Developing a Framework to Improve Critical Infrastructure Cybersecurity

Presented by Joe Wilson
Network Security Engineer
TelcoCapital IT Systems, LLC

Dissertation Presented in Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy

Cybersecurity Framework Development: Design Science Research toward an Intercloud Transparent Bridge Architecture

(ITCOBRA)

CAPELLA UNIVERSITY
A National Center of Academic Excellence in Information Assurance Education
(CAE/IAE)

March 2013

Abstract

This dissertation uses design science research to develop a cloud-based simulator that implements industry standards for developing a cybersecurity framework for critical infrastructure protection (CIP) in the United States. This research asserts that an agile and neutral framework extending throughout the cyber-threat plane is needed for effectively defending against sophisticated cybersecurity attacks. An effective framework should have predictive analysis and interdiction (PAI) capabilities for preemptive threat mitigation. The outcome of this research is the Intercloud Transparent Bridge Architecture/Simulator Model (ITCOBRA/SM). Inspiration for the ITCOBRA/SM is drawn from the intersection of cloud computing advancements, information technology (IT), cybersecurity, and critical infrastructure protection techniques. The operational context of the ITCOBRA is analogous to that used by meteorologist to forecast the weather. Weather forecasts are made by collecting quantitative data about the current state of the atmosphere on a given location. Using scientific understanding of atmospheric processes, meteorologist can project how the atmosphere will evolve over time (Intellicast.com). Likewise, the ITCOBRA enables projections to be made about events occurring in the cyber threat plane. Using Markov modeling, holistic information about the state of cyber critical systems is collected. Accelerated threat analytics in centralized databases integrate, correlate and synchronize the information to make projections about how threats will evolve and which systems are at risk. The gathered intelligence is used to make informed decisions that reflect organizations' predefined security policies. It is noteworthy that the accelerated space-time domain is simulated by the ITCOBRA/SM. In real world deployments that use the ITCOBRA Framework

("Framework"), the accelerated predictive analysis is performed by applications resident in the system. It is also envisioned that quantitative data will be extracted from an organization such as the US Computer Emergency Readiness Team (US-CERT), and/or similar databases. Autonomic computational methods are recommended in future research for the ITCOBRA Framework to enable organic functionality for higher levels of efficiency. Finally, this research is timely since cybersecurity practices in the United States diverge significantly and have failed to establish a 21st century cyber protection framework for the nation's critical systems (Shiffman & Gupta, 2013).

Table of Contents

List of Tables

List of Figures

Introduction

Cloud Paradigm. The cloud paradigm introduces significant performance metrics and economies of scale over traditional IT technologies. Web-based technologies are increasingly being used to deploy core services in critical infrastructure cybersecurity protection networks (Cardellini, Casalicchio, Tucci, & dei Ministri, 2006). Simultaneously, there is on-going research towards developing an Inter-Cloud Architecture (ICA) to address architectural challenges in creating a transparent information plane over different provider systems to allow seamless application services (Demchenko, Ngo, Makkes, Stgrijkers, & de Laat, 2012) . Advancements in cloud computing and cloud simulation technologies provide organizations the opportunity to evaluate application scenarios that would be too costly or prohibitive in today's vendor specific cloud computing environments.

Effectively coordinating and managing cybersecurity data requires a federated intercloud architecture. The need for intercloud negotiation is a topic of high interest and established as a priority in literature (R. N. Calheiros, Ranjan, De Rose, & Buyya, 2009). The global expansion of the Internet makes it possible for adversaries to launch cyber attacks from any location on the globe (Bhatia, 2011; Geers, 2010). In this dissertation research the ITCOBRA/SM model will be developed to answer the research question related to comprehensive cybersecurity coordination. The requirement for dynamic exchange of cybersecurity information remains a difficult, unresolved challenge for organizations responsible for critical infrastructure protection (Warfield, 2012). The threats posed by cyber terrorism have been a major topic for public and private

organizations during the past decade (Fischer, 2011). The corollary is that the vitality of the nation's economy and the livelihood of its citizens depend on these critical systems and structures (Moteff, 2010). The call for the federal government to modernizing the current protection framework is also growing in government and industry. This research investigates and implements innovations in emerging cloud computing technologies for high density cyber security coordination.

The ITCOBRA/SM accomplishes inter-domain communications in a federated deployment by focusing on the security access domain, policy management and open source API (Application Program Interface) standards. The artifact is run and tested on a general purpose computer in a lab environment. This dissertation extends the research instruments and theory developed by (A. Beloglazov & Buyya, 2011; 2011; R. N. Calheiros, Ranjan, Beloglazov, De Rose, & Buyya, 2011; 2010; Martin, 2011). Design Science Research (DSR) is used in this study to explore the intersection of CIP strategies, cybersecurity frameworks, cloud computing technologies and virtualized resource modeling and simulation.

Research Methodology for the ITCOBRA/SM

The research methodology for this dissertation is shown in Figure 1. This research belongs to the design science paradigm (A. R. Hevner, March, Park, & Ram, 2004; March & Smith, 1995). It strives for developing a practically relevant IT artifact in form of a domain independent, purpose specific artifact (Becker, Janiesch, Pfeiffer, & Seidel, 2006). The research methodology is based on the work of Takeda et al. (Takeda, Veerkamp, & Yoshikawa, 1990).

Research Method

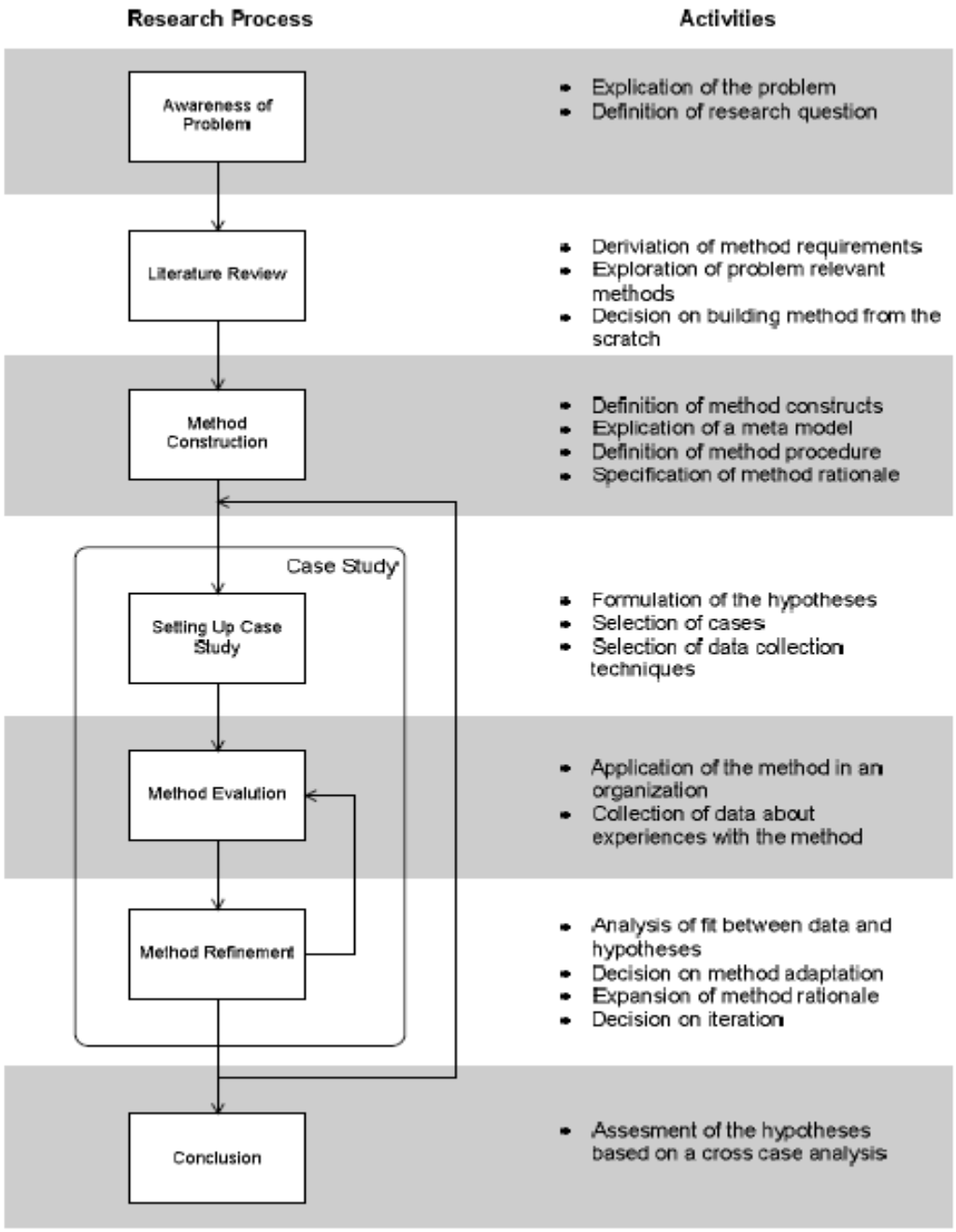


Figure 1. Research Methodology of this Paper

Background of the Study

Critical infrastructures are dispersed throughout the United States government and private industry. The majority of these are in private sector organizations that are subject to direct government oversight. Catastrophic disruptions to any of these systems can significantly impact United States societies (Warfield, 2012).

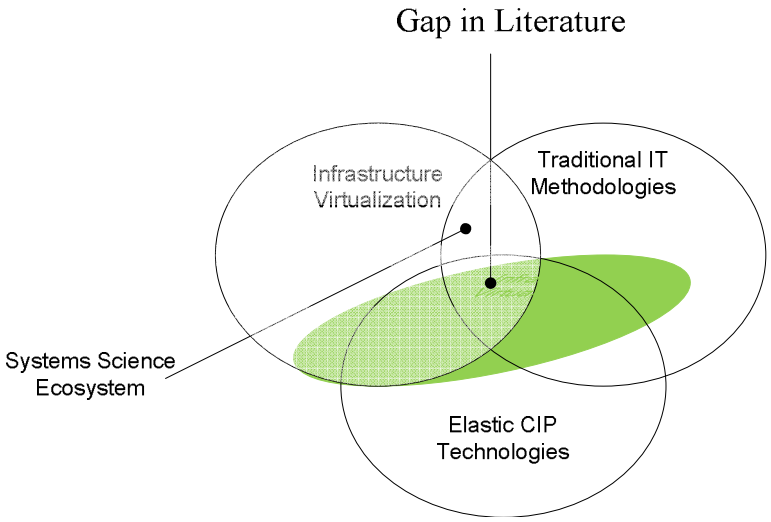
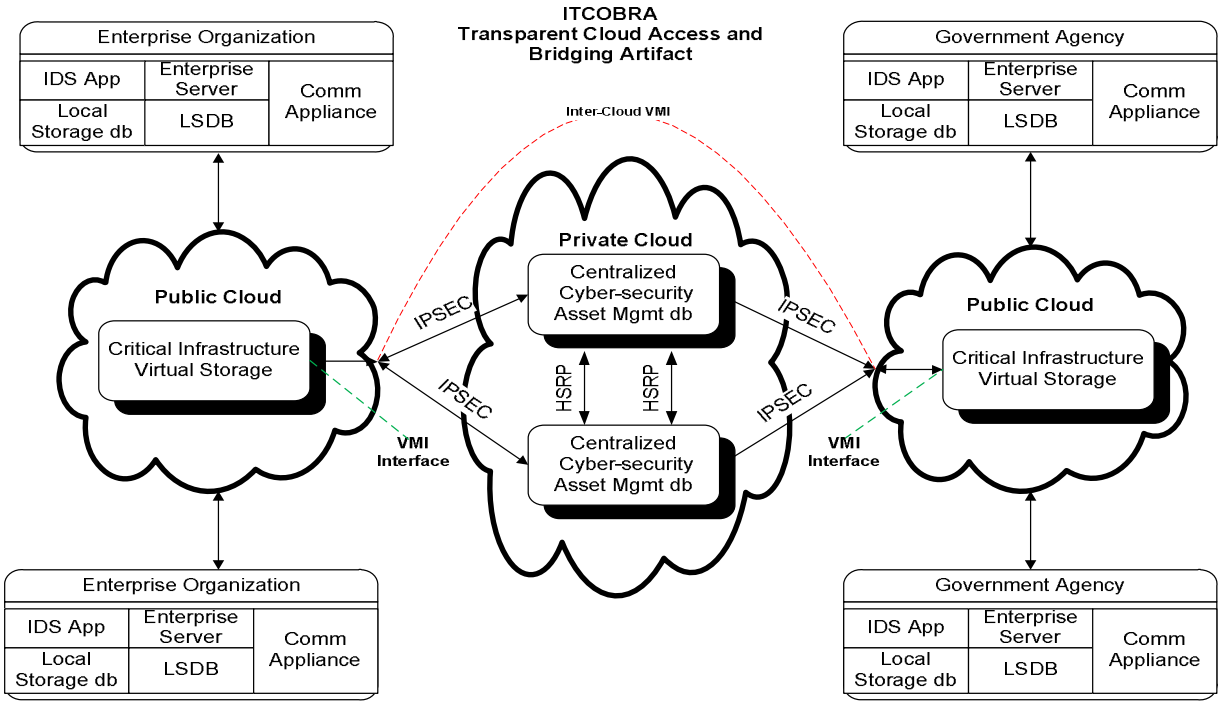


Figure 2. ITCOBRA/SM Intervention
The three synthesis domains for the transparent cloud access and Development/Prototyping methodology to address the gap in current research and development are shown in Figure 2. Source: The author of this dissertation research. Adapted from Martin (2011)

This research develops an intercloud communications artifact for more efficient coordination of critical infrastructure information in public and private organizations. The ITCOBRA/SM prototype uses existing techniques for developing the prototype model.

ITCOBRA Initial Conceptual Diagram



Legend:
IDS Intrusion Detection System
LSDB Local Storage Database
VMI Virtual Machine Interface

Figure 3. The ITCOBRA/P Simple Message Exchange

CHAPTER 2. LITERATURE REVIEW

Critical infrastructures are dispersed throughout the United States government and private industry. The majority of these are in private sector organizations that are subject to direct government oversight. Catastrophic disruptions to any of these systems can significantly impact United States societies (Warfield, 2012).

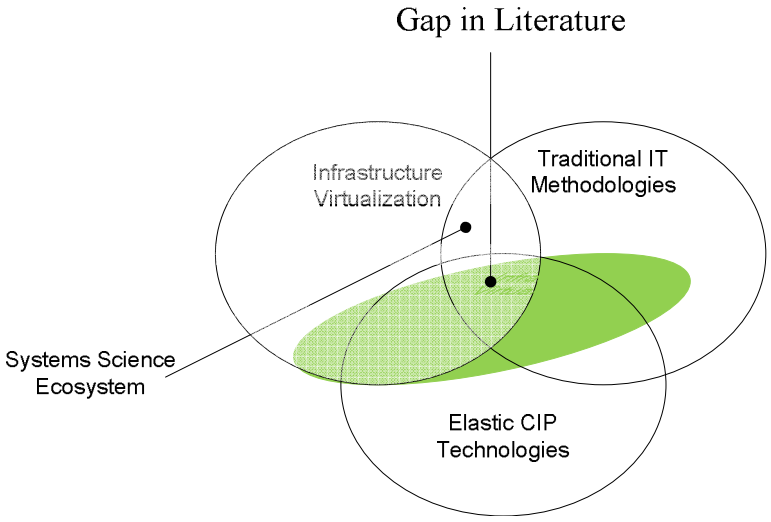


Figure 4. Gap in Literature
In Figure 4 (recaptured from Figure 3) shows the research domains and development environment that the transparent cloud access and Development/Prototyping methodology are synthesized to address the gap in current research and development. Source: The author of this dissertation research. Adapted from Martin (2011).

REFERE CES

Alcaraz, C., Lopez, J., Zhou, J., & Roman, R. (2011). Secure SCADA framework for the protection of energy control systems. *Concurrency and Computation: Practice and Experience, 23*(12), 1431-1442.

Alexander, K. (2012). Agencies won't read Americans' email for security: General - technology & science - security - NBCNews.com. Retrieved 9/10/2012, 2012, from http://www.msnbc.msn.com/id/48128455/ns/technology_and_science-security/t/spy-agencies-wont-read-americans-email-security-general/

Allen, J., Burch, L., Carter, C., Jose, J., Mcclain, C., & Olds, D. (2010). In Novell I. (Ed.), *System and method for transparent cloud access - patent application no. 20100235903*(726 15 ed.) AG06F2100FI. Retrieved from http://www.faqs.org/patents/app/20100235903

Anderson, A., Doll, A., Giblin, A., Jennings, M., Pirrong, R., Shaffer, S., & Stasny, G. (2011). Critical infrastructure and cyber security. A project for dr. Engel's capstone at the bush school of government and public service. *CE TRA Technology*, Retrieved from http://scholar.googleusercontent.com/scholar?q=cache:56yfAq6xUIAJ:scholar.google.com/&hl=en&as_sdt=1,3

An-ka, Z., Ping, S., Bing-xia, H., & Min-jiao, Z.Reflection of the nation Cybersecurity's evolution.

Annapureddy, K. (2011). *Security challenges in hybrid cloud infrastructures. aalto university, T-110.5290 seminar on network security* Retrieved from http://www.cse.hut.fi/en/publications/B/11/papers/annapureddy.pdf

Apke, T. M., & Parry, R. O. (2007). Planning ownership of intellectual property rights in web and software development. *.27(3)*(8)

Avizienis, A., Laprie, J., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on, 1*(1), 11-33.

Basu, S. (2011). *Simple and secure VM migration to and from the cloud.* ().

Becker, J., Janiesch, C., Pfeiffer, D., & Seidel, S. (2006). Evolutionary method Engineering–Towards a method for the analysis and conception of management

information systems. Paper presented at the *Proceedings of the 12th Americas Conference on Information Systems*, 3922-3922.

Beloglazov, A., & Buyya, R. (2012). Managing overloaded hosts for dynamic consolidation of virtual machines in cloud data centers under quality of service constraints. *IEEE Transactions on Parallel and Distributed Systems (TPDS),*

Beloglazov, A., Buyya, R., Lee, Y. C., & Zomaya, A. (2011). A taxonomy and survey of energy-efficient data centers and cloud computing systems. *Advances in Computers, 82*, 47-111.

Beloglazov, A., & Buyya, R. (2011; 2011). Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers *Concurrency and Computation: Practice and Experience*, , n/a <last_page> n/a. doi: 10.1002/cpe.1867

Benjamin, R. (2007).
Ending the cyber jihad: Combating terrorist exploitation of theInternet with the rule of law and improved tools for cyber governance. *Comm Law Conspectus, 15*, 119-186.

Bernstein, D., Vij, D., & Diamond, S. (2011). An intercloud cloud computing economy-technology, governance, and market blueprints. Paper presented at the *SRII Global Conference (SRII), 2011 Annual*, 293-299.

Bernstein, D. (2009). Keynote 2: The intercloud: Cloud interoperability at internet scale. Paper presented at the *etwork and Parallel Computing, 2009. PC '09. Sixth IFIP International Conference on*, xiii-xiii.

Bernstein, D., & Vij, D. (2010). Intercloud security considerations. Paper presented at the *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, 537-544.

Bhatia, M. S. (2011). World war III: The cyber war. *International Journal of Cyber Warfare and Terrorism (IJCWT), 1*(3), 59-69.

Bhatti, D., Awais, M., Hussain, F., KalianiSundram, D., & Pandiyan, V. (2012). An soa based real time information exchange between military and government owned rescue services. *Far East Journal of Psychology and Business, 7*(3), 29-55.

Biesecker, C. (2011). House members introduce cyber bill to protect critical infrastructure. *Defense Daily, 252*(52), 10-10. Retrieved from http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=70534734&site=ehost-live&scope=site

Biswas, S. (2012). US army awards first cloud computing contract | CloudTweaks Retrieved 9/8/2012, 2012, from http://www.cloudtweaks.com/2012/01/us-army-awards-first-cloud-computing-contract/

Bohn, R. B., Messina, J., Fang Liu, Jin Tong, & Jian Mao. (2011). NIST cloud computing reference architecture. Paper presented at the *Services (SERVICES), 2011 IEEE World Congress on*, 594-596.

Bompard, E., Napoli, R., & Xue, F. (2009). Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection, 2*(1-2), 5-12. doi: DOI: 10.1016/j.ijcip.2009.02.002

Branscomb, L. M. (2006). Sustainable cities: Safety and security. *Technology in Society, 28*(1-2), 225-234. doi: DOI: 10.1016/j.techsoc.2005.10.004

Buyya, R., Broberg, J., & Andrzej, G. (2011). *Cloud computing* Wiley Online Library.

Buyya, R., Ranjan, R., & Calheiros, R. (2010). Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. *Algorithms and Architectures for Parallel Processing, ,* 13-31.

Buyya, R. (2010). Cloud computing: The next revolution in information technology. Paper presented at the *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*, 2-3.

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. F., & Buyya, R. (2011). CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and Experience, 41*(1), 23-50.

Calheiros, R. N., Ranjan, R., De Rose, C. A. F., & Buyya, R. (2009). Cloudsim: A novel framework for modeling and simulation of cloud computing infrastructures and services. *Arxiv Preprint arXiv:0903.2525,*

Calheiros, R. N., Toosi, A. N., Vecchiola, C., & Buyya, R. (2012). A coordinator for scaling elastic applications across multiple clouds. *Future Generation Computer Systems,*

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. F., & Buyya, R. (2011; 2010). CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms *Software: Practice and Experience, 41*(1), 23 <last_page> 50. doi: 10.1002/spe.995

Cao, H., Zhu, P., Lu, X., & Gurtov, A. (2013). A layered encryption mechanism for networked critical infrastructures. *etwork, IEEE, 2*(1), 12-18.

Cardellini, V., Casalicchio, E., Tucci, S., & dei Ministri, P. C. (2006). AGENT-BASED MODELING OF WEB SYSTEMS IN CRITICAL INFORMATION INFRASTRUCTURES. *Proceedings of Complex etwork Infrastructure Protection,*

Castro, D. (2011). uS federal cyberSecuriTy policy. *Cybersecurity: Public Sector Threats and Responses,* , 127.

Chen Yiming, & Zhu Yiwei. (2011). SaaS vendor selection basing on analytic hierarchy process. Paper presented at the *Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on,* 511-515.

Chen, S., Nepal, S., & Liu, R. (2011). Secure connectivity for intra-cloud and inter-cloud communication. Paper presented at the *Parallel Processing Workshops (ICPPW), 2011 40th International Conference on,* 154-159.

Chessa, S., & Santi, P. (2001). Comparison-based system-level fault diagnosis in ad hoc networks. Paper presented at the *Reliable Distributed Systems, 2001. Proceedings. 20th IEEE Symposium on,* 257-266.

Chittester, C. G., & Haimes, Y. Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security & Emergency Management, 1*(4), 1-20. Retrieved from http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=15215257&site=ehost-live&scope=site

Cohen, F. (2010). What makes critical infrastructures critical? *International Journal of Critical Infrastructure Protection, 3*(2), 53-54. doi: 10.1016/j.ijcip.2010.06.002

Collins, H., & Samuels, A. (2010). In MCKENNA C., (Ed.), *SYSTEMS A D METHODS FOR REAL-TIME E DPOI T APPLICATIO FLOW CO TROL WITH ETWORK STRUCTURE COMPO E* WIPO Patent WO/2010/042,578.

Copeland, C., & Cody, B. (2007). Terrorism and security issues facing the water infrastructure sector. *Focus on Terrorism,* , 257.

Crowther, K. G. (2008). Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input–output model. *International Journal of Critical Infrastructure Protection, 1,* 53-67. doi: DOI: 10.1016/j.ijcip.2008.08.009

Cukier, K., Mayer-Schoenberger, V., & Branscomb, L. (2005). Ensuring (and insuring?) critical information infrastructure protection. *SSR Working Paper Series,* Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=1451419261&Fmt=7&clientId=62763&RQT=309&VName=PQD

Dayananda, M., & Kumar, A. (2012). Architecture for inter-cloud services using IPsec VPN. Paper presented at the *2012 Second International Conference on Advanced Computing & Communication Technologies*, 463-467.

Demchenko, Y., de Laat, C., Van der Ham, J., Ghijsen, M., Yakovenko, V., & Cristea, M. (2011). On-demand provisioning of cloud and grid based infrastructure services for collaborative projects and groups. Paper presented at the *Collaboration Technologies and Systems (CTS), 2011 International Conference on*, 134-142.

Demchenko, Y., Ngo, C., Makkes, M., Stgrijkers, R., & de Laat, C. (2012). Defining inter-cloud architecture for interoperability and integration. Paper presented at the *CLOUD COMPUTI G 2012, the Third International Conference on Cloud Computing, GRIDs, and Virtualization*, 174-180.

Desmedt, Y. (2002). Is there a need for survivable computation in critical infrastructures? *Information Security Technical Report, 7*(2), 11-21. doi: DOI: 10.1016/S1363-4127(02)02003-4

Devenny, J. (2004). *Critical digital infrastructure protection: An investigation into the intergovernmental activities of information technology directors in florida counties.* (Ph.D., University of Central Florida). *ProQuest Dissertations and Theses*, . (MSTAR_305082755).

DHS. (n.d.). Secure cyber networks | homeland security Retrieved 9/15/2012, 2012, from http://www.dhs.gov/secure-cyber-networks

DHS | national cyber security awareness month Retrieved 7/29/2012, 2012, from http://www.dhs.gov/files/programs/gc_1158611596104.shtm

Dunn Cavelty, M., & Suter, M. (2012). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection.

Eack, K. (2008). State and local fusion centers: Emerging trends and issues. *Homeland Security Affairs*, , 1-6.

Egan, M. J. (2007). Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. *Journal of Contingencies & Crisis Management, 15*(1), 4-17. doi: 10.1111/j.1468-5973.2007.00500.x

E-Government Unit. (2000). *E-government: Protecting new Zealand's infrastructure from cyber-threats.* (No. SI 3/2/12). New Zealand: State Services Commission. Retrieved from http://archive.ict.govt.nz/plone/archive/policy/trust-security/niip-report/niip-report.pdf

FCC. (n.d.). Topic 19: Communications interdependencies Retrieved 8/4/2012, 2012, from http://transition.fcc.gov/pshs/techtopics/techtopics19.html

Fielding, R. T., & Taylor, R. N. (2002). Principled design of the modern web architecture. *ACM Transactions on Internet Technology (TOIT), 2*(2), 115-150.

Fischer, E. A. (2011). Federal laws relating to cybersecurity: Discussion of proposed revisions.

Fittkau, F., Frey, S., & Hasselbring, W. (2012). CDOSim: Simulating cloud deployment options for software migration support.

Gable, K. (2009). Cyber-apocalypse now: Securing the internet against cyberterrorism and using universal jurisdiction as a deterrent. *SSR Working Paper Series,* Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=1852426531&Fmt=7&clientId=62763&RQT=309&VName=PQD

GAO. (2009). *Critical infrastructure protection: OMB leadership needed to strengthen agency planning efforts to protect federal cyber assets.* (Congressional No. GAO-10-148).U.S. GAO. . (Report to Congressional Requesters)

GAO. (2011). *CRITICAL I FRASTRUCTURE PROTECTIO : Cybersecurity guidance is available, but more can be done to promote its use.* (Report to Congressional Requesters No. GAO-12-92).

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review, 26*(3), 298-303. doi: DOI: 10.1016/j.clsr.2010.03.003

Gorge, M. (2007). Cyberterrorism: Hype or reality? *Computer Fraud & Security, 2007*(2), 9-12. doi: DOI: 10.1016/S1361-3723(07)70021-0

Gorman, S. P., Schintler, L., Kulkarni, R., & Stough, R. (2004). The revenge of distance: Vulnerability analysis of critical information infrastructure. *Journal of Contingencies & Crisis Management, 12*(2), 48-63. doi: 10.1111/j.0966-0879.2004.00435.x

Granado, N., & White, G. (2008). Cyber security and government fusion centers. Paper presented at the *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual,* 205-205.

Haimes, Y. Y., & Chittester, C. G. (2005). A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems. *Journal of Homeland Security & Emergency Management, 2*(2), 1-21. Retrieved from

http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=17714056&site=ehost-live&scope=site

Hamaker, C. (2006). What's next for cyber-security? *Public Utilities Fortnightly, 144*(8), 34. Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=1096130151&Fmt=7&clientId=62763&RQT=309&VName=PQD

Hare, F., & Goldstein, J. (2010). The interdependent security problem in the defense industrial base: An agent-based model on a social network. *International Journal of Critical Infrastructure Protection, 3*(3–4), 128-139. doi: 10.1016/j.ijcip.2010.07.001

Harrison, W., Krings, A., Hanebutte, N., & McQueen, M. (2002). On the performance of a survivability architecture for networked computing systems. Paper presented at the *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, 2534-2542.

Haslum, K. (2010). *REAL-TIME ETWORK I TRUSIO PREVE TIO ,*

Hato, K., Bo Hu, Murata, Y., & Murayama, J. (2012). Designing inter-cloud system architecture. Paper presented at the *Optical Internet (COI), 2012 10th International Conference on*, 75-76.

Hennessy, J. L., Patterson, D. A., & Lin, H. (2003). *Information technology for counterterrorism: Immediate actions and future possibilities* Natl Academy Pr.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly, ,* 75-105.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-75-105. Retrieved from http://library.capella.edu/login?url=http://search.proquest.com/docview/218119584?accountid=27965

Holgate, J., Williams, S. P., & Hardy, C. A. (2012). Information security governance: Investigating diversity in critical infrastructure organizations.

Host, P. (2012). Northrop CEO: Info sharing, right to monitor networks critical to potential cyber bills. *Defense Daily, 254*(10), 1-1. Retrieved from http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=76258097&site=ehost-live&scope=site

Howell, F., & McNab, R. :. (1997). *SimJave: A discrete event simulation library of java.* Edinburg, Scotland: University of Edinburg.

Hutchinson, K. (2012). HUTCHISON: A cybersecurity solution | politics - home Retrieved 8/11/2012, 2012, from http://www.ksat.com/news/politics/HUTCHISON-A-cybersecurity-solution/-/2567674/16064608/-/4cqg85/-/index.html

Hwang, K., Fox, G. C., & Dongarra, J. J. (2011). Cloud architecture and datacenter design. *Distributed and cloud computing: Clusters, grids, clouds, and the future internet* (pp. 7-1-7-57). Watham, MA: Morgan Kaufmann. Retrieved from http://www.cs.gsu.edu/~cscnxx/Chapter7-Cloud-Architecture-May2-2010.pdf

IBM. (2012). *System programming APIs* [null] (IMS Version 11 ed.) IBM Corporation.

Jain, S., Hutchings, C., Lee, Y., & McLean, C. (2010). A knowledge sharing framework for homeland security modeling and simulation. Paper presented at the *Winter Simulation Conference (WSC), Proceedings of the 2010,* 3460-3471.

James, J., & Verma, B. (2012). EFFICIENT VM LOAD BALANCING ALGORITHM FOR A CLOUD COMPUTING ENVIRONMENT. *International Journal, 4*

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *IST Special Publication,* 800-144.

Jiang, G., Cybenko, G., & McGrath, D. (2001). Infrastructure web: Distributed monitoring and managing critical infrastructures. Paper presented at the *Enabling Technologies for Law Enforcement,* 104-114. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.124.2912

Jin, H., Ibrahim, S., Bell, T., Qi, L., Cao, H., Wu, S., & Shi, X. (2010). Tools and technologies for building clouds. *Cloud Computing,* , 3-20.

Jones, A. (2005). Cyber terrorism: Fact or fiction. *Computer Fraud & Security, 2005*(6), 4-7. doi: DOI: 10.1016/S1361-3723(05)70220-7

KDM Analytics. (2012). A security assurance company. Retrieved February/15, 2013, from http://www.kdmanalytics.com/kdma/index.html

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer, 36*(1), 41-50.

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud migration: A case study of migrating an enterprise it system to iaas. Paper presented at the *2010 IEEE 3rd International Conference on Cloud Computing,* 450-457.

Knapp, K., & Boulton, W. (2006). Cyber-warefare threatens corporations: Expansion into commercial environments. *Information Systems Management, 23*(2), 76-87.

Krings, A., & Oman, P. (2003). Secure and survivable software systems. *IEEE Proc.HICSS-36, Minitrack on Secure and Survivable Software Systems*, , 334a.

Krings, A., & Azadmanesh, A. (2005). A graph based model for survivability applications. *European Journal of Operational Research, 164*(3), 680-689.

Krings, A., Harrison, W., Azadmanesh, M., & McQueen, M. (2002). The impact of hybrid fault models on scheduling for survivability. Paper presented at the *Wkshp on Scheduling in Computerand Manufacturing Systems, Seminar, , 2231*

Krings, A. W. (2004). Agent survivability: An application for strong and weak chain constrained scheduling. Paper presented at the *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 8 pp.

Krings, A. W., WILLIAM, S. H., Azadmanesh, A., & Mcqueen, M. (2004). Scheduling issues in survivability applications using hybrid fault models. *Parallel Processing Letters, 14*(01), 5-22.

Krings, A., & Oman, P. (2003). A simple GSPN for modelling common mode failures in critical infrastructures. Paper presented at the *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, 10 pp.

Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. *European Journal of Information Systems, 17*(5), 489-504.

Kuechler, W., & Vaishnavi, V. (2008). *Design science research methods and patterns: Innovating information and communication technology*. Boca Raton, FL: Auerbach Pub.

Kuechler, W., & Vaishnavi, V. (September 30, 2011.). Design science research in information systems. Retrieved 11/26, 2011, from http://desrist.org/desrist

Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. *European Journal of Information Systems, 17*(5), 489-489-504. Retrieved from http://library.capella.edu/login?url=http://search.proquest.com/docview/218790486?accountid=27965

Kuehl, D., & Miller, R. A. (2009). Cyberspace and the “First battle” in 21st-century war. *Center for Technology and ational Security Policy ational Defense University, 68*(September 2009)

Kundra, V., & Chief Information Officers Council (U.S.). (2011). *Federal cloud computing strategy*. (Congressional Report).The White House. Retrieved from

http://www.theresearchpedia.com/sites/default/files/Federal%20Cloud%20Computing%20Strategy.pdf

Kurze, T., Klems, M., Bermbach, D., Lenk, A., Tai, S., & Kunze, M. (2011). Cloud federation. Paper presented at the *CLOUD COMPUTI G 2011, the Second International Conference on Cloud Computing, GRIDs, and Virtualization*, 32-38.

Lakhani, J., & Kumar, P. (2012). Resource selection strategy based on propagation delay in cloud. Paper presented at the *Communication Systems and etwork Technologies (CS T), 2012 International Conference on*710-713.

Lewis, T. G. (2006a). *Critical infrastructure protection in homeland security: Defending a networked nation* John Wiley and Sons.

Lewis, T. G. (2006b). *Critical infrastructure protection in homeland security: Defending a networked nation* John Wiley and Sons.

Liden, R., Halls, D., Waterhouse, S., & Benoit, P. (2011). *Systems and methods for establishing a cloud bridge between virtual storage resources - patent application* (711163rd ed.) AG06F1200FI. Retrieved from file:///G:/CAPELLA/2012_SummerTerm/AAA_Committee%20Work/Research/Patents/CloudBridge%2020110022812/CloudBridge%20between%20Virtual%20Storage%20Resources.htm

Limbani, D., & Oza, B. (2012). A proposed service broker strategy in CloudAnalyst for cost-effective data center selection. *Int.J.Computer Technology & Applications, Vol 3 (3), ISS :2229-6093*1082-1087) Retrieved from http://www.ijccr.com

Lindquist, C. (2005). A new blueprint for I.T. ; A service-oriented architecture can be a powerful tool for changing your business-or a good way to boil the ocean. the keys to a successful SOA project are setting limits, mitigating risks, and giving the business what it wants and needs. *CIO, 18*(21), 1. Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=883243471&Fmt=7&clientId=62763&RQT=309&VName=PQD

Liu, E., Stevens, G., Ruane, K. A., Dolan, A. M., & Thompson, R. M. (2012). Cybersecurity: Selected legal issues. *Congressional Research Service, 7-5700*

Mabry, P. L., Marcus, S. E., Clark, P. I., Leischow, S. J., & Mendez, D. (2010). Systems science: A revolution in public health policy research. *American Journal of Public Health, 100*(7), 1161.

Malhotra, M. (2011). Simulation for enhancing the response and processing time of datacenters. *International Journal of Computing and Corporate Research, 1*(3) Retrieved from http://www.ijccr.com/November2011/8.pdf

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

Marshall, P., Keahey, K., & Freeman, T. (2011). Improving utilization of infrastructure clouds. Paper presented at the *Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on*, 205-214.

Martin, D. (2011). *ovamente artificial general intelligence: Design science research towards a designing / prototyping model.* Capella University). *ProQuest Dissertations and Theses, .* (MSTAR_904636893).

McCrohan, K. F. (2003). Facing the threats to electronic commerce. *Journal of Business & Industrial Marketing, 18*(2), 133-145.

Medina, A., Lakhina, A., Matta, I., & Byer, J. (2001). BRITE: An approach to universal topology generation. [null] *Proceedings of the 9th International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems,* (MASCOTS 2001)

Melvin, J. (2012). White house may use executive order to protect key computer networks. Retrieved 11/19/2012, 2012, from http://in.reuters.com/article/2012/08/08/net-us-usa-security-cyber-idINBRE8771F220120808

Merkel, C. M. (2012). Article 9: Information sharing and transparency. Paper presented at the *The U ESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions*, 245-282.

Microsoft TechNet. (2012). Private cloud principles, patterns, and concepts - TechNet articles - united states (english) - TechNet wiki. Retrieved 8/1/2012, 2012, from http://social.technet.microsoft.com/wiki/contents/articles/4346.private-cloud-principles-patterns-and-concepts.aspx

Miyamoto, T., Hayashi, M., & Nishimura, K. (2010). Sustainable network resource management system for virtual private clouds. Paper presented at the *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, 512-520.

Monwar, M. M., Gavrilova, M., & Wang, Y. (2011). A novel fuzzy multimodal information fusion technology for human biometric traits identification. Paper presented at the *Cognitive Informatics & Cognitive Computing (ICCI*CC), 2011 10th IEEE International Conference on*, 112-119.

Moteff, J. D. (2010). *Critical infrastructures: Background, policy, and implementation.* (Prepared for Members and Committees of Congress No. RL30153). Washington,

DC: Congressional Research Service, Library of Congress. Retrieved from http://www.fas.org/sgp/crs/homesec/RL30153.pdf

Nayak, S., & Yassir, A. (2012). Cloud computing as an emerging paradigm. *IJCS S, 12*(1), 61.

OASIS. (2011). Reference architecture foundation for service oriented architecture version 1.0. Retrieved 8/7/2012, 2012, from http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra.html

Offermann, P., Blom, S., Schönherr, M., & Bub, U. (2010). Artifact types in information systems design science–A literature review. *Global Perspectives on Design Science Research*, , 77-92.

Oman, P., Schweitzer, E., & Roberts, J. (2002). Protecting the grid from cyber attack, part II: Safeguarding IEDS, substations and SCADA systems. [null] *Utility Automation, 7*(1), 25-32.

Piazza, P. (2003). Measuring the value of IT security. *Security Management, 47*(11), 37. Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=459582521&Fmt=7&clientId=62763&RQT=309&VName=PQD

Porcelli, N., Selby, S., Tantono, W., Bagner, J., & Sonu, C. (2002). Hearing addresses protection of nation's critical infrastructure. *Intellectual Property & Technology Law Journal, 14*(2), 31. Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=109795045&Fmt=7&clientId=62763&RQT=309&VName=PQD

Potok, T., Elmore, M., Reed, J., & Sheldon, F. T. (2003). VIPAR: Advanced information agents discovering knowledge in an open and changing environment. Paper presented at the *Proc. 7th World Multiconference on Systemics, Cybernetics and Informatics, Orlando FL*, 28-33.

Potok, T., Phillips, L., Pollock, R., Loebl, A., & Sheldon, F. (2003). Suitability of agent technology for command and control in fault-tolerant, safety-critical responsive decision networks. Paper presented at the *Proc. 16th Int'l Conf. Parallel and Distributed Computing Systems, Reno V,*

Pounder, C. (2002). The US's national strategy for homeland security. *Computers & Security, 21*(6), 503-505. doi: DOI: 10.1016/S0167-4048(02)01005-2

Preparata, F. P., Metze, G., & Chien, R. T. (1967). On the connection assignment problem of diagnosable systems. *Electronic Computers, IEEE Transactions on*, (6), 848-854.

Qiang, Q. (2009). In Nagurney A. (Ed.), *etwork efficiency/performance measurement with vulnerability and robustness analysis with application to critical infrastructure*. United States -- Massachusetts: Management. Retrieved from http://search.proquest.com/docview/304924975?accountid=27965

Rak, A. (2002). Information sharing in the cyber age: A key to critical infrastructure protection. *Information Security Technical Report, 7*(2), 50-56. doi: DOI: 10.1016/S1363-4127(02)02006-X

Rich, E., Gonzalez, J. J., Qian, Y., Sveen, F. O., Radianti, J., & Hillen, S. (2009). Emergent vulnerabilities in integrated operations: A proactive simulation study of economic risk. *International Journal of Critical Infrastructure Protection, 2*(3), 110-123. doi: 10.1016/j.ijcip.2009.07.002

Rosenzweig, P. (2012). The alarming trend of cybersecurity breaches and failures in the U.S. government. *The Heritage Foundation, Leadership for America, 2695*

Rupley, S. (2009). 11 top open-source resources for cloud computing — tech news and analysis Retrieved 11/16/2012, 2012, from http://gigaom.com/2009/11/06/10-top-open-source-resources-for-cloud-computing/

Salehie, M., Pasquale, L., Omoronyia, I., & Nuseibeh, B. (2012). Adaptive security and privacy in smart grids: A software engineering vision. Paper presented at the *Software Engineering for the Smart Grid (SE4SG), 2012 International Workshop on*, 46-49.

Schweitzer, D. (2005). Be prepared for cyberterrorism. *Computerworld, 39*(13), 42.

Seifert, J. W. (2002). The effects of september 11, 2001, terrorist attacks on public and private information infrastructures: A preliminary assessment of lessons learned. *Government Information Quarterly, 19*(3), 225-242. doi: DOI: 10.1016/S0740-624X(02)00103-X

Shan, C., Heng, C., & Xianjun, Z. (2012). Inter-cloud operations via NGSON. *Communications Magazine, IEEE, 50*(1), 82-89.

Sharma, M., & Sharma, P. (2012). Performance evaluation of adaptive virtual machine load balancing algorithm. *Performance Evaluation, 3*(2)

Sheldon, F., Potok, T., Langston, M., Krings, A., & Oman, P. (2004). *Autonomic approach to survivable cyber-secure infrastructures* [null]

Sheldon, F. T., Kavi, K. M., Tausworthe, R., Yu, J. T., Brettschneider, R., & Everett, W. W. (1992). Reliability measurement: From theory to practice. *Software, IEEE, 9*(4), 13-20.

Sheldon, F. T., Elmore, M. T., & Potok, T. E. (2003). An ontology-based software agent system case study. Paper presented at the *Information Technology: Coding and Computing [Computers and Communications], 2003. Proceedings. ITCC 2003. International Conference on*, 500-506.

Sheldon, F. T., Jerath, K., & Chung, H. (2002). Metrics for maintainability of class inheritance hierarchies. *Journal of Software Maintenance and Evolution: Research and Practice*, *14*(3), 147-160.

Sheldon, F. T., Jerath, K., & Greiner, S. A. (2002). Examining coincident failures and usage-profiles in reliability analysis of an embedded vehicle sub-system. Paper presented at the *Proc inth Int'l Conf. on Analytical and Stochastic Modeling Techniques [ASMT 2002]*, 3-5.

Sheldon, F., Potok, T., & Kavi, K. (2004). Multi-agent systems for knowledge management and decision networks. *Informatica*, *28*, 79-89.

Shi, Y., Jiang, X., & Ye, K. (2011). An energy-efficient scheme for cloud resource provisioning based on CloudSim. Paper presented at the *Cluster Computing (CLUSTER), 2011 IEEE International Conference on*, 595-599.

Shiffman, G., & Gupta, R. (2013). Crowdsourcing cyber security: A property rights view of exclusion and theft on the information commons. *International Journal of the Commons*,

Smith, J. (2012). GOP senators rework cybersecurity bill - tech daily dose.*2012*(8/12/2012)

Stark, A. (2007). Policymaking for critical infrastructure: A case study on strategic interventions in public safety telecommunications by gordon A. gow. *Journal of Contingencies & Crisis Management*, *15*(1), 65-66. doi: 10.1111/j.1468-5973.2007.00506.x

Stickman, J. F. (2001). *Assessing united states information assurance policy response to computer-based threats to national security.* (D.P.A., University of Southern California). , 701. Retrieved from http://proquest.umi.com.library.capella.edu/pqdweb?did=725983671&Fmt=7&clientId=62763&RQT=309&VName=PQD. (3027782).

Suo, S., Techatassanasoontorn, A. A., & Purao, S. (2011). The interplay between cloud-based SOA and IT departments: Research directions.

Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. *AI Magazine*, *11*(4), 37.

Tao, J., Franz, D., Marten, H., & Streit, A. (2012). An implementation approach for inter-cloud service combination. *International Journal on Advances in Software, 5*(1 and 2), 65-75.

Taylor, C., Harrison, W., Krings, A., Hanebutte, N., & McQueen, M. (2001). Low-level network attack recognition: A signature-based approach. Paper presented at the *Proc. 13th International Conference on Parallel and Distributed Computing and Systems, Anaheim, California,* 570-574.

Taylor, C., Krings, A., Harrison, W., & Hanebutte, N. (2002). Merging survivability system analysis and probability risk assessment for survivability analysis. Paper presented at the *IEEE DS* ,

Taylor, C., Krings, A., Harrison, W., Hanebutte, N., & McQueen, M. (2002). Considering attack complexity: Layered intrusion tolerance. *IEEE Proc.DS* ,

Taylor, C., Krings, A., & Alves-Foss, J. (2002). Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening. Paper presented at the *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC, , 64*

Taylor, C., Oman, P., & Krings, A. (2003). Assessing power substation network security and survivability: A work in progress report. Paper presented at the *Proceedings of the International Conference on Security and Management (SAM '03),*

Tehan, R. (2012). *Cybersecurity: Authoritative reports and resources.* (No. R42507). Washington, DC: Congressional Research Service, Library of Congress.

Tien, J. M. (2005). Homeland security services system: Critical decision issues. Paper presented at the *2005 International Conference on Services Systems and Services Management, 2005. Proceedings of ICSSSM'05,* 1-6.

Tristram, C. (2003). From artificial intelligence to artificial biology? [null] *Technology Review, 106*(9), 40.

Ubuntu. (2012). OpenStack with ubuntu | ubuntu Retrieved 11/16/2012, 2012, from http://www.ubuntu.com/cloud/private-cloud/openstack

Van Der Linden, R., Halls, D., & Waterhouse, S. (2010). WO Patent WO/2010/127,365.

Vijayan, J. (2012). White house exploring executive order to secure critical networks - computerworld Retrieved 8/12/2012, 2012, from http://www.computerworld.com/s/article/9230099/White_House_exploring_executive_order_to_secure_critical_networks

Wang, L., Zhan, J., & Shi, W. (2011). In cloud, can scientific communities benefit from the economies of scale? *Parallel and Distributed Systems, IEEE Transactions on, PP*(99), 1-1.

Warfield, D. (2012). Critical infrastructures: IT security and threats from private sector ownership. *Information Security Journal: A Global Perspective, 21*(3), 127-136.

Wickremasinghe, B. (2009). CloudAnalyst: A CloudSim-based tool for modelling and analysis of large scale cloud computing environments. *MEDC Project Report*,

Wickremasinghe, B., Calheiros, R. N., & Buyya, R. (2010a). CloudAnalyst: A CloudSim-based visual modeller for analysing cloud computing environments and applications. Paper presented at the *2010 24th IEEE International Conference on Advanced Information etworking and Applications*,446-452.

Wickremasinghe, B., Calheiros, R. N., & Buyya, R. (2010b). 2010 24th IEEE international conference on advanced information networking and applications; CloudAnalyst: A CloudSim-based visual modeller for analysing cloud computing environments and applications Paper presented at the 446 <last_page> 452. doi: 10.1109/AINA.2010.32

Yadav, A. K., Tomar, R., Kumar, D., & Gupta, H. (2012). Security and privacy concerns in cloud computing. *International Journal, 2*(5)

Zhou, Z., Sheldon, F., Potok, T., & Orlando, J. (2003). 31-aug. 2, 2003, modeling with stochastic message sequence charts. Paper presented at the *IIIS Proc. Int'l. Conf. on Computer, Communication and Control Technology*,

APPE DIX A. CYBERSECURITY BROADCASTS

CSPAN-2 (3/7/13). Retrieved on 3/9/13, from: http://www.c-spanvideo.org/program/311370-1

CSPAN-2 (2/14/13). Retrieved on 2/16/13, from: http://www.c-spanvideo.org/program/311281-1

CSPAN-2 (2/22/13). Retrieved on 2/25/13, from: http://www.c-spanvideo.org/program/311129-5

CSPAN-2 (2/13/13). Retrieved on 2/13/13, from: http://www.c-span.org/Events/Deputy-Commerce-Secretary-Discusses-Cybersecurity-Priorities/10737438030/

CSPAN-2 (9/28/12). Retrieved on 9/28/12, from: http://www.c-span.org/Events/Homeland-Security-Secretary-Speaks-on-Cybersecurity/10737434500/

CSPAN-2 (9/22/12). Retrieved on 9/22/12, from: http://www.c-spanvideo.org/program/308353-6

CSPAN-2 (9/19/12). Retrieved on 9/19/12, from: http://www.c-span.org/Events/Top-Federal-Security-Chiefs-Update-Congress-on-Homeland-Threats/10737434210-1/

CSPAN-2 (9/14/12). Retrieved on 9/14/12, from: http://www.c-span.org/Events/House-Subcmte-Examines-2009-Attack-at-Fort-Hood-Texas/10737434111/

CSPAN-2 (8/14/12). Retrieved on 8/14/12, from: http://www.c-spanvideo.org/program/KeithA

CSPAN-2 (10/6/11). Retrieved on 3/3/13, from: http://www.c-spanvideo.org/program/301933-1

CSPAN-2 (10/22/2010). Retrieved on 3/10/13, from: http://www.c-spanvideo.org/program/311370-1

APPE DIX B. DEFI ITIO OF TERMS

- **Autonomic computing** - *computer systems capable of self-management.*

- **Client–server model** - *Client–server computing refers broadly to any distributed application that distinguishes between service providers (servers) and service requesters (clients).*

- **Cloud Computing** - *A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (www.nist.gov)*

- **Cloud Oriented Architecture** - *A term coined by Jeff Barr at Amazon Web Services to describe an architecture where applications act as services in the cloud and serve other applications in the cloud environment.*

- **Cloud provider** - *A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals, usually for a fee.*

- **Collaboration** - *Means the process of working together to achieve shared goals.*

- **Coordinate** - *A consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.*

- **Critical infrastructure** - *critical infrastructure has the meaning given the term in 42 U.S.C. 5195c(e), "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

- **Data Transfer Time** - *The time taken by a given amount of data to be transported from one point to another. This is taken to be equivalent to the available bandwidth divided by the size of the unit of data.*

- **Data Transmission Latency** - *This document uses "Transmission Latency" to mean the network delay (based on geographical distance, operation of network equipment etc.) between 2 points. This can be considered equivalent to half of the ping round-trip time.*

- **Disruptive technology** - *A term used in the business world to describe innovations that improve products or services in unexpected ways and change*

both the way things are done and the market. Cloud computing is often referred to as a disruptive technology because it has the potential to completely change the way IT services are procured, deployed, and maintained.

- **Elastic computing -** *The ability to dynamically provision and de-provision processing, memory, and storage resources to meet demands of peak usage without worrying about capacity planning and engineering for peak usage.*

- **Grid computing** - a form of distributed computing and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks

- **IaaS -** *Infrastructure as a service. IaaS a basic cloud service model where cloud providers offer computers as physical or more often as virtual machines, raw (blocks) storage, firewalls, load balancers, and networks. IaaS providers supply these resources on demand from their large pools installed in data centers. Local area networks including IP addresses are part of the offer. For the wide area connectivity, the Internet can be used or - in carrier clouds - dedicated virtual private networks can be configured.*

- **Mainframe computer** - *powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as census, industry and consumer statistics, enterprise resource planning, and financial transaction processing.*

- **On-demand service -** *A model that allows a user to purchase cloud services as needed; for instance, if users need to utilize additional servers for the duration of a project, they can do so and then drop back to the previous level after the project is completed.*

- **PaaS (Platform as a service) -** *PaaS is a category of cloud computing services that provide a computing platform and a solution stack as a service. It is a service model of cloud computing. In this model, the consumer creates the software using tools and libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers and storage.*

- **Peer-to-peer** - *a distributed architecture without the need for central coordination, with participants being at the same time both suppliers and consumers of resources (in contrast to the traditional client–server model).*

- **Public cloud -** *Services offered over the public Internet and available to anyone who wants to purchase the service.*

- **Resilience** - *The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.*

- **Response Time -** *The time taken by an Internet application defined as the time interval between sending the request and receiving a response.*

- **SaaS (Software as a service)** - *SaaS sometimes referred to as on-demand software, is a software delivery model in that have software and associated data centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser.*

- **Sector-Specific Agency (SSA)** - *Means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.*

- **Secure and Security –** *These terms refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.*

- **SLA -** *Service level agreement are contractual agreement that defines the level of service, responsibilities, priorities, and guarantees regarding availability, performance, and other aspects of the service provided by the service provider.*

- **Utility computing** - *The packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity.*

APPE DIX C. ACRO YMS

- **A SI** American National Standards Institute
- **API –** Application Program Interface
- **AR function** Arrival Rate Function
- **CDO** Cloud Deployment Option
- **CEC** Cloud Environment Constraint
- **CIP** critical infrastructure protection
- **CRM** Customer Relationship Management
- **DHHS** Department of Health and Human Services
- **DHS** Department of Homeland Security
- **FERC** Federal Energy Regulatory Commission
- **FFIEC** Federal Financial Institutions Examination Council
- **FISMA** Federal Information Security Management Act
- **HSPD-7** Homeland Security Presidential Directive 7
- **IaaS** Infrastructure as a Service
- **IEC** International Electro-technical Commission
- **ISA** International Society of Automation
- **ISO** International Organization for Standardization
- **KDM** Knowledge Discovery Meta-Model
- **MWC** Method Workload Characteristic
- **CSD** National Cyber Security Division
- **ERC** North American Electric Reliability Corporation

- **IPP** National Infrastructure Protection Plan
- **IST** National Institute of Standards and Technology
- **RC** Nuclear Regulatory Commission
- **OCR** Office for Civil Rights
- **PaaS** Platform as a Service
- **REST** – Representational State
- **RPC** Remote Procedure Call
- **SCC** sector coordinating council
- **SOA** Service Oriented Architectures
- **QoS** Quality of Service
- **SaaS** Software as a Service
- **VM** Virtual Machine
- **VMM** Virtual Machine Monitor