’s, and hybrid devices become more prevalent, it is reasonable to assume that security threats, such as spyware/adware will increasingly target them.
- *Wireless security.* The growing number of people using wireless connectivity has brought a corresponding increase in the number of concerns posed by insecure wireless access points.
- *VoIP threats.* According to a recent study, by the end of this year, it is expected that two-thirds of the Global 2000 companies will have adopted VoIP (Voice over Internet Protocol) as their primary means of voice communication. The introduction of VoIP on enterprise networks in the absence of appropriate security measures could introduce another entry point for attackers to exploit⁸. (In October, Skype Technologies warned that flaws in its Internet telephony software could allow attackers to take control of a user’s system.)
- *Shift to non-PCs.* One of the biggest developments over the next year will be attacks and attempts on alternative devices and platforms. As networked and user devices gain more intelligence and more computing power, they may become targets (for example: router, switch backup device). Also cell phones and mobile devices will become ripe for hacking as software becomes interoperable and financial data are loaded onto their hard drives and networks.
- *IM (Instant Messaging).* The rapid adoption of IM networks by corporate users makes instant messaging a viable vehicle for malicious threats. Real-time communication solutions like IM create a new attack vector for threats to enter an enterprise network. IM worms are also the most dominant threat type hitting the public IM networks, and all of the popular networks have been attacked; for the new generation of financially motivated hackers, 2006 will present numerous opportunities to develop increasingly more sophisticated attack methods; for today’s real-time enterprises, that makes 2006 a year in which they must take aggressive steps to minimize the risk of business disruption due to information security threats.

Every government has played a key role in both the development of information technology and in the efforts to deal with new challenges that arise from its use. Solutions to the new challenges posed by information technology are inherently horizontal in nature and require an inclusive approach to policy development, involving a wide variety of stakeholders both inside and outside government. Various government departments and agencies deal with cyber crime, such as the “RCMP’s Computer Crime Prevention” website, as well as the integrated partnership between International, Federal and Provincial law enforcement agencies, at “Reporting Economic Crime On-Line” (or RECOL)⁹. Other federal government departments working on national security, criminal justice, the private sector, foreign policy, critical infrastructure and social issues are all involved in the ongoing efforts to develop solutions to this increasingly prevalent crime. In this study we remark international

organizations such as the G8 High-Tech Sub-Group of Lyon/Roma Anti-Crime and Terrorism Group, the Committee of Experts on Crime in Cyberspace of the Council of Europe, and most recently, at the Organization of American States (OAS) and the Working Group to Prepare a “*Draft Cybersecurity Strategy*” for Member States (Clarke, 1999, 2001) (Draetta, 2004).

Harmonisation has seen both the extension of existing law and the creation of new law (Garnett, 2004). There have also been moves towards international harmonisation (and national harmonisation within federal states), most prominently through the development of model criminal codes such as the Council of Europe's Convention on Cybercrime (Russell et al., 2004).

2 THE COUNCIL OF EUROPE'S CONVENTION ON CYBER CRIME

Since the late 1980s, the CoE (Council of Europe) has been working to address the growing international concern over the threats posed by hacking and other computer-related crimes. In 1989, it published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks (Esterle et al., 2005). This was followed by a second study, published in 1995, which contained principles concerning the adequacy of criminal procedural laws in this area. Building on the principles developed in the 1989 and 1995 reports, in 1997 the CoE established a Committee of Experts on Crime in Cyberspace (PC-CY) to begin drafting a binding convention to facilitate international cooperation in the investigation and prosecution of computer crimes. The United States, represented by the Department of Justice, played a key role in the drafting stages, even though the USA was only an observer member of the Committee. The first publicly-released draft of the convention was Draft 19, which was made available for public comment in April 2000.

Several more drafts have been released since then, culminating in the final draft released on 29 June 2001¹⁰: the Convention has been submitted to the Council of Ministers for adoption and will be open for signature late in 2001 (Budapest, on 23 November 2001). An additional Protocol to the Convention on cyber crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems has been made on 2003 (Strasbourg, 28.I.2003)¹¹. The Convention on cybercrime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organisation.

The Convention aims principally at harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form setting up a fast and effective regime of international co-operation.

The Convention, accordingly, contains four chapters:

- Use of terms;
- Measures to be taken at domestic level – substantive law and procedural law;
- International co-operation;
- Final clauses.

Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights. Section 2 of Chapter II (procedural law issues) – the scope of which goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form – determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. It then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data. Chapter II ends with the jurisdiction provisions. Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties. Finally, Chapter IV contains the final clauses, which – with certain exceptions – repeat the standard provisions in Council of Europe treaties.

The next steps in E.U. Area, when awareness among users reached a high level, consists in providing proper software and services, offering better quality and making the Internet more attractive. Attackers always find new ways to overtake state-of-the art protection and even experienced network engineers and security experts are often surprised by the newness of some attacks.

What is required is an early warning system that can quickly alert all the users by advises teaching how to tackle attacks. Business also need this kind of system with the possibility of using more confidentiality, not to risk to loose consumers' trust. "*Computer Emergency Response Teams*" (CERT's) are entities that have done much work in this area. Every State in Europe has got one of this team that have the task to alert all the users about possible threats. Worldwide coordination is done through CERT/CC, where cooperation between US and Europe collaborate together¹². Cooperation is complex and these complexity have so far limited European joint actions. Despite clear difficulties cooperation remains the key word to ensure early warning throughout the Union through the exchange of information on the first sign of an attack. New technologies offer the possibility for governments to become far more responsible to the will of the people, to work and make the democracy work better than ever before.

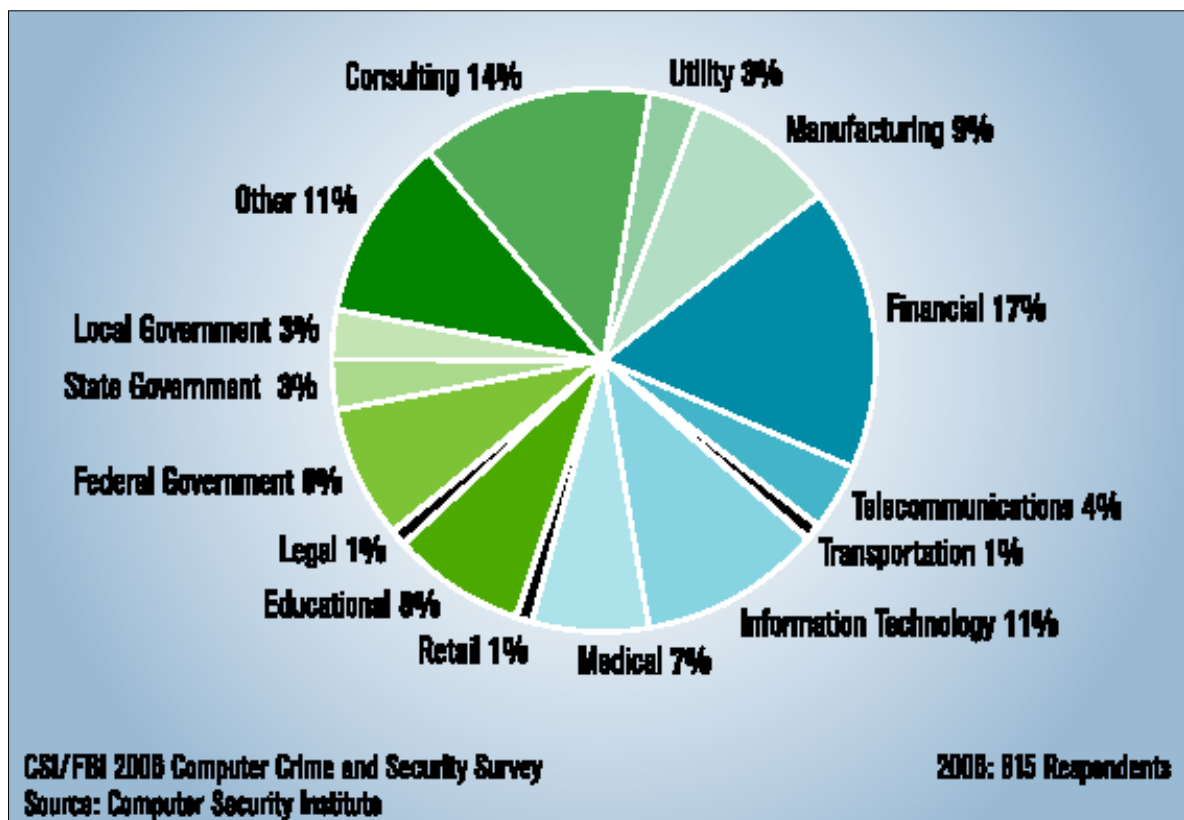
They offer governments the opportunity to achieve a quantum leap towards tomorrow's democracy. This is one of those exciting moments in the history when leaders and authorities are challenged to act (De Vel, 2002). New challenges ask for new co-ordinated responses. Networks are not stopped by national borders, so governments should co-operate in order to take advantage of the new opportunities and to limit the risks they make arise. Thanks to its over 50 years of international co-operation experience, the Council of Europe is ready to play its part, both as a standard setting body and as a service provider, on the international arena, to help public authorities and citizens to maximise the benefits of new technologies (De Vel, 2002).

3 SOME EMPIRICAL EVIDENCES FROM U.S. SECURITY INITIATIVES

The costs of eGovernment initiatives¹³ are almost always underestimated because of two reasons: under-appreciate their complexity and lack good models or guides for identifying all cost factors (Giacomello G., 2004.). Statistics may show the trend on cyber-crime activities but are not a reliable source to determine the actual position of the computer crime rate. Criminologists use the term "*dark figure*" to describe the undetermined actual position which refer to those undetected computer crimes activities. Several contributing factors below may explain why it is called "*dark figure*". First, the fast operational speed of today's computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity. Third, once criminal activity has been detected, many businesses are reluctant to lodge a report due to fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions (NISER, 2004).

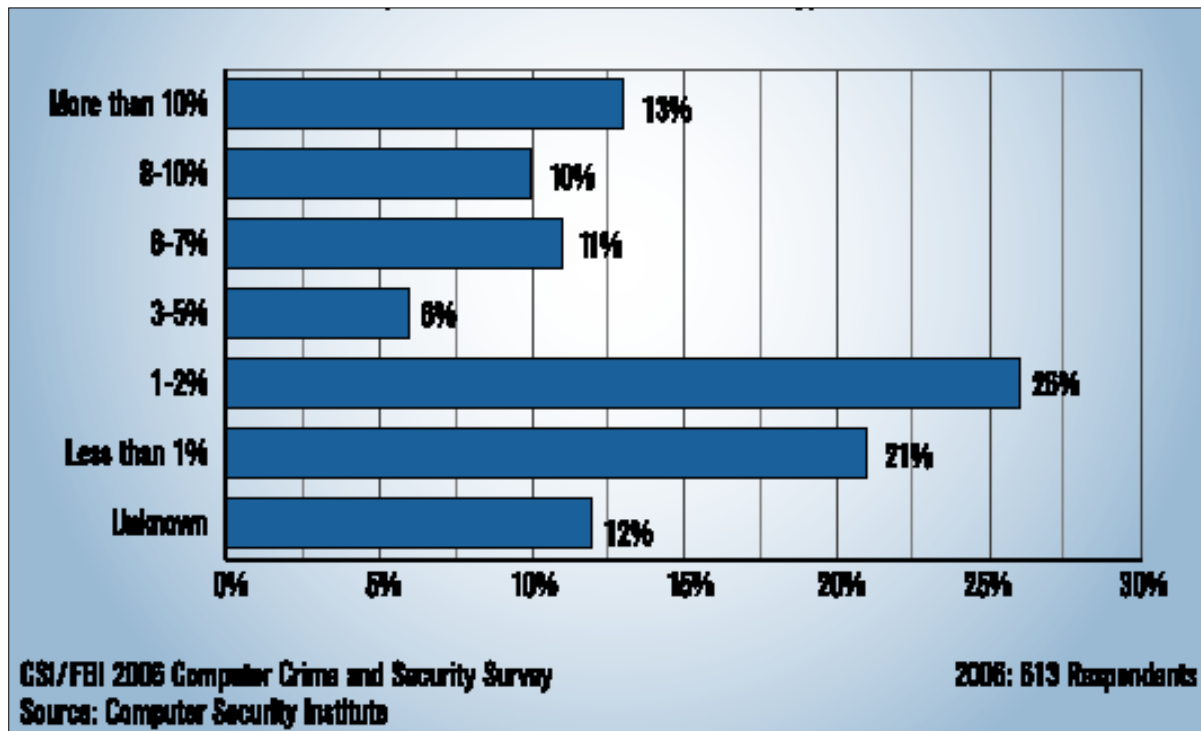
The cost estimation models we do have usually capture the cost of dedicated staff and purchases such as hardware, software, and consulting services. These costs are certainly real, but they fall short of the full costs of engaging in a new eGovernment effort¹⁴. According to "*The Computer Crime and Security Survey*"¹⁵, a study is conducted by the Computer Security Institute (CSI¹⁶) in conjunction with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey includes many areas from both private and public sectors (see [Figure 1.](#)): the sectors with the largest number of responses came from finance (17 %), followed by consulting (14 %), information technology (11 %) and manufacturing (9 %).

Figure 1. Respondents by Industry and Public Sectors. (Source: 2006 CSI, FBI Computer Crime and Security Survey).



The government agency portion (combining federal 8%, state 3% and local levels 3%) was 14 % (Gordon L. A., Loeb M. P., Lucyshyn W. and R. Richardson, 2006). [Figure 2](#) illustrates that 47 % of respondents indicated that their organization allocated less than 3 % of the total IT budget to security, which compares to 35 % in last year's survey. However, 34 % of respondents indicated that their organization allocated more than 5 % to security, and this compares to 27 % in last year's survey.

Figure 2. Percentage of IT Budget Spent on Security. (Source: 2006 CSI, FBI Computer Crime and Security Survey).



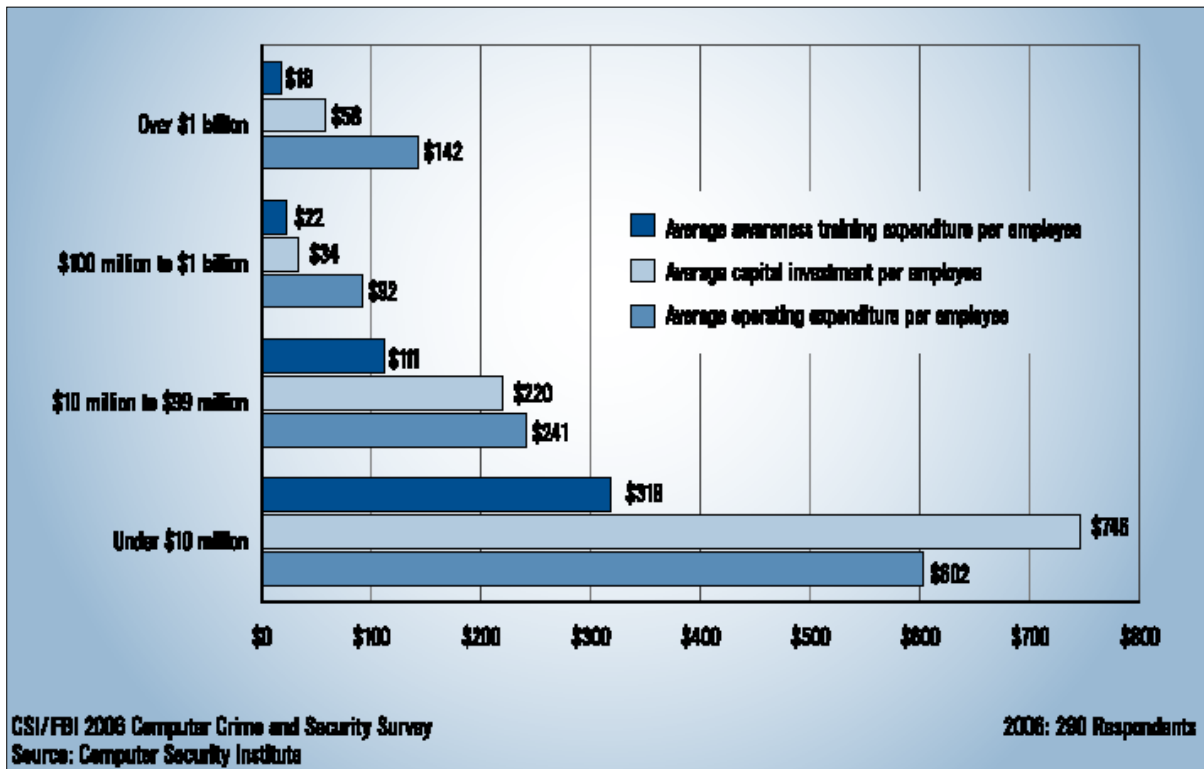
The percentage of respondents indicating that their organizations allocate between 3 and 5 % of their IT budgets to security activities declined from 24 % last year to only 6 % this year, indicating a shift to both higher and lower extremes (Gordon et al., 2006).

As can be seen from [Figure 3](#), the average awareness training expenditures per employee decrease with an organization's size. The smallest organizations, those with revenues of less than \$10 million, spend \$318 per employee and the largest organizations, those with annual revenues of over \$1 billion, spend \$18 per employee.

Thus, there appear to be economies of scale in providing awareness training. The average computer security operating expense and investment per employee - consistent with last year's results - initially displays economies of scale and then, diseconomies of scale. In particular, the average information security expenditure and investment per employee decreases as the organizations get larger, but then increases when moving to the largest organizations (those with over \$1 billion in revenue) (Gordon et al., 2006).

Improving the ability to identify all cost categories and estimate specific costs is a growing concern in public (and private) sector IT (Campbell et al., 2003). The increasing number of expensive and public failures has raised this concern to a leadership level (Modigliani et al., 1958). As a result, new tools and techniques are emerging to improve information technology investment planning and decision making¹⁷ (Gallaher et al., 2006).

Figure 3. Average Reported Computer Security. Expenditure per employee. (Source: 2006 CSI, FBI Computer Crime and Security Survey).



The factors necessary to success are the following:

- formal support:
 - in the form of legislation;
 - from upper management;
 - from the budget authority;
 - from the highest level of government involved in planning functions;
- a comprehensive state-wide strategic plan to help judge how well a new idea fits with the government's larger goals;
- good communication between legislative, budget, and IT functions and between the IT oversight agency and the procurement office.

There are six factors that influence the complexity of the cost of eGovernment projects¹⁸: 1) building, maintaining, and managing relationships; 2) the similarity of existing processes and work to the envisioned ones; 3) the similarity of existing technologies to desired technologies; 4) reparability of tasks; 5) intended degree of integration in the final product; and 6) variations in data sources.

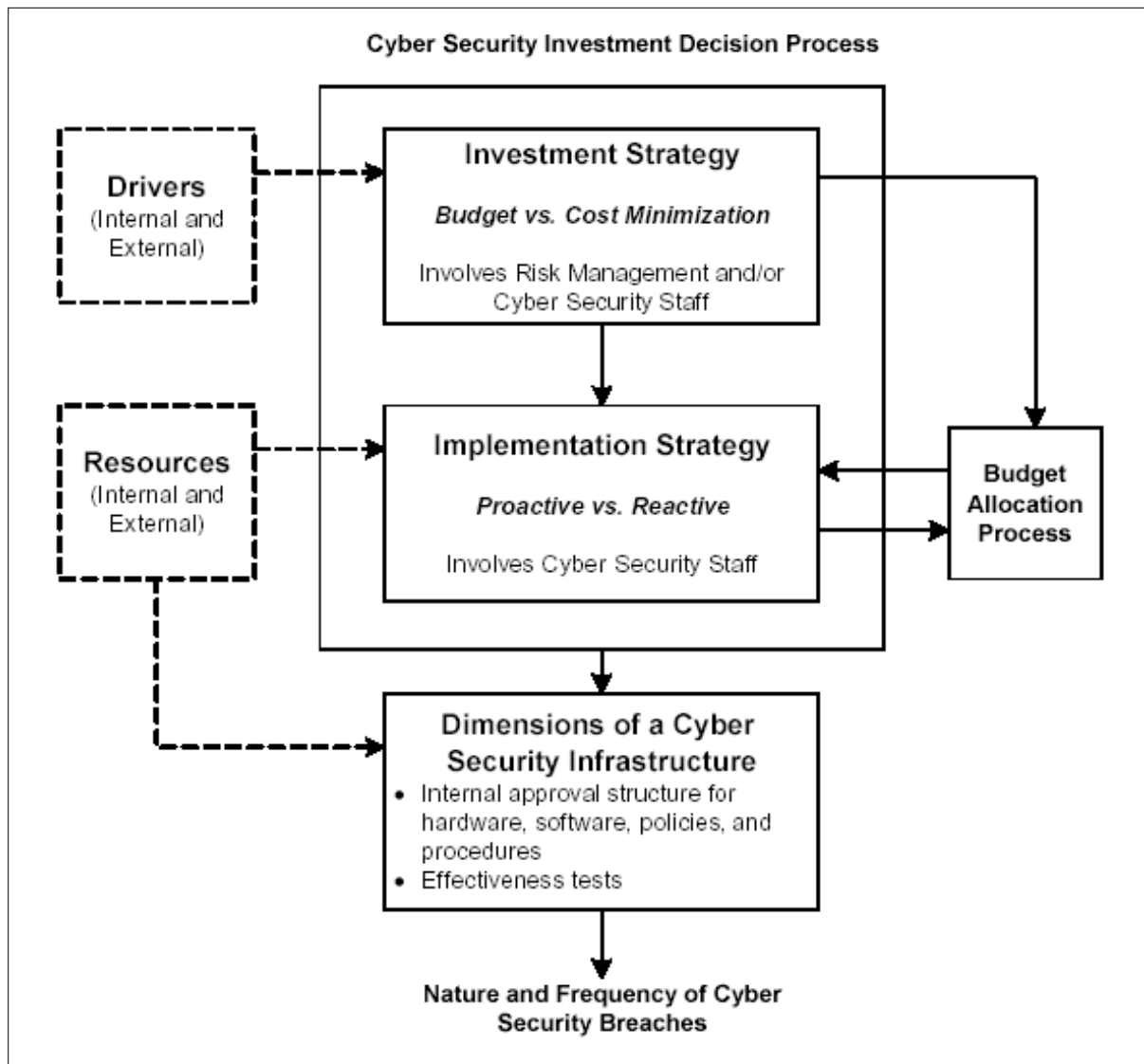
In addition it is necessary to consider the costs of information security, which are:

- Capital costs, such as hardware, software, networks, servers and switches.
- Administration costs, such as management of the assets, security monitoring and follow-up, legal assistance, and audit department.
- Technical support costs, when all the people call the help desk, documentation of the calls, end-user training, etc..

- End user operational costs, such as the management of user data of resources breached, awareness training of users.

All parts of an organization are affected by IT-related decisions; thus, all parts of an organization can potentially offer relevant views that could benefit the whole (Ryan, 1982; Schechter, 2004; Gordon et al., 2003). Therefore, management is beginning to realize that cyber security decisions should be viewed in terms of risk management. Every organization is vulnerable to the risk of a security breach, so protecting the privacy of the organization is a managerial issue of priority (Ross, 1978). Furthermore, many breaches can result in legal and human resources issues, so administrative units are becoming more involved in certain decision making, often related to the determination of user policies (Rowe et al., 2006). Schematically, [Figure 4](#) is a diagram of the flow of decision making and the information sources that act as inputs to this process (Rowe et al., 2006).

Figure 4. Diagram of Cyber Security Investment Decisions Inputs and Outputs. (Source: Rowe B. R. and M. P. Gallaher 2006. 'Private Sector Cyber Security Investment Strategies: An Empirical Analysis'. Presented at The Fifth Workshop on the Economics of Information Security (WEIS 2006), University of Cambridge, England: 7).



To segment the decision-making process, we make a distinction between analyses conducted as part of an investment strategy, where management determines security priorities and investment resources in light of overall business operations, as opposed to analyses conducted as part of an implementation strategy, where IT staff determine the most efficient approach to meet the organization's security needs. In smaller organizations, the distinction between these two decision processes is blurred: the same staff are involved and analyses are intermingled (Gordon et al. 2004). However, in larger organizations, organizational hierarchy leads to compartmentalizing different phases of the decision process that determine the overall level of cyber security (Rowe et al., 2006).

4 CONCLUSIONS

The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future (Stiglitz, 1988). Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities. A conspicuous feature of information technology is the impact it has had and will have on the evolution of telecommunications technology. Classical telephony, involving the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. Circuit-switched connections have been replaced by packet-switched networks. It is no longer relevant whether a direct connection can be established; it suffices that data is entered into a network with a destination address or made available for anyone who wants to access it (Varian, 2000). The pervasive use of electronic mail and the accessing through the Internet of numerous web sites are examples of these developments. They have changed our society profoundly. The ease of accessibility and searchability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has led to an explosive growth in the amount of information available and the knowledge that can be drawn there from (Varian, 2002). These developments have given rise to an unprecedented economic and social changes, but they also have a dark side (Anderson, 2001): the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries (Gordon et al., 2006). Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour (Sofaer et al., 2001; Taylor, 2006; Trachtman, 2006).

As I have said in the previous pages, technological revolution and cyber crimes regard also the Public Sector with reference to the e-government processes. The concept of e-government (or e-administration) is referred to the use of modern Information and Communication Technologies (ICT) linked to the development of electronics and the Internet in the modernisation process of the Public Administration (Pollifroni, 2003). The different processes of e-government may be analysed with reference to the various models, that the Public Institution may adopt during the modernisation process of the structure. The different e-government models are:

- G2C model (Government to Citizen model): this model concerns the activities carried out by the Public Institution towards citizens (for example to build Institutional Portal Web and to provide Internet on line services such as the presentation of the Individual Tax Return in electronic format, or the application of electronic documents by the Registry Offices, etc.).
- G2B model (Government to Business model): this model concerns the activities carried out by the Public Institution towards business companies (for example to provide Internet on line services

such as the presentation – in electronic format - of the following documents: Income Tax Return, Annual Report, etc).

- B2G model (Business to Government model): this model concerns the activities carried out by the Public Institution towards external supplier (for example e-procurement activities, e-auctions on line, etc.; in Italy these activities are made by Consip S.p.A., a Public Company of the Italian Treasury Department).
- G2E model (Government to Employees model): this model concerns the activities carried out by the Public Institution towards employees (for example to provide Internet on line services such as e-learning activities).
- G2G model (Government to Government model): this model concerns the activities carried out by the Public Institution towards other Domestic Public Institution (electronic integration between several Departments or between Central and Local Public Institution) or towards other International or Foreign Public Institutions (for example intelligence activities, International Co-operation actions, etc.).

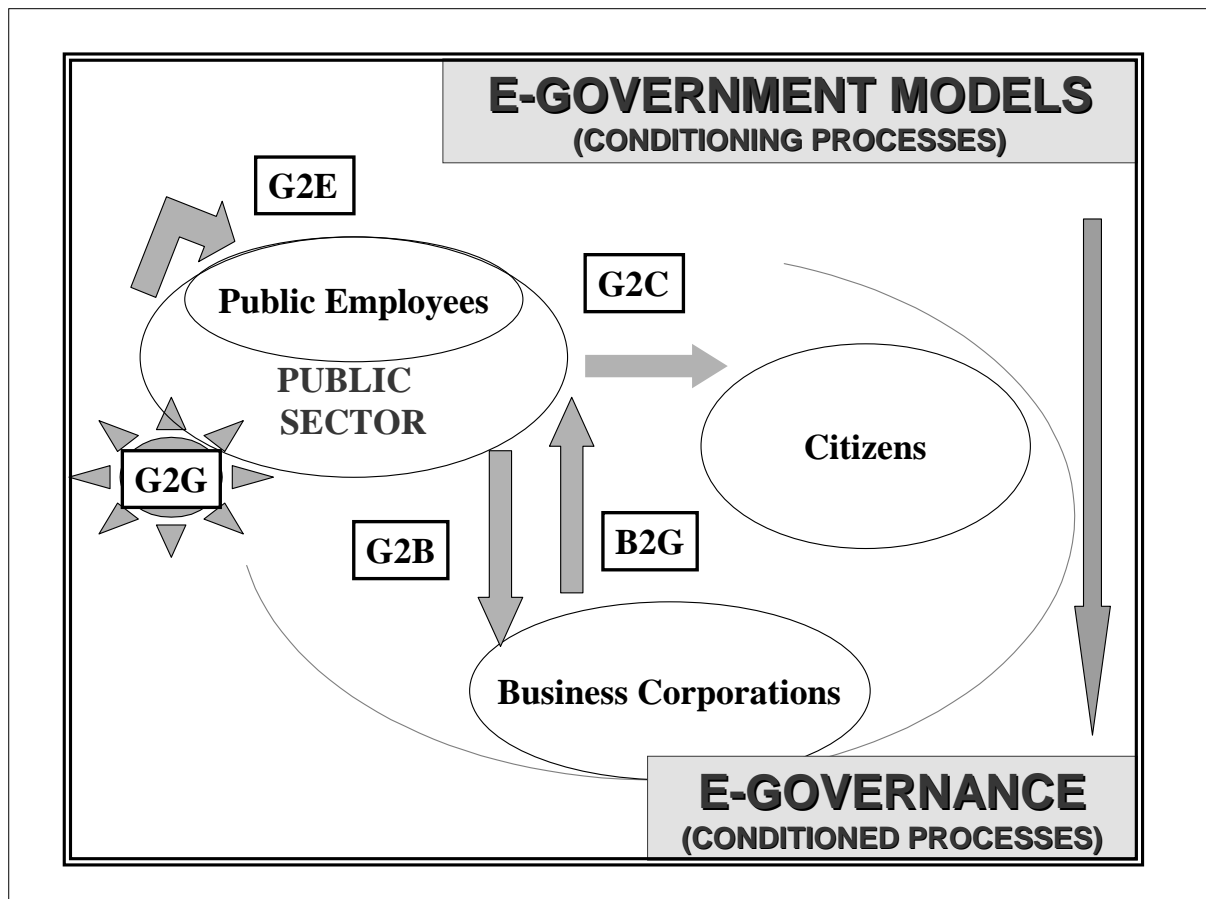
The development of the e-government processes (conditioning processes or causes) determines an improvement in the governance processes of the Public Institution that - using highly technological solutions - are named e-governance processes (conditioned processes or effects) (Ref. [Figure 5.](#)). Consequently, the e-governance is the second aspect of technological innovation applied to Public Administration processes: that is to say the possibilities for the improvement of the democratic participation processes offered by the new technologies (Pollifroni, 2005). The digital revolution multiplies the individual's possibilities of communication and interaction in an exponential fashion, making it possible to re-launch the classic idea of the individual at the center of the "*Res Publica*". These e-governance processes [also called digital democracy (or e-Democracy)] include, for example:

- direct participation of the employees to the internal decision of the Public Institution: these processes influence the internal governance with activities, e.g., of internal electronic poll, also called e-Decision;
- direct participation of the citizens to the political choices: these processes influence the external governance of the Public Institution by e-Voting activities.

So it is possible to conclude that cyber crimes concern also the digital democracy (or e-Democracy) for the improvement of the democratic participation processes offered by the new technologies (e.g., e-Decision, e-Voting, etc.), where this technology is used to give more power to citizens, facilitating access to civil and political rights. It is also possible to underline that the new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory (Pekari, 2004; Podesta et al., 2005; Podgor, 2004). So, in a new eGovernment effort to contrast cyber crime it is necessary (FeiYan, 2004):

- to establish an international cooperation mechanism to build computer crime intelligence database to share information such as crime trends, digital evidence, crime clue and digital forensic technology;
- to introduce training initiatives to help the developing country to combat cyber crime by: establishing cyber crime reporting mechanism (setting up an online cyber crime complaint center in each country); enhancing digital forensic technology research; adopting standardized investigation procedure; improving technology support (cooperating with institutes, information technology enterprises, ISP, ICP and other organizations); training regularly;
- to develop international law, necessitating the adoption of adequate international legal instruments.

Figure 5. Relations between the E-Government Models and the E-Governance processes. [Source: Pollifroni M. 2005. 'The 'S-EPI MODEL': a Theoretical Model that links the E-Government processes to the Instruments of the Public Sector Social Responsibility'. In Proceeding of the International Workshop e_Government'05 (e_GOV'05), Workshop organised by the Brunel University, 13 September 2005, West London (GB)].



New technologies offer the possibility for governments to become far more responsible to the will of the people, to work and make the democracy work better than ever before. They offer governments the opportunity to achieve a quantum leap towards tomorrow's democracy (De Vel, 2002).

This is one of those exciting moments in the history when leaders and authorities are challenged to act. New challenges ask for new co-ordinated responses.

Networks are not stopped by national borders, so governments should co-operate in order to take advantage of the new opportunities and to limit the risks they make arise.

5 APPENDIX

In this appendix are reported the most important websites, agencies and organisations in the world on Cyber crimes.

- **Australia**
 - AusCERT (Australian Computer Emergency Reporting Team)
 - Australasian Centre for Policing Research : e-crime research and coordination
 - Australian Federal Police : e-crime
 - Australian High Tech Crime Centre
 - Baker and MacKenzie Cyberspace Law and Policy Centre, UNSW Faculty of Law
 - Business Software Association of Australia
 - CAUBE.AU - Coalition Against Unsolicited Bulk Email, Australia
 - Electronic Frontiers Australia
 - Internet Industry Association : Cybercrime Virtual Taskforce
 - Internet Industry Association : security portal
 - NetAlert - Australian Internet Safety Advisory Body
 - New South Wales Society for Computers and the Law
 - Oz NetLaw
 - Scamwatch
- **Canada**
 - Foreign Affairs Canada : International crime and terrorism
 - Information Technology Association of Canada : Cyber security and privacy
- **United States**
 - Cybercrime.gov : Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division, Department of Justice
 - Center for Democracy and Technology : Cybercrime
 - Computer Law Association
 - Crimes of persuasion : schemes, scams, frauds
 - Cyber Criminals Most Wanted
 - Internet Crime Complaint Center
 - Internet Fraud Watch
 - National Criminal Justice Reference Service: Internet safety | Electronic crime resources
 - National White Collar Crime Center
 - UCLA Institute for Cyberspace Law and Policy
 - University of Dayton School of Law : Cybercrime
- **United Kingdom**
 - Cyberspace Research Unit, University of Central Lancashire, Preston
 - Internet Crime Forum
 - Internet Watch Foundation
 - National High Tech Crime Unit
 - Society for Computers and the Law
- **International**
 - Business Software Alliance
 - Council of Europe : Cybercrime
 - Cybercrime Law : a global survey of cybercrime legislation
 - CyberAngels

- CyberLawEnforcement.org
- Fraud Watch International
- Inhope - the Association of Internet Hotline Providers in Europe
- International Association of Computer Investigative Specialists
- International High Tech Crime Investigation Association
- Internet ScamBusters
- International Web Police
- Interpol : information technology crime
- SaferInternet.Org
- Society for the Policing of Cyberspace
- Virtual Global Taskforce
- WiredSafety

References

- Anderson R. 2001. 'Why Information Security is Hard? An Economic Perspective'. Presented at the Annual Computer Security Applications Conference, New Orleans,
- Campbell K., Gordon L., Loeb M. P. and L. Zhou 2003. 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market'. *Journal of Computer Security* 11(3):431-448.
- Clarke R. 1999. 'Threats to U. S. National Security: Proposed Partnership Initiatives towards Preventing Cyber Terrorist Attacks'. *DePaul Business Law Journal*, 12(1): 33-43.
- Clarke R. 2001. 'Draft International Convention to enhance Protection from Cyber Crime and Terrorism'. *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford, CA, Stanford University, Hoover Institution Press: 249-265.
- Council of Europe 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms* as amended by Protocol No. 11, Rome, 4.XI.1950.
- Council of Europe 2000. *Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, 4.XI.2000.
- Council of Europe 2001. *Convention on Cybercrime*, Budapest, 23.XI.2001.
- Council of Europe 2003. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, 28.I.2003.
- De Vel G. 2002. 'The Council of Europe in the New Information Era'. Presented at the Agenda E-governance Agenda-setting Workshop, Strasbourg, 10-11 June 2002.
- Draetta U. 2004. 'The Internet and Terrorist Activities'. *Enforcing International Law Norms against Terrorism*, Oxford, Hart: 453-464.
- Duggal P. 2002. *Cyberlaw: The Indian Perspective*, Saakshar Law Publications, Delhi
- Esterle A. and R. Hanno 2005. 'Information security: a new challenge for the EU'. Institute for Security Studies, European Union, Paris: 78.
- Fei Yan C. 2004. 'Cyber crime and legislation overview', Information Security Supervision Bureau (ISSB), Ministry of Public Security of China, Hanoi.
- Gallaher, M. P., Rowe, B.R. and A. N. Link 2006. 'Economic Analysis of Cyber-Security and Private-Sector Investment Decisions'. Draft report to DHS, RTI International, Research Triangle Park, NC.
- Garnett R. 2004. 'Cyberterrorism: a New Challenge of International Law'. *Enforcing International Law Norms against Terrorism*, Oxford, Hart: 465-488.
- Giacomello G. 2004. 'Bangs for the Buck: a Cost-Benefit Analysis of Cyberterrorism'. *Studies in Conflict and Terrorism*, 27(5): 387-408.
- Gordon L., Loeb M. P., Lucyshyn W. and R. Richardson 2006. '2006 CSI, FBI Computer Crime and Security Survey', Computer Security Institute: 1-30.
- Gordon L. and M. Loeb 2006. 'Managing Cyber Security Resources: A Cost-Benefit Analysis'. New York: McGraw Hill.
- Gordon L. and R. Richardson. 2004. 'Infosec Economics: New Approaches to Improve Your Data Defenses.' *Network Computing* April:67-70.
- Gordon L., Loeb M. and W. Lucyshyn. 2003. 'Sharing Information on Computer Systems Security: An Economic Analysis'. *Journal of Accounting and Public Policy*. Vol. 22, pp. 461-485.
- Gulapa A. L. 2006. 'Cyberattacks, Cyberterrorism and Cyber-use of Force: countering the unconventional under international Law'. *Ateneo Law Journal*, 48 (4): 1051-1163.
- Iqbal M. 2004. 'Defining Cyberterrorism'. *The John Marshall Journal of Computer & Information Law*, 22(2): 397-408.
- Modigliani, F. and M.H. Miller. 1958. 'The Cost of Capital, Corporation, Finance, and the Theory of Investment'. *American Economic Review* 48(3):261-297.
- NISER 2004. 'Is cyber crimes reigning on a no man's land?', National ICT Security and Emergency Response Centre (NISER), 1: 4-5

- Pekari C. 2004. 'Das Internet als Medium des weltweiten Terrorismus'. *Internationales Wirtschaftsrecht im Schatten* des 11. September 2001 : Tagungsband des 4. Graduiertentreffen im internationalen Wirtschaftsrecht in Jena 2003, Stuttgart, Boorberg: 287-309.
- Podesta, J. D. and G. Ray 2005. 'Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World'. *Yale Law & Policy Review*, 23 (2): 509-527.
- Podgor E. S. 2004. 'Cybercrime-Cyberterrorism. *International Criminal Law: quo vadis?*', Proceedings of the International Conference Held in Siracusa, Italy, 28 November - 3 December 2002, on the Occasion of the 30th Anniversary of ISISC, Romonville Saint-Agne, Erès: 283-301.
- Pollifroni M. 2003. 'Processi e modelli di e-government ed e-governance applicati all'azienda pubblica', Giuffrè, Milan: 3-7.
- Pollifroni M. 2005. 'The 'S-EPI MODEL': a Theoretical Model that links the E-Government processes to the Instruments of the Public Sector Social Responsibility'. In Proceeding of the International Workshop e_Government'05 (e_GOV'05), Workshop organised by the Brunel University, 13 September 2005, West London (GB).
- Ross S. A. 1978. 'The Current Status of the Capital Asset Pricing Model'. *Journal of Finance* 33:885-901.
- Rowe B. R. and M. P. Gallaher 2006. 'Private Sector Cyber Security Investment Strategies: An Empirical Analysis'. Presented at The Fifth Workshop on the Economics of Information Security (WEIS 2006), University of Cambridge, England: 1-23.
- Russell G. S., Grabosky P. and G. Urbas 2004, 'Cyber Criminals on Trial', Cambridge University Press.
- Ryan R. J. 1982. 'Capital Market Theory. A Case Study of Methodological Conflict'. *Journal of Business Finance and Accounting*:443-458.
- Schechter S. 2004. 'Computer Security Strength & Risk: A Quantitative Approach'. PhD thesis, Harvard University.
- Sofaer A. D. and C. Mariano-Florentino 2001. 'The transnational dimension of cyber crime and terrorism', Stanford, CA, Stanford University, Hoover Institution Press, XIX: 292.
- Sofaer A. D. and G. Seymour 2001. 'Cyber Crime and Security: the Transnational Dimension. *The Transnational Dimension of Cyber Crime and Terrorism*', Stanford, CA, Stanford University, Hoover Institution Press: 1-34.
- Stiglitz J. 1988. 'Economics of the Public Sector'. New York: W.W. Norton and Company.
- Taylor R. W. 2006. 'Digital crime and digital terrorism'. Upper Saddle River, NJ : Pearson Prentice Hall, XVII: 397.
- Trachtman J. P. 2006. 'Global Cyberterrorism, Jurisdiction, and International Organization'. *The Law and Economics of Cybersecurity*, New York, NY, Cambridge University Press: 259-296.
- Varian H. June 2000. "Managing Online Security Risk." New York Times.
- Varian H. May 2002. 'System Reliability and Free Riding'. In: Proceedings of the First Workshop on Economics and Information Security. May 16-17, University of California, Berkeley.

Endnotes

¹ Source: www.crime-research.org/library/Cybercriminal.html

² Source: www.uncjin.org/Documents/EighthCongress.html

³ NISER evolved from what was originally the Malaysian Computer Emergency Response Team (MyCERT) in March 1997. Throughout these years MyCERT was able to give good assistance to many Malaysians in handling ICT security problems such as intrusion, spamming, and many more. NISER was formed by the National Information and Communication Technology Council (NITC) to address ICT security issues covering both proactive and reactive measures. Today, NISER exists as a national body to monitor the National e-Security aspects under the supervision of the Ministry of Science, Technology and Innovation (MOSTI).

⁴ Source: <http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp>

⁵ Pavan Duggal is one of the pioneers in the field of Cyberlaw and is Asia's leading authority on Cyberlaw. He is a practicing Advocate, Supreme Court of India and a Cyberlaw Consultant. He is the President of Cyberlaws.Net, The Cyberlaw Consultancy which is Internet's unique and first ever consultancy dedicated exclusively to the new field of Cyberlaw. He is the Founder President of Cyberlaw Asia, Asia's pioneering organization committed to the passing of dynamic Cyberlaws in the Asian continent. Cyberlaw Asia is engaged in the process of creating greater awareness about Cyberlaws in different countries of Asia. Pavan has been associated with UNESCO on Ethical, Legal, and Societal Challenges of Cyberspace in Asia and the Pacific. He is the consultant to United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) on the Asia Pacific Conference on Cybercrime and Information Security 2002. He is Member of Nominating Committee of The Internet Corporation for Assigned Names and Numbers (ICANN) . He is also member of the Membership Advisory Committee and Membership Implementation Task Force (MITF) of ICANN and is involved in the legal issues of At Large Membership of this global body. He is the Member of the Public Interest Registry's Org Advisory Council. Source: <http://cyberlaws.net/cyberindia/column.htm>

⁶ For more information see the following document "*New targets for hacking*", available on the Website: <http://www.ameinfo.com/79557.html>

⁷ Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

⁸ In October'05, Skype Technologies warned that flaws in its Internet telephony software could allow attackers to take control of a user's system.

⁹ Reporting Economic Crime Online (RECOL) is an initiative that involves an integrated partnership between International, Federal and Provincial Law Enforcement agencies, as well as, with regulators and private commercial organizations that have a legitimate investigative interest in receiving a copy of complaints of economic crime. For more information see: <https://www.recol.ca/intro.aspx>

¹⁰ Source: <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>

¹¹ Source: <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

¹² The CERT® Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute in Pittsburgh, Pennsylvania, U.S.A. The Software Engineering Institute is a Department of Defense-sponsored federally funded research and development center. The CERT/CC was established in 1988 to deal with security issues on the Internet. It now partners with and supports the Department of Homeland Security's National Cyber Security Division and its US-CERT to coordinate responses to security compromises; identify trends in intruder activity; identify solutions to security problems; and disseminate information to the broad community. The CERT/CC also conducts R&D to develop solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues. For more information see: <http://www.cert.org>

¹³ Source: <http://www.netcaucus.org/books/egov2001/pdf/egovtcos.pdf>

¹⁴ Source: <http://www.nysfirm.org/projpubs/whitpaper.html>

¹⁵ The Computer Crime and Security Survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey is now in its 11th year and is, we believe, the longest running continuous survey in the information security field. This year's survey results are based on the responses of 616 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. For more information see: <http://www.gocsi.com>

¹⁶ Computer Security Institute (CSI) is the world's leading membership organization specifically dedicated to serving and training the information, computer and network security professional. Since 1974, CSI has been providing education and aggressively advocating the critical importance of protecting information assets. For more information see: <http://www.gocsi.com>

¹⁷ Several U.S. States have developed comprehensive new approaches to analyzing and selecting IT initiatives (e.g. Arizona, California, Idaho, North Carolina, Pennsylvania).

¹⁸ All of these factors demand serious consideration in up-front analysis and cost estimation. For more information see: <http://www.ctg.albany.edu/static/usinginfo/Cost/cost.htm>