Department of Impresa e Management

Master Degree in Consulenza Aziendale

Thesis in Competition and High-Tech markets

CRITICAL ATTACKS: HOW ECONOMY COULD BE SAVED BY CYBER INSURANCE

TUTOR

Professor Andrea Renda

CO-TUTOR

Professor Francesco Rullani

CANDIDATE

Eleonora Bianchi

ID 651901

Academic year 2013/2014

INDEX

Chapter four

The impact of cybercrime on security

Chapter five

The economics of cyber insurance

SUMMARY

Nowadays, it is consolidated the large and massive use of the Internet and its applications, causing more and more structures to be laid upon the Internet and its interconnections; it goes from simple users, that surf the Net for searching general information and social interactions, to business users, that rely on the Internet for economic and working issues, to administrative users, in this group stand large and important users such as banks and financial institutions and governments.

The heavy and important dependence of society on information technology implies that valuable and key assets are potentially and easily exposed to global cyber threats, and furthermore that any users can be susceptible to cyber attacks, paralysing their operative terms and leaving them exposed to further damages (A practical guide to assessing your cyber security strategy, 2012). For thus, this outlines the need of employing cyber security measures, which consist of "*a combination of technology and security procedures*" (U.S. Department of Homeland Security, 2013). Applying cyber security is the first step of security combination, it consists of technologies, processes and practices designed to protect networks and data from attacks, damages and unauthorized access; but, since attackers are always one step further and can exploit any kind of vulnerabilities in the system, cyber security cannot prevent all potential attacks which networks are exposed to.

So, there is need to check out security confidence, through cyber assurance, that systems are confident enough to meet operational need (Alberts et al., 2009), also in stress situations like attacks, failures, accidents and unexpected events. In this case, it is helpful to prepare a disaster plan, according to strategic risk management, that can be activated in case of cyber attacks. At the same level, there is information assurance that comprehends operations of protection and defence of information systems by ensuring and controlling their availability, integrity, authentication, confidentiality, and non-repudiation, including the restoration of information systems by incorporating protection, detection, and reaction capabilities. It consists essentially of systematic

protection throughout acquisition, elaboration and storage of information and data. As last step of combination, companies arrive to cyber insurance in order to transfer risk to other parties. Cyber insurance has as purpose to mitigate losses caused by cyber accidents. Its main goal and benefit is to sensitively reduce number of cyber attacks thanks to preventive measures that discourage them. The fundamental mechanism of insurance applied to IT is the encouragement of implementation of best practices, by basing premiums on the level of self-protection adopted by insured party (U.S. Homeland Security, 2012); in this way insurance can limit the level of losses faced during and after a cyber attack.

The principal hypothesis this thesis is aiming to answer to is that cyber insurance can effectively be a vital tool and strategy for firms, in particular for critical infrastructures owners and operators, in order to mitigate all those risks that cannot be covered and absorbed by cyber security strategies implemented by companies. Indeed, the major objective of the dissertation is to highlight the significant role of critical infrastructures and to encourage cyber security with more than one approach and strategy.

Therefore, the principal assumption on which this dissertation is relying is the importance and criticality of critical infrastructures, that, consequently, need further and more focused protection against both physical failures and damages and, especially, cyber-related attacks. Nowadays, all the world rely on a well-functioning Internet, for any kind of services, from transportation to energy, from health care to energy, from food to government. The "*interconnectedness within and across systems also means that infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures*" (National Research Council, 2002). The stronger the interconnection between users, infrastructures and security, the less resilient is the system made by critical infrastructures. When an infrastructure provides vital and fundamental services to nation's well-being, which comprehends state-of-art functioning systems, security and public order within national borders, is called critical infrastructure.

European Council formulated the Directive 2008/114/EC of 8th December, 2008, which establishes common procedure for identification and designation of European Critical Infrastructure (ECI). ECI is defined as "*critical infrastructure located in the EU Member States, the disruption or destruction of which would have a significant impact on at least two Member States of the EU*"(Holt, 2013). The list of Critical Infrastructures is growing at an increased pace. The most important macro areas are Finance and Banking, Manufacturing, Food and Agriculture, Health, Energy, Water, Transportation and Postal services, Security and Emergency services, Government and Information and Communications Technology.

Critical infrastructures, indeed, represent the backbone of modern society, as they become more and more important for civilized economies and also developing countries' economies. Thanks to a deep analysis of their definition, since it affects further considerations, critical infrastructures are demodulated in order to identify those infrastructures whose incapacity or destruction would have a debilitating impact on the defence or economic security of the nation (in Moteff, Parfomak, 2004). Another sign of criticality is the strong dependency on other infrastructures and thus strong interdependency (Hammerli, Renda, 2010), consequently, the interdependency and importance of these infrastructure are the focus for economy, government and social life, therefore these infrastructures are considered critical, since their malfunctioning and failures can bring a general disturbance or, worse, to a loss of investments, efficiency and life comfort.

Singularly, nations have listed different critical infrastructures depending on national interests and weaknesses, even if there are common industries that are controlled by the majority of nations, such as electric power supply, water supply, banking and finance, defence, food, public health, telecommunications and transportation.

Their existence is woven into society's habits, therefore they are under the spotlight of governments and policy attention. It is essential that critical infrastructures are robust, reliable and resilient, able to face possible risks, coming from nature or human error or attack. Several new technology-based infrastructures have been created over the last century and half (Goodman *et*

al., 2003), their development and intensive usage characterize modern society and determine its vulnerabilities.
Moreover, critical infrastructures are such a complex issues because they are vital and ubiquitous, therefore their lack of capacity or even their destruction affects not only security and social issues of one nation, but it has devastating cascade effects across national borders, causing shock transmissions across borders and across numerous infrastructures, which determine the impossibility to consider and analyze a single-standing infrastructure isolated from environment or other infrastructures.

Since physical parts of these networks have to undergo to alarming range of threats coming from nature, such as earthquakes, extreme winds, floods, tsunamis, and wildfires, they are also threatened by terrorist acts, design faults, aging materials and inadequate maintenance. Maintenance itself is a key aspect against failure, but it is also the aspect less assessed by investors, declining constantly the resilience of systems and thus increasing the probability of severe failures.
Failure of major infrastructure could provoke catastrophic effects, indeed the failure of these significant systems can cause environmental damages, important cost to economy and possible threats to life. The solution to be undertaken in order to decrease the likelihood of failures is to adequately maintain and protect critical infrastructures and to build reserve capacity, useful during emergency actions; it is essential for this purpose to better include private sectors, since they can easily and better assess systems status and address proper protection, because of firsthand information and data (Brömmelhörster *et al*., 2004).

Therefore, serious protection issues have to not be just limited to engineering design systems, but need to embrace topic of legacy systems, the difficulty to understand strategic threats, the need for training and information sharing. In order to face properly critical infrastructure protection (CIP), it must be acknowledged numerous challenges that, if addressed, will improve security. First of all, it has been noticed a limited pool of resources available in order to address security problems, that could increase risks and inhibit businesses.

Then, the lack of sharing news about threats and incident among government and private actors can increase the risk of attacks because there is a sense of unpreparedness among actors. Moreover, it results chaos and inefficiencies created by poor coordination among public agencies. Furthermore, the increasing sophistication of tools and methods used by hackers worsens the fastness of response and its efficacy, requiring high level of cyber security, in order to be prepare for cyber attacks.

This is also the result of difficultness of establishing effective partnerships between government and businesses. In order to improve the protection aver critical infrastructures, a clear and effective cooperation among government and private companies must be set to maximize the security over critical infrastructure and minimize costs and disadvantages that can arise during a non-efficient collaboration, which can create obstacles to the final objective, which is protecting critical infrastructures.

First of all, incentives must be put clear and motivating for private companies in order to undertake all the necessary actions for reducing infrastructure vulnerabilities; often it is more convenient from a business point of view to accept the risk of an hypothetical or possible terrorist attacks or damages than coping with sure costs, that tend to outweigh the future benefits. Even if government can set goals, it lays on private companies to efficiently implement steps, because they have deep knowledge of the overall system. However National Strategy for Homeland Security (2002) represents an obsolete approach to the problem, where government addresses protection activities only to markets that do not provide adequately on their own. The strategy assures that there are enough and enough strong incentives in private market to supply sufficiently protection, ensuring to rely on private sector. Even if numbers agree with this statement, as 85% of critical infrastructures is privately owned, it is consolidated that a backup support of government is essential, since "*market forces alone are, as a rule, insufficient to induce needed investments in protection*" (National Strategy for Homeland Security, 2002).

Despite a lack of incentives for private companies, large corporations have political and financial forces and credibility to assume the role of protecting infrastructures, moreover they have, or at least they can afford, technical

expertise and experience. However, they face uncertainties because of asymmetrical information, as other critical infrastructure tends to retain information about their own infrastructures, and therefore, they can underestimate the emergency behind protecting critical infrastructures.
In order to foster cooperation, owners of critical infrastructure should know the reaction of jurisdiction to attacks and its actions to prevent them and the level of coordination among local jurisdiction and government.

In order to give proper considerations, the dissertation goes on analyzing Critical Information Infrastructures (CII), critical information infrastructures are more sensitive to external attacks and technological vulnerabilities, which can be easily exploited by malicious attackers. Internet is by design open and exposed to threats, but at the same time it leaves room to improvements and to reduce vulnerable points of access, in order to improve and boost resilience and robustness of Internet and consequently of all other critical infrastructures which rely upon.
In the dissertation, it is given a full description of three of the most important and concerning aspects of the dark side of the Internet, cyber attacks, cyber warfare and cyber terrorism, as these aspects represent the evolution of cybercrime, which comes alongside with technology advancements, and reflect the different intentions of attackers. Moreover, a clear and net distinction between these terms is useful when a strategy for security and protection need to be designed, and it needs to take into account the different consequences and targets. Cyber threats require awareness and improved security practices, which need to be shared by any users and to be aware. Therefore, it should be addressed the creation and implementation of robust culture of cyber security (Cornish *et al*., 2011) in order to create an homogenous basis of security which is shared by the majority of users.

The conclusion of the discussion about cyber security ends in stating that, in order to prevent or mitigate damages of cyber attacks, security frameworks help managers and strategists to construct and apply a suitable and tailored cyber security which is consistent with factors, such as economical, political and cultural. Implementing basic principles at IT system infrastructure, as

dictated by Dr. Amoroso (2011), may ensure an efficient cyber security for the most technological structures, such as critical infrastructures which need a special and more focused security and defense in order to avoid severe damages for society.

Consequently, the organization which runs critical infrastructure by employing an efficient CIP and CIIP, it has assured the information supply chain and secured its cyber infrastructures against cyber crime, ensuring stakeholders and insurance operators that the organization has low likelihood of suffering severe damages provoked by cyber criminals. By implementing these protections and security strategies, an organization is reassuring and stating its risk appetite in order to successful underwrite a cyber insurance which helps to mitigate unexpected or residual risks and damages, which are unprotected through all the undertaken security actions.

Since there is a growing dependency on technology and an increased threat of unauthorized access to data and information, there is also a response of insurance market to these challenges, backed by an increased awareness and knowledge of corporations about cyber risks and exposure (Airmic technical, 2012), consequently, the potentiality of insurance results significant for organizations as a control mechanism.

Cyber insurance has been described as "an *effective, market-driven way of increasing cyber security*" (U.S. Department of Commerce, 2011). In fact, it is nearly impossible to reach a perfect coverage by attack and damages. The impossibility comes due to several causes (Pal, Hui, 2012), first of all because there is not yet sound and proven technical solutions; then because of the diverse intentions that lay behind attacks; but also misaligned incentives between network users, security providers and regulatory authorities leave room for attacks; there are strong externalities and free-riding problem; moreover it is difficult to measure quantitatively and qualitatively risks; system failure is amplified by customer lock-in and first mover effects of vulnerable security products and by problem of lemons market, which is the electronic medium of computers networks, "*via which online communications takes place*"(Pal, Hui, 2012).

In this failing system, cyber insurance is catching on, according to Pal and Hui, thanks to three reasons. It increases the overall network safety by adopting self-defence strategy, in order to respond to an increase to insurance premium. Cyber insurance integrates the partial protection offered by cyber security strategies; in fact, these means cannot reach absolute protection unless it upgrades technologies and it should face enormous expenditures to adequate security systems. Therefore, it is optimal choice to transfer risks, faced because of lack of total security, to a third party that can leverage them. Cyber insurance, moreover, can be a solution to misaligned incentives, by combining benefits that actors seek on the Internet. Insurers earn profit from premiums, network users will be able to hedge potential losses, while security software producers can benefit from first mover advantage and lock-in strategies.

The thesis, at this point, reaches its objective to expose the benefits of implementing cyber insurance for firms, and especially, for critical infrastructures and CII.

Even if insurance market may still present possible failures, insurance for critical infrastructure is a possible way to protect nations' capabilities to ensure society future and present wellbeing. Therefore, the insurance may act as a facilitator tool in order to collect information and risk assessment (Cukier, 2005), which will enable insurers with greater information power as they may improve insurance conditions, terms and premiums. Insurance, as a result, acts as a collector of information and best practices which are shared across the industry, improving the efficiency and the protection of data, software and business.

Furthermore, insurance market in order to be the most fair and efficient, needs to have a reasonable and enough good knowledge about the expected losses and their likelihood of occurring by tracing and knowing the probability distribution of the insured events (Rowlands, Devlin, 2006). However, because of non-independency of events, since, in the case of CI, the interrelation among events, components and infrastructures are present and strong, the analytics of past events in order to foreseen future ones is challenged and complex (Rowlands, Devlin, 2006).

Another benefit of cyber insurance implementation is that cyber insurance has the power to improve information about security, since it requires a wide collection of data about cyber threats and cyber attacks; at the same way, cyber insurance can affect positively security decisions and the overall network environment, spreading the adoption of these mitigation strategies.

Incentives are requested and needed in order to boost and improve the accessibility to insurance in order to mitigate risks and costs. In order to improve economic efficiency, it is required to encourage firms in engaging the optimal level of risk mitigation (Rowlands, Devlin, 2006); it is possible by requiring, as terms of insurance contracts, more investment. It is still important the government contribution to insurance market and critical infrastructures, where government should focus on major cyber/physical events and on helping stakeholders by assuming the role of *super partes* (US Homeland Security, 2012). Even if governmental agencies succeeded in identifying cyber threats and theirs sources, it is up to organizations to insure their operations by deciding which cyber threats address, as it is useless and inefficient to "*insure against everyone and everything*" (US Homeland Security, 2012), by implementing protection strategies which address basic cyber threats, and by relying on agencies cooperation if a complex cyber attack should occur.
Cyber insurance has still to address challenges in order to improve and boost its adoption towards firms and industries. In fact, an increased adoption of cyber insurance is proved to improve the Internet conditions for the majority of users, even those that do not purchase cyber insurance (Lelarge, Bolot, 2009), to improve cyber security and to reassure stakeholders.

In conclusion, it is possible to state that, as this thesis tried to prove and explain, cyber insurance market is essential and a vital presence for companies that want to transfer cyber risks to third parties, and it will have a larger role for industries as soon as governments will clarify and reason cyber security investments.
In special way for critical infrastructures, cyber insurance represents an effective and efficient tool in order to encourage owners and operators to implement improved cyber security strategies and it reassures stakeholders of

the reliability and resilience of these backbone structures, which are assumed to continue providing their services for the sake of society well being.

This thesis is structured in five main chapters, which face principal topics and issues related to critical infrastructures and cyber insurance.

Chapter one rotates around the figure of Critical Infrastructures and their interdependencies with the external environment, formed by society, economics and politics. Through a deep and transversal theoretical investigation, it is possible to notice how critical infrastructures are fundamental and essential for the entire world.

Chapter two investigates in critical infrastructure particularities which are Critical Information Infrastructures. These are the base of many other critical sectors, linked with strong interdependencies and nebulous boundaries as Internet and telecommunications technologies (ICT) improve and enter daily life with numerous and different applications.

Chapter three deals with the importance and value of information and data, which constitute the essential raw material for any business. As WikiLeaks has proven, the security and protection of sensitive information and data becomes a priority for organizations, which try to construct valiant models that could help business to deal efficiently with everyday operations and processes. Therefore, models and management strategies would be useful and indispensable for business in order to handle carefully these key assets.

Chapter four shows the risks that organizations, and general users, meet by using and running IT infrastructures, which represent the pivotal structure for modern organizations. In fact, cyberspace and computer machines are now the key platform in which the complex relation between human factors and economic advantage takes place, as the Internet and its infrastructure connect people, provide governmental services and help running businesses and services. However, the complexities are evident for any users, since risks, threats and vulnerabilities are the first threats to organizational security, and it also represents one of the top threats to national security, second only to terrorism.

Chapter five introduces the importance of cyber insurance, which transfers cyber risks to an insurance company that can effectively and profitably mitigate risks in return of premiums. In fact, as the importance of the Internet grows, firms are more vulnerable to threats and risks coming from cyber criminals, who attempt to gain unauthorized credentials and access to sensitive information, causing significant financial and business losses to firms. However, cyber insurance proves that, if effectively implemented alongside with cyber security strategies and risk management procedures, it is a valid ally for mitigating those risks that remain uncovered by normal security strategies. Moreover, cyber insurance may affect positively other industries and users, thanks to improved cyber security spread over the Internet and IT infrastructures.

REFERENCES

About Critical Infrastructure, Public Safety Canada, [www.ps-sp.gc.ca]

Airmic technical, Airmic Review of Recent Developments in the Cyber Insurance Market & commentary on the increased availability of cyber insurance products, 2012

Alberts C., Ellison R.J., Woody C., Cyber Assurance, CERT, 2009

American Petroleum Institute and the National Petrochemical & Refiners Association, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, May 2003

Amoroso E.G., Cyber Attacks: Protecting National Infrastructure, Elsevier, 2011

An Emergency Management Framework for Canada, Ministers responsible for Emergency Management, 2011, [http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf]

Anderson B., Anderson B., Seven Deadliest USB Attacks, Syngress, 2010

Anderson R., Fuloria S., Security economics and critical national infrastructure, The Eight Workshop on the Economics of Information Security, 2009

Anderson R.D., Insurance Coverage for Cyber Attacks, issue of The Insurance Coverage Law Bulletin , Vol. 12, No. 4, June 2013

Angelini M., *et al*., 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness, Research Centre of Cyber Intelligence and Information Security "Sapienza" Università di Roma, December 2013, Casa Editrice Univarsità La Sapienza, [http://www.dis.uniroma1.it/~cis/media/CIS%20Resources/2013CIS-Report.pdf]

Antinori A., Information Communication Technology & Crime: the Future of Criminology, Rivista di Criminologia, Vittimologia e Sicurezza Vol. II - N. 3 , Settembre-Dicembre 2008

Antinori A., Sviluppo nell'ambito nazionale del concetto di information assurance relativo alla protezione delle informazioni nella loro globalità, CEMISS, 2011

Armerding T., The 15 Worst Data Security Breaches of the 21st Century, 2012, [http://www.pcworld.com/article/250197/the_15_worst_data_security_breaches_of_the_21st_century.html]

Art. 8 EU Charter Fundamental Rights

Assaf D., Models of critical information infrastructure protection, International Journal of Critical Infrastructure Protection, Volume 1, Pages 6–14, December 2008, [http://ac.els-cdn.com/S1874548208000097/1-s2.0-S1874548208000097-main.pdf?_tid=1cd9c180-adcb-11e3-9c53-00000aab0f6c&acdnat=1395057542_58d0a30b9713f06f7a6a01180029def6]

Aviation Week and Space Technology, October 22, 2012, [http://www.aviationweek.com]

Aviram A. , Tor A. , Overcoming impediments to information sharing, Alabama Law Review 55 (2), pag. 231-279, 2004

Baker L., 2010 USA - Telecoms, Wireless, Broadband and Forecasts, 2010

Baker S. *et al*., In The Crossfire: Critical Infrastructure In The Age Of Cyber War 3, Mcafee, Inc., 2009, [http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf]

Baltzan P., Phillips A., Detlor B., Business-driven information systems, 1st Canadian Ed. Whitby, Ontario, Canada: McGraw-Hill Ryerson, 2008

Barlow J. P., The netizen: the powers that were, Wired, 4(9) , 53–56, 195, 197, 199, 1996

BBC, Passwords revealed by sweet deal, 2004, [http://news.bbc.co.uk/1/hi/technology/3639679.stm]

Belissent J., Getting clever about smart cities : New opportunities require new business models, Forrester research, 2010,[http://www.forrester.com/Getting+Clever+About+Smart+Cities+New+Opportunities+Require+New+Business+Models/fulltext/-/E-RES56701]

Bernard R., Understanding Cyber Insurance , Security Technology & Design, ISSN 1069-1804, Volume 18, no. 7, p. 16, 2008

Bohme R., Kataria G., Models and Measures for Correlation in Cyber-Insurance, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK, June 2006

Bohme R., Schwartz G., Modelling Cyber-Insurance: Towards A Unifying Framework, Workshop on the Economics of Information Security (WEIS), Harvard, June 2010

Bolot J., Lelarge M., Cyber Insurance as an Incentive for Internet Security, Seventh Workshop on the Economics of Information Security, 25-28 June, 2008

Boritz J. E., IS Practitioners' Views on Core Concepts of Information Integrity, International Journal of Accounting Information Systems, Elsevier, 2011

Bowerman B., Braverman J., Taylor J., Todosow H., Von Wimmersperg U., The vision of a smart city, 2nd International Life Extension Technology Workshop, 2000

Branin J. (Ed.), Collection Management in the 1990s. Chicago, IL: American Library Association, 1990

Brenner S. W., Cybercrime, cyber terrorism and cyber warfare, Revue internationale de droit pénal, Vol. 77, no. 3, p. 453-471, 2006, [www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm]

Brenner S.W., Clarke L.L.., Civilians in Cyber warfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol. 43, 1011, 2010

Brenner S.W., Cyber threats: The Emerging Fault Lines of the Nation State, pp. 71–161, 2009

Brinkman J., Supporting sustainability through smart infrastructures: the case of Amsterdam, Network Industries Quarterly , vol. 13, no 3, 2011, [http://newsletter.epfl.ch/mir/index.php?module=epflfiles&func=getFile&fid=244&inline=1]

Brinkman J., Supporting sustainability through smart infrastructures: the case of Amsterdam, NGInfra Conference, Virginia Beach, November 2011, [http://sinfras.com/conferences/nginfra2011/files/2011/12/NGInfra_2011_Amsterdam.pdf]

Brömmelhörster J., Fabry S., Wirtz N., Critical Infrastructure Protection: Survey of World-Wide Activities, 2004,[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile]

Buckler G., Can you afford to lose your data? How to insure your company's electronic files is a growing issue, and more needs to be done to address it, The globe and Amil, 2005

Cabinet Office, Sector Resilience Plans for Critical National Infrastructure 2010, March 2010

Caldwell T., Ethical hackers: putting on the white hat, Network Security, Volume 2011, Issue 7, Pages 10–13, July 2011, [http://ac.els-cdn.com/S1353485811700757/1-s2.0-S1353485811700757-main.pdf?_tid=754aba56-d4f7-11e3-8521-00000aab0f6c&acdnat=1399364684_269af6e21b6eef1ff5476f83cfcda69c]

CAMM steering committee, CAMM response to cloud computing: a consultative document, 22nd may, 2011

Capgemini, Using insurance to mitigate cybercrime risk, Challenges and recommendations for insurers, 2012

Càrdenas A.A., Radosavac S., Grossklags J., Chuang J., Hoofnagle C., An Economic Map of Cybercrime, The 37th Research Conference on Communication, Information and Internet Policy (TPRC), George Mason University Law School, Arlington, 25th September, 2010

Cateddu D., Security - Resilience in Governmental Clouds, ENISA, 2011, [https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds]

Caudle D.L., Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers, University of Phoenix, School of Advanced Studies, 2010

Center for Strategic and International Studies, The Economic Impact Of Cybercrime And Cyber Espionage, July 2013, [http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf]

Centre for Security Studies (CSS), Focal Report 1 Critical Infrastructure Protection, Crisis and Risk Network (CRN), 2008, [http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.71944.DownloadFile.tmp/focalreport1.pdf]

CESG, Guide to IA Self-Assessment Using the HMG IA Maturity Model and Assessment Framework, 2013

CESG,HMG IA Standard No.1 - Technical Risk Assessment , Issue 3.51, October 2009, [http://www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf]

CESG,HMG information assurance maturity model and assessment framework, CESG, 27th may,2010

Chaffey N., People power: making your people an essential part of your cyber security strategy, [http://www.paconsulting.com/our-thinking/why-a-human-side-is-essential-to-effective-cyber-security/]

Choo C. W., [http://choo.fis.utoronto.ca/Imfaq/], 2008

Clemente D., Cyber Security and Global Interdependence: What Is Critical?, Chatham House, Feb 2013, [http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf]

CNSSP No. 22, Policy on Information Assurance Risk Management for National Security Systems, Committee on National Security Systems, January 2012, [http://www.ncix.gov/publications/policy/docs/CNSSP_22.pdf]

Colwill C .J., Todd M. C., Fielder G. P., Natanson C., Information assurance, Technology Journal, Volume 19, no 3, pp. 107 - 114 ,07/2001, [http://download.springer.com/static/pdf/166/art%253A10.1023%252FA%253A1011998517801.pdf?auth66=1395582573_bc478b20a703fcd7e6c9cc92862a6acc&ext=.pdf]

Commission of European Parliament, COM(2007) 267- Towards a general policy on the fight against cyber crime, 2007, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF]

Commission of European Parliament, COM(2007) 267- Towards a general policy on the fight against cyber crime, 2007

Commission of the European Communities, Green paper on a European Programmes for Critical Infrastructure Protection COM(2005)576, 2005

Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, European Commission Working paper, 2013

Common Assurance Maturity Model Steering Committee, Common Assurance Maturity Model Guiding Principles, 2010,[http://common-assurance.com/resources/Common-Assurance-Maturity-Model-vision.pdf]

Communication from the Commission on a European Programme for Critical Infrastructure Protection, 12th December 2006

Conference on Information Law and Policy for the Information Economy, organized by Professors Branscomb L.M., Mayer-Schönberger V. of Harvard University's John F. Kennedy School of Government, 16th-18th June, 2005

Conrad S.H., LeClaire R.J., O'Reilly G.P., Uzunalioglu H., Critical National Infrastructure Reliability Modelling and Analysis, Bell Labs Technical Journal 11(3), 57–71, 2006, [http://www.lucent.com/enrich/v1i22007/pdf/BLTJ_20178.pdf]

Constantin L.., Most IT and security professionals see Anonymous as serious threat to their companies, Infoworld, April 23rd, 2012, [http://www.infoworld.com/d/security/most-it-and-security-professionals-see-anonymous-serious-threat-their-companies-191502]

Council Directive 2008/114/EC of 8 December 2008

Counter-terrorism strategy [www.security.homeoffice.gov.uk]

Critical infrastructure- Resilience strategy, Australian government, 2010

Cukier K., Ensuring (and Insuring?) Critical Information Infrastructure Protection, Rueschlikon Conference on Information Policy, 2005, [http://www.vmsweb.net/attachments/pdf/R-05_Report_Online.pdf]

Cybercrime Report: The Human Impact, Symantec, 2010

Damage Toll for Nimda, less than was expected, 2001, [http://www.xatrix.org/news/damage-toll-for-nimda-less-than-was-expected--773/]

Dardick G.S., Cyber Forensics Assurance, Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, November 30th 2010, [http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1076&context=adf]

Daskala B., Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology, 2010, [http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology]

Dekker M., Liveri D., Lakka M., Incident reporting for cloud computing, ENISA, 2013, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing]

Department of the Air Force, Identification and Authentication, AFMAN 33–223, HQ USAF, Washington, 1998

Deputy Assistant Secretary of Defence, Cyber, Identity, and Information Assurance Strategy, The Office of the Assistant Secretary of Defence for Networks and Information Integration / DoD Chief Information Officer, 2009, [http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf]

Desouza K. C., Hensgen T., Semiotic Emergent Framework to Address the Reality of Cyber terrorism, Technological Forecasting and Social Change, Vol. 70, no. 4, pag. 385–396, 2003

Detlor B., Information Management, International Journal of Information Management, ISSN 0268-4012, Volume 30, no. 2, pp. 103 - 108, 2010, [http://www.sciencedirect.com/science/article/pii/S0268401209001510]

Difference between a computer virus and a computer worm, USCB ScienceLine.

Digital Agenda for Europe site, [http://ec.europa.eu/digital-agenda/en/internet-things]

Dipert R.R., The Ethics of Cyber warfare, Journal of Military Ethics , Volume 9, Issue 4, Special Issue- Ethics and Emerging Military Technologies, 2010, [http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404]

Dodge M., Understanding Cyberspace Cartographies: A Critical Analysis of Internet Infrastructure Mapping, PhD Thesis, 2008

Dunn Cavelty M., Critical information infrastructure: vulnerabilities, threats and responses, ICTs and International Security, 2007

Dunn Cavelty M., Systemic cyber/in/security – from risk to uncertainty management in the digital realm, Swiss Re Centre for Global Dialogue, 15 September 2011, [http://cgd.swissre.com/features/Systemic_Cyber_In_Security.html]

Dunn M. , Mauer V. , International CIIP Handbook, vol. 2, Centre for Security Studies, Swiss Federal Institute of Technology, Zurich, Switzerland, 2006, [http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-04.pdf]

Dyer G., Intelligence Chief in US Cyber-attack Warning, Financial Times, March 13, 2013

Eckert S., Protecting Critical Infrastructure: The Role of the Private Sector, in Guns and Butter: The Political Economy of International Security", Dombrowski, P. (Eds.), 2005, [http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf]

Egan M., Geopolitical Tensions Invade Cyberspace, FOX Business, March, 11th, 2014, [http://www.foxbusiness.com/technology/2014/03/11/geopolitical-tensions-invade-cyber-space/]

ENISA, Appropriate security measures for smart grids, 2012, a

ENISA, Cloud Computing Security Risk Assessment, 2009, b, [https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment]

ENISA, Critical Cloud Computing-A CIIP perspective on cloud computing services, 2013, a, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing]

ENISA, ENISA Smart Grid Security Recommendations, 2012, d

EU Charter Fundamental Rights

EU Commission, Achievements and next steps: towards global cyber-security, 2011, a, [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0163&from=EN]

EU Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing
preparedness, security and resilience,2009, [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&from=EN]

European Commission , Energy infrastructures: increasing security of supply in the Union, Memo, DG for Energy and Transport, 2003

European Commission, Proposal amending Council Directive 2008/114/EC Identification and designation of European critical infrastructures, Version 1, August 2011b,

[http://ec.europa.eu/governance/impact/planned_ia/docs/2012_home_010_directive_critical_infrastructures_en.pdf]

European Communication 149/2009

European Communication 786/2006

Everett C., The lucrative world of cyber-espionage, Computer Fraud & Security, Volume 2009, Issue 7, Pages 5–7, July 2009, [http://ac.els-cdn.com/S1361372309700843/1-s2.0-S1361372309700843-main.pdf?_tid=2b5efe30-d4f6-11e3-972d-00000aacb362&acdnat=1399364130_1869f41c1e2791b5201503549a01ea5c]

Executive Order 13228. Section 3 (e) (i), (ii), (iv), (v) and (vi), pp. 51813-51814

Executive Order 13010. p 37347, 15th July 1996

Executive order 13636 : Improving critical infrastructure security, department of homeland security, 12th june,2013,

Finklea K. M., Theohary C.A., Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, Congressional Research Service, 9th January, 2013, [http://www.fas.org/sgp/crs/misc/R42547.pdf]

Frigo M.L., Anderson R.J., What Is Strategic Risk Management?, Strategic Finance, April 2011, [http://www.markfrigo.com/What_is_Strategic_Risk_Management_-_Strategic_Finance_-_April_2011.pdf]

Furnell S.M., Warren M.G., Computer hacking and cyber terrorism: the real threats in the new millennium?, Computers & Security, Volume 18, Issue 1, Pages 28–34, 1999, [http://ac.els-cdn.com/S0167404899800066/1-s2.0-S0167404899800066-main.pdf?_tid=df0726e6-d4f7-11e3-a01c-00000aacb35f&acdnat=1399364861_7cd8df0fa2916ed473a3f6461220f4e0]

Geers K., Kindlund D., Moran N., Rachwald R., World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, FireEye Labs, 2013, [http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf]

Geers K., The Cyber Threat to National Critical Infrastructures: Beyond Theory, Information Security Journal: A Global Perspective, Vol. 18, Issue 1, p1-7. 7p, 2009, [http://se5fj2qs2v.scholar.serialssolutions.com/?sid=google&auinit=K&aulast=Geers&atitle=The+cyber+threat+to+national+critical+infrastructures:+Beyond+theory&id=doi:10.1080/19393550802676097&title=Information+security+journal.&volume=18&issue=1&date=2009&spage=1&issn=1939-3555]

Gengler B., Politicians Speak Out on Cyber terrorism, Network Security, 10,pag. 6, 1999

German Federal Ministry of the interior , Protecting Critical Infrastructures – Risk and Crisis Management

Gheorghe A.V., Masera M., de Vries L., Weijnen M., Kroger W., Critical infrastructures: the need for international risk governance, International Journal of Critical Infrastructures, Vol.3, No.1/2, pp.3 - 19, 2007, [http://www.nextgenerationinfrastructures.eu/download.php?field=document&itemID=449529]

Givens A. D. , Busch N. E. ,Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, International Journal of Critical Infrastructure Protection, Volume 6, Issue 1, Pages 39–50, March 2013, [http://ac.els-cdn.com/S187454821300005X/1-s2.0-S187454821300005X-main.pdf?_tid=3e1cafe8-adca-11e3-a503-00000aab0f26&acdnat=1395057168_301d295d8707db05293ee5c6011119b0]

Gonzàlez Fuster G., Gutwirth S., The core content of personal data protection: a conceptual controversy, PRESCIENT International Conference, 28th Nov.2012, [http://www.prescient-project.eu/prescient/inhalte/download/4-Gonzales-Fuster.pdf]

Gorniak S., *et al*., Priorities for Research on Current and Emerging Network Technologies, ENISA, 2010, [https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/procent]

Government Accountability Office, Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats- GAO-07-705, 2007, [http://www.gao.gov/new.items/d07705.pdf]

Graham A., Canada's critical infrastructure -When is Safe Enough Safe Enough?, National security strategy for Canada series, The Macdonald-Laurier Institute, 2011, [http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf]

Grauman B., Cyber-security: The vexed question of global rules - An independent report on cyber-preparedness around the world, Security & Defence Agenda, 2012, [http://www.mcafee.com/au/resources/reports/rp-sda-cyber-security.pdf]

Green Paper - A European Strategy for Sustainable, Competitive and Secure Energy, COM/2006/0105 final

Hahn R. W., Layne-Farrar A., The Law and Economics of Software Security, Harvard Journal of Law and Public Policy, 30(1): 283-353, 2006

Hallinan D., Friedewald M., McCarthy P., Citizens' Perceptions of Data Protection and Privacy in Europe, Computer law and security review, Vol. 28, No 3, pp. 263-272, 2012

Hamill J.T., Deckro R.F., Kloeber J.M., Evaluating information assurance strategies , Decision Support Systems, Volume 39, Issue 3, Pages 463–484, May 2005, [http://ac.els-cdn.com/S0167923604000284/1-s2.0-S0167923604000284-main.pdf?_tid=e0ac61dc-b107-11e3-92ad-00000aacb361&acdnat=1395413494_cb1b040578a40c17b4e294d3cfd89e51]

Hammerli B., Renda A., Protecting critical infrastructure in the EU, CEPS task force report, 2010

Hardin G., The tragedy of the commons, Science 13 (162), pag. 1243–1248, 1968

Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan H., Perdue W., Spiegel J., The Law Of Cyber-Attack, California Law Review, Vol. 100, No. 4, August 2012, [http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf]

Healey J., Grindal K., A Fierce Domain: Conflict in Cyberspace, 1986-2012 , Cyber Conflict Studies Association, 2013

Herath H.S.B., Herath T.C., Copula-based actuarial model for pricing cyber-insurance policies, 2011

Herath H.S.B., Herath T.C., Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management, 2006

Hesseldahl A., 'Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting', All Things D, 14 July 2011, [https://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-internet-is-and-how-big-its-getting/]

Hildreth S.A., Cyber warfare, Congressional Research Service, June 19, 2001, [http://www.fas.org/irp/crs/RL30735.pdf]

Hinde S., Cyber Wars and other threats, Computers & Security, Volume 17, Issue 2, Pages 115–118, 1998

Hinde S., Cyber-terrorism in context, Computers & Security, Volume 22, Issue 3, Pages 188–192, April 2003, [http://ac.els-cdn.com/S0167404803003031/1-s2.0-S0167404803003031-main.pdf?_tid=ad8b2362-d4f5-11e3-93c7-00000aab0f27&acdnat=1399363919_66a5531b754095c9ffe538c94015d570]

Hinde S., Incalculable potential for damage by cyber-terrorism, Computers & Security, Volume 20, Issue 7, Pages 568–572, 31 October 2001, [http://ac.els-cdn.com/S0167404801007040/1-s2.0-S0167404801007040-main.pdf?_tid=9793463c-d4f7-11e3-b3c3-00000aacb360&acdnat=1399364741_97074ecb4c451fee70b11b5f64f5c0eb]

Holt M.W., Critical Infrastructure Protection in the European Union, The CIP report, May 2013

Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, 2013, [http://mutualink.net/PDF/NIPP-2013-Partnering-for-Critical-Infrastructure-Security-and-Resilience-Dec-2013.pdf]

Hromada M., Lukas L., Critical Infrastructure Protection and the Evaluation Process, International Journal of Disaster Recovery and Business Continuity, Vol.3, 2012,[http://www.sersc.org/journals/IJDRBC/vol3/5.pdf]

Hua J., Bapna S., The Economic Impact of Cyber Terrorism, The Journal of Strategic Information System, Vol. 22, no.2, pag. 175-186, June 1, 2013

Huffaker B., Fomenkov M., Claffy kc, Internet Topology Data Comparison, Cooperative Association for Internet Data Analysis (CAIDA), May 2012, [http://www.caida.org/publications/papers/2012/topocompare-tr/topocompare-tr.pdf]

Huntley T.C., Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change, Nature of Warfare, 2010

I Love You, WHoWhatWhereWhenWhy.com

IAAC Dependencies and Risk Working Group, Policy paper, July 2000

IACC, IAAC's Identity Assurance Programme 2006-2008: Concluding Report, September 2008, [http://www.iaac.org.uk/_media/IdAConcludingReportSept08.pdf]

ICE, The state of the nation : Defending critical infrastructure, 2009

Industry security notice, 2010

Information & Records Management Officer, Information Management Strategy, Cumbria Constabulary, 2009

Information Management Strategy, Alberta service, 2013, [http://www.im.gov.ab.ca/documents/publications/Information_Management_Strategy_FINAL.pdf]

Information Management Strategy, In-Form email Management, 2004, [http://dlmforum.typepad.com/Information_Management_Strategyv1.pdf]

Internet World Stats, 2012, [http://www.internetworldstats.com/stats.htm]

ITU-T Recommandation Y.2001, [http://www.itu.int/rec/T-RECY.2001-200412-I/en]

Jamasb T., Pollitt M., Electricity Market Reform in the European Union: Review of Progress toward Liberalization & Integration, Centre for Energy and Environmental Policy Research, 2005, [http://18.7.29.232/bitstream/handle/1721.1/45033/2005-003.pdf?sequence=1]

Janczewski L. J., Colarik A M., eds., Cyber Warfare and Cyber Terrorism, Hershey (PA), Information Science Reference, 2008

Juster K. I., Tritak J.S., Critical Infrastructure Assurance: A Conceptual Overview, in: Joint Economic Committee, United States Congress: Security in the Information Age – New Challenges, New Strategies (Washington, DC: White House), p. 12, 2002

Kameda T., Tsukasaki T., Hastie R., Berg N., Democracy uncertainty: The wisdom of crowds and the free-rider problem in group decision making, Psychological Review Vol, 118, Issue 1, pag. 76–96, 2011

Kapto A.S., Cyber warfare: Genesis and doctrinal outlines, Herald of the Russian Academy of Sciences, Volume 83, Issue 4, pp 357-364, July 2013, [http://download.springer.com/static/pdf/458/art%253A10.1134%252FS1019331613040023.pdf?auth66=1399802684_901c984d3238ffbc752deaa2d6473827&ext=.pdf]

Katz D.M. , Companies Counterattack Cyber Villains, 20th August, 2013, a, [http://ww2.cfo.com/risk-management/2013/08/companies-counterattack-cyber-villains/]

Katz D.M., Data Threats Spark Insurance Hunger, 21st August, 2013 , b, [http://ww2.cfo.com/risk-management/2013/08/data-threats-spark-insurance-hunger/]

Kim W., Jeong O., Kim C., So J., The dark side of the Internet: Attacks, costs and responses, Information Systems, Volume 36, Issue 3, Pages 675–705, Special Issue on WISE 2009 - Web Information Systems Engineering, May 2011,[http://ac.els-cdn.com/S0306437910001328/1-s2.0-S0306437910001328-main.pdf?_tid=29659b26-d4f5-11e3-bcd8-00000aacb360&acdnat=1399363697_406bac77fa7965db757e74c9658fc2fa]

Kramer A.,E-mail spam falls after Russian crack down, The New York Times, October 26,2010

Kramer F.D., Teplinsky M.J., Cybersecurity and Tailored Deterrence, Atlentic Council, 2014, [http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf]

Kshetri N., Pattern of global cyber war and crime: A conceptual framework, Journal of International Management, Volume 11, Issue 4 Pages 541–562, Global Security Risks and International Competitiveness, December 2005, [http://ac.els-cdn.com/S1075425305000700/1-s2.0-S1075425305000700-main.pdf?_tid=d58c29fa-d4f6-11e3-8952-00000aacb35e&acdnat=1399364416_35fefc7f45fe0cfab6c4c860a2aed617]

Lancaster H., Europe - Telecommunications Infrastructure and NGNs, 2013

Landry C. E., Li J., Participation in the Community Rating System of NFIP: Empirical Analysis of North Carolina Counties, Natural Hazards Review, 13(3): 205–220, 2012

Larson R., Marks D., Dahleh M., Ilic M., The 3 R's of Critical Energy Networks: Reliability, Robustness and Resiliency, MIT Energy Research Council, 2005, [http://cesf.mit.edu/papers/ThreeRs.pdf]

Lelarge M., Bolot J., Economic incentives to increase security in the internet: The case for insurance, Proceedings - IEEE INFOCOM, ISSN 0743-166X, ISBN 9781424435135, pp. 1494 - 1502, 2009

Levy, M., Salvadori, M., Why Buildings Fall Down, *W.W*. Norton & Compan, New York, 1992

Lewis A. M. , Ward D., Cyra L. , Kourti N., European Reference Network for Critical Infrastructure Protection, International Journal of Critical Infrastructure Protection, Volume 6, Issue 1, Pages 51–60, March 2013, [http://ac.els-cdn.com/S1874548213000073/1-s2.0-S1874548213000073-main.pdf?_tid=411f4b2e-adca-11e3-a116-00000aab0f6b&acdnat=1395057174_b02a376d678d7f7466871309a9791c50]

Lewis J. A., Assessing the risks of cyber terrorism, cyber war, and other cyber threats, 2002, [http://www.dtic.mil/dtic/]

Lewis T.G., Critical Infrastructure, Protection in homeland security- Defending a Networked Nation, Wiley Interscience, 2006, [http://books.google.it/books?hl=en&lr=&id=xoICniGegE0C&oi=fnd&pg=PR5&dq=critical+infrastructure+structure&ots=sC4M51MiY5&sig=8VWC5wdriXgukujcBg-8ZCuuqrc#v=onepage&q=critical%20infrastructure%20structure&f=false]

Little R.G., Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, 36th Hawaii International Conference on System Sciences, 2002, [http://www.computer.org/csdl/proceedings/hicss/2003/1874/02/187420058a.pdf]

Lord Jopling (Special Rapporteur), 162 CDS 07 E rev 1 – The Protection of Critical Infrastructures, 2007

Markoff J., A Code for Chaos, New York Times, October 2, 2010, [http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html]

Marsh, Benchmarking Trends: More Companies Purchasing Cyber Insurance, March 2013, [http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/29870/Benchmarking-Trends-More-Companies-Purchasing-Cyber-Insurance.aspx]

Marsh, Cyber Risk: Trends And Solutions, 2013, [http://usa.marsh.com/Portals/9/Documents/Marsh%20NROR%20September%202013%20Cyber%20Risk.pdf]

Màtl O., Smarter Cities as an European Agenda , IBM, 2010, [http://www-05.ibm.com/cz/public/pdf/Chytrejsi_mesta_jako_evropske_tema.pdf]

McAfee Labs, Global Energy Cyberattacks - “Night Dragon”, 2011

McAfee, Operation "Aurora" Hit Google, Others, 2010

Morningstar C., Farmer F.R., The Lessons of Lucas film's Habitat. The New Media Reader, Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, 2003. 664-667

Moteff J., Parfomak P., Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, 2004, [http://www.dtic.mil/dtic/tr/fulltext/u2/a454016.pdf]

Moteff J., Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, The Library of Congress, 2005, [http://www.fas.org/sgp/crs/homesec/RL32561.pdf]

Moteff J.D., Critical Infrastructures: Background, Policy and implementation, Report for Congress, 2002

Murer R., Internet of Things – Fundamentals, Agencia Click Isobar, 2010, [http://www.theinternetofthings.eu/content/internet-things-%E2%80%93-fundamentals-ricardo-murer]

Näf M., Ubiquitous Insecurity? How to 'Hack' IT Systems, Information & Security: An International Journal, no. 7, pp. 104–118, 2001

National Critical Information Infrastructure Protection Centre (NCIIPC), 2013

National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009, 2006

National Research Council, Making the Nation safer: The role of Science and Technology in Countering Terrorism, Committee on Science and Technology for Countering Terrorism, National Academy of Sciences, 2002 , [http://www.aaas.org/sites/default/files/migrate/uploads/ch23.pdf]

National Strategy for Critical Infrastructure Protection, CIP Strategy, Federal Republic of Germany
Federal Ministry of the Interior, 2009,
[http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf]

National Strategy for Critical Infrastructure Protection, CIP Strategy, 2009

NATO Cooperative Cyber Defense Centre of excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013,
[http://web.archive.org/web/20140306081257/http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf]

NISRA, Information Assurance policy statement by UK census office, June 2011

NIST, Improving Critical Infrastructure Cyber security Executive Order 13636 - Preliminary Cyber security Framework, 2014,
[http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf]

Norton Cybercrime Report, 2011

OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, 2002, [http://www.oecd.org/sti/ieconomy/15582260.pdf]

OECD Ministerial background report, Development of policies for protection of critical information infrastructures, 17th-18th June, 2008, [http://www.oecd.org/sti/40761118.pdf]

OECD recommendation of the council on the protection of critical information infrastructures, OECD ministerial meeting on the future of the Internet economy, 17th-18th June, 2008, [http://www.oecd.org/sti/40825404.pdf]

OECD, Shaping policies for the future of the Internet Economy, OECD Ministerial Meeting on the Future of the Internet Economy, 2008, [http://www.oecd.org/internet/ieconomy/40821707.pdf]

Ogut H., Menon N., Raghunatan S., Cyber Insurance and IT Security Investment : Impact of Interdependent Risk, University of Texas, 2004

Orszag P., Homeland and the Private Sector: Testimony before the National Commission on Terrorist Attacks Upon the United States, 19 November 2003, [http://www.brookings.edu/views/testimony/orszag/20031119.pdf]

Paget F., Hacktivism- Cyberspace has become the new medium for political voices, McAfee white paper, 2012

Pal R., Golubchik L., Psounis K., Aegis-A Novel Cyber-Insurance Model, University of Southern California, 2011

Pal R., Hui P., Cyber Insurance for Cyber Security- A Topological Take On Modulating Insurance Premiums, SIGMETRICS Performance Evaluation Review 40(3): 86-88, 2012

Pal R., Hui P., Cyber Insurance for Cyber Security- A Topological Take On Modulating Insurance Premiums, SIGMETRICS Performance Evaluation Review 40(3): 86-88, 2012

Passive Infrastructure Sharing in Telecommunications, kpmg, 2011, [http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Passive-Infrastructure-Sharing-in-Telecommunications.pdf]

Pederson P. , Dudenhoeffer D. , Hartley S., Permann M. , Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International Research, Idaho National Laboratory, August 2006, [http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf]

Perks J., Hyde J., Falconer A., Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, Final Report to European Commission Directorate-General Justice, Freedom and Security, 4th September, 2009, [http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf]

Perrin C., The CIA Triad, 2008,[http://www.techrepublic.com/blog/it-security/the-cia-triad/#]

Pfanner E., Europe unleashes online gambling to fill coffers, The New York Times, July 27,2010

Ponemon Institute LLC, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, august 2013

Power System Outage Task Force — Final Report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004

President Releases National Strategy for Homeland Security, 16 July, 2002, [http://www.hsdl.org/?view&did=474932]

President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations: Thinking Differently, GPO, Washington, 1997

President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, The White House, Washington, DC , 1997 [chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf]

Presidential Policy Directive 21 (PPD-21)-Critical Infrastructure Security and Resilience, 2013

Renn O., Risk Governance Towards an integrative approach, International Risk Governance Council, 2005, [http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf]

Reponen T., Information management strategy — an evolutionary process, Scandinavian Journal of Management, Volume 9, Issue 3, Pages 189–209, September 1993, [http://ac.els-cdn.com/095652219390016L/1-s2.0-095652219390016L-main.pdf?_tid=8d1badf4-cef1-11e3-8a61-00000aab0f27&acdnat=1398702440_731dd8aa4ff238688e917925eb044a6f]

Report on Critical Infrastructure protection; Ministry of the Interior 16/9/05

Riptech, Riptech Internet Security Threat Report, vol II, July 2002 , [http://www.4law.co.il/276.pdf]

Ritholtz B., Timeline of Cyber-Attacks from China, 2013, [http://www.ritholtz.com/blog/2013/02/china-cyber-attacks/]

Roberts A., Wallace W., McClure N., Strategic Risk Management, Edinburgh Business School, 2012, [http://www.ebsglobal.net/documents/course-tasters/english/pdf/h17rk-bk-taster.pdf]

Roper C. , Risk Management for Security Professionals, Butterworth-Heinemann, 1999

Rosen P.K. *et al.*, Cyber Insurance: A Last Line of Defense When Technology Fails, Latham & Watkins, April 15th, 2014

Rowlands D., Devlin A., Critical Energy Infrastructure Protection Policy Research Series-Insurance and Critical Infrastructure Protection Is there a Connection in an Environment of Terrorism? , n°8, 2006

Samani R., Common Assurance Maturity Model (CAMM)- The new business assurance barometer, CTO Cyber Security Forum, 2010, [http://www.fstech.co.uk/fst/FSTech_Conference_2011/Common_Assurance_Maturity_Model_Raj_Samani.pdf]

Sarrocco C., Ypsilanti D., Convergence and Next-Generation Networks , OECD, 2008, [http://www.oecd.org/sti/40761101.pdf]

Schelling T., Arms and Influence, New Haven: Yale University Press, 1966

Schmidt E., Cohen J., The New Digital Age: Reshaping the Future of People, Nations and Business, Knopf, 2013

Schultz E. E., A framework for understanding and predicting insider attacks, Proc. Of Compsec, pages 526–531, London, UK, October 2002

Sherstobitoff R., Analyzing Project Blitzkrieg, a Credible Threat, McAfee white paper, 2012

Shetty N., Schwartz G., Felegyhazi M., Walrand J., Competitive Cyber-Insurance and Internet Security, Economics of Information Security and Privacy, 229-247, 2010

Soafer A. D., The Best Defense? Legitimacy and Preventive Force, Stanford, Hoover Institution Press, 2010

Stanton, J.J., Terror in Cyberspace, American Behavioral Scientist, Vol. 45, no.6, pag.1017–1032, 2002

Strategic risk management, NYU Stern School of Business, [http://people.stern.nyu.edu/adamodar/pdfiles/papers/strategicrisk.pdf]

Suter M., A Generic National Framework For Critical Information Infrastructure Protection (CIIP), International telecommunication unit, 2007, [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf]

Tatum M., What Is a Cyber-attack?, 2010, [http://www.wisegeek.com/what-is-a-cyberattack.htm]

Thales, A practical guide to assessing your cyber security strategy, White paper, March 2012

The American Heritage Dictionary of the English Language, Fourth Edition, Houghton,2000

The Department of Commerce- Internet Policy Task Force, Cyber security, Innovation and the Internet Economy, June 2011, [http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf]

The Parliamentary Office of Science and Technology, Resilience of UK Infrastructure, no 362, 2010, [http://www.google.it/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=6&cad=rja&ved=0CF8QFjAF&url=http%3A%2F%2Fwww.parliament.uk%2Fbriefing-papers%2Fpost-pn-362.pdf&ei=uVcHU_fWI4el4ASk_YHwCw&usg=AFQjCNEZWRq81ObgzipvBaIr3uUB1iZhUQ&sig2=7kPJjrJYNF0_vW7Tl0zTzA&bvm=bv.61725948,d.bGQ]

The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought, Business Insider,20 November 2013, [http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11]

Thissen W.A.H., Herder P.M. (Eds.), Critical Infrastructures. State of the Art in Research and Application, Kluwer Academic, 2003

Townsend A. M., Moss M.L., Telecommunications infrastructure in disasters: Preparing cities for crisis communications, Centre for Catastrophe Preparedness and Response and Robert F. Wagner Graduate School of Public Service New York University, 2005, [http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf]

Trimintzios P., Hall C., Clayton R., Anderson R., Ouzounis E., Resilience of the Internet Interconnection Ecosystem, ENISA, 2011, [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report]

U.S. Intelligence Community's March 2013 Worldwide Threat Assessment, [www.intelligence.senate.gov/130312/clapper.pdf]

U.S. Office of Homeland Security. July 16, 2002

UK Government Actuary's Department, A practical guide to strategic risk management, 28th August, 2013, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/256431/A_Practical_Guide_to_Strategic_Risk_Management.pdf]

Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, PUBLIC LAW 107–56—OCT. 26, 2001, [http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf]

US Department of Defence Directive 8500.1, Information Assurance, October 24, 2002

US Department of Homeland Security, Blueprint for a Secure Cyber Future: The Cyber security Strategy for the Homeland Security Enterprise, November 2012, [http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm]

US Government, H. R. 2281 Digital Millennium Copyright Act , 1998

US Government's Paperwork Reduction Act of 1980

US Homeland Security, Cyber security Insurance workshop, 2012, [http://www.dhs.gov/publication/cybersecurity-insurance]

van Eeten M.J.G. , Roe E.M., Schulman P., de Bruijne M.L.C. , The Enemy Within: System Complexity and Organizational Surprises, in M. Dunn and V. Mayer (eds), International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects, Zurich, Center for Security Studies at ETH Zurich, pp. 89–109, 2006, [www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>]

Vanston L.K., Hodges R.L., Forecasts for the US Telecommunications Network, Telenor ASA, 2009, [http://www.tfi.com/pubs/w/pdf/telektronikk_telecom.pdf]

Virilio P., Lotringer S., Pure War, New York: Semiotext, 1983

WBGU , World in Transition – Strategies for Managing Global Environmental Risks, Annual Report, 1998

Wehde E.,US Vulnerable to Cyber terrorism, Computer Fraud & Security, pag. 6-7, 1998

Wenger A., Metzger J., Dunn M., International CIIP Handbook- An inventory of protection policies in eight countries, Centre for Security Studies, ETH Zurich, 2002, [http://e-collection.library.ethz.ch/eserv/eth:31123/eth-31123-01.pdf]

What is critical infrastructure?, Australian National Security, [www.ag.gov.au/agd]

Wilke B.J., A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events, Carnegie Mellon University, 2007

Wilsker I., Cyber Crime, Cyber Terrorism, Cyber War, [http://apcug2.org/sites/default/files/cybercrime_cyberterrorism_cyberwar_apcug80412.pdf]

Wilson C., Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. CRS Report for Congress, January 29th, 2008

Wired, Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise, 2007, [http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1]

World Wide Web Size, 2014, [http://www.worldwidewebsize.com/]

Zacaria F., Big Data, Meet Big Brother. If computers can now predict our behaviour, should governments watch our every movie?, in Time 8-15 July, 2013